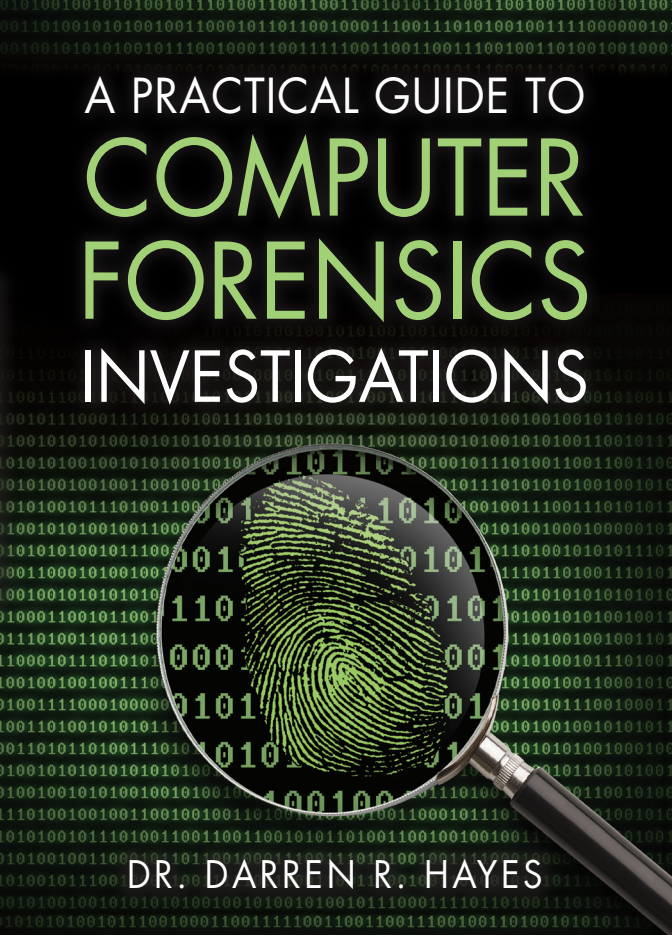
# A PRACTICAL GUIDE TO COMPUTER FORENSICS INVESTIGATIONS



DR. DARREN R. HAYES

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

# A Practical Guide to Computer Forensics Investigations

Dr. Darren R. Hayes

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

## A Practical Guide to Computer Forensics Investigations



ISBN-13: 978-0-7897-4115-8
ISBN-10: 0-7897-4115-6

Library of Congress Control Number: 2014955541

Printed in the United States of America

First Printing: December 2014

### Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

### Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

### Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

**Associate Publisher**
Dave Dusthimer

**Acquisitions Editor**
Betsy Brown

**Development Editor**
Jeff Riley

**Managing Editor**
Sandra Schroeder

**Project Editor**
Mandie Frank

**Copy Editor**
Krista Hansing

**Indexer**
Larry Sweazy

**Proofreader**
Megan Wade-Taxter

**Technical Editors**
Dennis Dragos
Shawn Merdinger

**Publishing Coordinator**
Vanessa Evans

**Designer**
Alan Clements

**Compositor**
Tricia Bronkella

# Contents at a Glance

# Table of Contents

# About the Author

**Dr. Darren R. Hayes** is a leading expert in the field of digital forensics and computer security. He is the director of cybersecurity and an assistant professor at Pace University, and he has been named one of the Top 10 Computer Forensics Professors by Forensics Colleges.

Hayes has served on the board of the High Technology Crime Investigation Association (HTCIA), Northeast Chapter, and is the former president of that chapter. He also established a student chapter of the HTCIA at Pace University.

During his time at Pace University, Hayes developed a computer forensics track for the school's bachelor of science in information technology degree. He also created a computer forensics research laboratory, where he devotes most of his time to working with a team of students in computer forensics and, most recently, the burgeoning field of mobile forensics. As part of his research and promotion of this scientific field of study, he has fostered relationships with the NYPD, N.Y. State Police, and other law enforcement agencies. He also organized a successful internship program at the cybercrime division of the New York County D.A. Office and the Westchester County D.A. Office.

Hayes is not only an academic, however—he is also a practitioner. He has been an investigator on both civil and criminal investigations and has been called upon as an expert for a number of law firms. In New York City, Hayes has been working with six to eight public high schools to develop a curriculum in computer forensics. He collaborates on computer forensics projects internationally and has served as an extern examiner for the MSc in Forensic Computing and Cybercrime Investigation degree program at University College Dublin for four years.

Hayes has appeared on Bloomberg Television and Fox 5 News and been quoted by *Associated Press, CNN, Compliance Week, E-Commerce Times, The Guardian (UK), Investor's Business Daily, MarketWatch, Newsweek, Network World, Silicon Valley Business Journal, USA Today, Washington Post*, and *Wired News*. His op-eds have been published by American Banker's BankThink and The Hill's Congress Blog. In addition, he has authored a number of peer-reviewed articles in computer forensics, most of which have been published by the Institute of Electrical and Electronics Engineers (IEEE). Hayes has been both an author and reviewer for Pearson Prentice Hall since 2007.

## About the Technical Reviewer

**Dennis Dragos**, President of DDragos Information Security and Investigation Corp. (DDIS) served 20 years in the New York City Police Department. For 11 years, he was assigned to the NYPD Computer Crimes Squad, Special Investigations Division, Detective Bureau, reaching the rank of 2nd grade detective. He is currently an adjunct assistant professor of the Cyber Security Systems Program within the College of Professional Studies at St. John's University, Queens, N.Y.

**Shawn Merdinger** is the CISO for Valdosta State University in Georgia. He has worked with Cisco Systems, 3Com/TippingPoint at University of Florida Health Science Center, and as an independent consultant. His current research focuses on medical device security, and he is the founder of the MedSec group on LinkedIn. Shawn has presented original research at security conferences such as DEFCON, Educause, ISSA, InfraGard, Ph-Neutral, ShmooCon, CONfidence, NoConName, O'Reilly, CSI, IT Underground, CarolinaCon, and SecurityOpus. He holds a bachelor's degree from University of Connecticut and a master's from the University of Texas at Austin.

# Dedication

*This book is dedicated to my loving wife, Nalini, and my children, Nicolai, Aine, Fiona, and Shay.*

# Acknowledgments

I should begin by acknowledging my supportive and patient wife, Nalini, who is my best friend. Long hours working on a book mean sacrifices for everyone in the family, and my children, Nicolai, Aine, Fiona, and Shay, have been brilliant. My parents, Annette and Ted, have been mentors throughout my life, and I will always be in their debt.

Professionally, I should acknowledge the former deans of the Seidenberg School at Pace University, Dr. Susan Merritt and Dr. Constance Knapp, who have always believed in me and supported me. My current dean, Dr. Amar Gupta, continues to support my passion for computer forensics and security. Others who deserve honorable mention are my colleagues at Pace, Dean Jonathan Hill, Dr. Catherine Dwyer, Dr. Nancy Hale, Dr. John Molluzzo, Dean Bernice Houle, Dr. Susan Maxam, Dr. Richard Kline, Professor Andreea Cotoranu, Dr. Li-Chiou Chen, Dr. Lixin Tao, Dr. Fred Grossman, Ms. Susan Downey, Ms. Bernice Tracey, Ms. Fran O'Gara, Dr. Narayan Murthy, Dr. James Gabberty, Professor Robert Benjes, Ms. Stephanie Elson, Ms. Kimberly Brazaitis, and many others.

The students at Pace University inspire me more than they realize and work many hours in the computer forensics lab. I appreciate all the hard work and dedication by Pace students Mr. Roman Perez, Ms. Renee Pollack, Mr. Mario Camilla, Mr. James Ossipov, Mr. Shariq Qureshi, Ms. Eileen Mulhall, Mr. Matthew Chao, Mr. Jakub Redziniak, and Ms. Fitore Balidemaj, to name but a few.

I wish to acknowledge my good friends from the Computer Crimes Squad, New York Police Department. We have enjoyed a marvelous relationship with the NYPD for many years, and I have attended many certification classes with them. My friends and colleagues include Det. Dennis Dragos, Det. Richard Macnamara, Det. Robert DiBattista, Det. Jorge Ortiz, Det. Joseph Garcia, Lt. Dennis Lane, Lt. Felix Rivera, Det. Owen Soba, Det. Waldo Gonzalez, Det. John Crosas, and a number of other wonderful detectives. I have also gained invaluable practical experience by working with former Lt. John Otero, former Det. Domingo Gonzalez, and former Det. Yalkin Demirkaya.

I would also like to mention other law enforcement and government agencies that have been marvelous friends and collaborators. They include the New York State Police, Federal Bureau of Investigation, United States Secret Service, Central Intelligence Agency, Bundeskriminalamt, U.K. law enforcement, and Europol.

My thanks to Mr. David Szuchman, Mr. Richard Brittson, and Mr. Steven Moran of the New York County D.A. Office. Thanks also to Mr. Michael Delohery, Bureau Chief, High Technology Crime Bureau, Westchester County D.A., and his colleagues.

Special thanks to Mr. Ryan Kubasiak, an expert in Mac forensics and my good friend; Mr. Thomas Ryan, Bristol Global; and Mr. Kenneth Citarella, one of the founding fathers of HTCIA Northeast. Thanks also to Dr. John Collins, Chairperson; and Mr. Bill Soo Hoo, College of Professional Studies, New Jersey City University. Ms. Bernadette Gleason, Citi, Ms. Dora Gomez, and Alex Allphin have been tremendous supporters as well. I appreciate the professional support and guidance from my good friend Francis X. Schroeder.

My sincere thanks to Mr. Warner Johnston and Ms. Ruth Fasoldt from the Association of Chartered Certified Accountants USA. Their tremendous support for our work at Pace has been well noted. I also wish to thank my friends at my alma mater, University College Dublin, Ireland. Dr. Pavel Gladyshev and Dr. Fergus Toolan have been terrific collaborators, and it was an honor to serve as extern examiner for their master of science in forensic computing and cybercrime investigation.

Ms. Debra Lesser, Executive Director, Justice Resource Center, has been very kind to me over the years and has allowed me to work with many magnificent high school teachers, including Mr. Stephen Bland, from Lehman High School. My thanks also to Ms. Gladys Aviles, Executive Assistant, and Carolyn Morway, Civic Education Coordinator, at the Justice Resource Center.

## We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

*Please note that we cannot help you with technical problems related to the topic of this book.*

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

## Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

# Introduction

The field of digital forensics is relatively new, and more books are being published on this subject matter in recent times. The problem is that many of books are very technical but are lacking in terms of the investigative skills. To be an exemplary computer forensics examiner, you need to have both technical and investigative skills. For example, simply finding the evidence on a computer is not good enough—you must be able to place the suspect behind the keyboard. Moreover, a good investigator must be able to think well beyond the scope of the computer. Chapter 11, "Mobile Forensics," is a good example of this: an investigator can retrieve an extraordinary amount of evidence about a user's activity on a smartphone without actually seizing the device. This book also clearly outlines the many different skills that are beneficial in the field of computer forensics, including knowledge of hardware, programming, and the law, as well as the ability to speak a second language and possession of solid writing skills.

This book assumes no prior knowledge of the subject matter, and I have written it for both high school and university students and professional forensics investigators. Additionally, other professions can clearly benefit from reading this book—it is useful for lawyers, forensic accountants, security professionals, and others who have a need to understand how digital evidence is gathered, handled, and admitted to court. The book places a significant emphasis on process and adherence to the law, which are equally important to the evidence that can ultimately be retrieved.

The reader of this book should also realize that a comprehensive knowledge of computer forensics can lead to a variety of careers. Digital forensics examiners and experts work for accounting firms, software companies, banks, law enforcement, intelligence agencies, and consulting firms. Some are experts in mobile forensics, some excel in network forensics, and others focus on personal computers. Other experts specialize in Mac forensics or reverse engineering malware. The good news for graduates with computer forensics experience is that they have a variety of directions to choose from: the job market for them will remain robust, with more positions than graduates for the foreseeable future.

This book is a practical guide, not only because of the hands-on activities it offers, but also because of the numerous case studies and practical applications of computer forensics techniques. Case studies are a highly effective way to demonstrate how particular types of digital evidence have been successfully used in different investigations.

Finally, this book often refers to professional computer forensics tools that can be expensive. You should realize that academic institutions can take advantage of significant discounts when purchasing these products. I also included many free or low-cost forensics tools in the book, and these can be just as effective as some of the expensive tools. You can definitely develop your own program or laboratory in a budget-conscious way.

Register this Book to unlock the data files that are needed to complete the end-of-chapter projects.

Follow the steps below:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780789741158
3. Click on the "Access Bonus Content" link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Chapter 9

# Mobile Forensics

## Learning Outcomes

After reading this chapter, you will be able to understand the following:

- The evolution and importance of cellphone forensics;
- An overview of cellular networks;
- The type of evidence available from cellphone carriers;
- Retrieving evidence from a smartphone;
- Conducting SIM card forensics;
- Analyzing cellphone operating systems;
- Legal considerations associated with cellphone investigations;
- Tablets, GPS and other mobile device forensics; and
- How to document a cellphone investigation.

## Introduction

The field of mobile forensics has exploded in recent times and is now one of the most important areas of research, for several reasons. First and foremost, the capabilities of cellphones have been greatly enhanced; these devices are arguably more important than desktop or laptop computers because they are generally always turned on and usually always mobile. Therefore, they continually record our movements and our activities and provide tremendous insight into our behavior. Communication on a cellphone is very different compared to a traditional computer; interestingly, criminals often say or text things on a cellphone that they would never do on a traditional computer.

Cellphone forensics has not always been taken seriously. Even in 2008, if you had asked someone in law enforcement about investigating cellphones, you would have typically heard that nobody in the laboratory worked on cellphones or that cellphones did not hold anything of value. Some people might

even have said that the only reason for cellphone forensic software was that some suspicious spouses bought the software to see if their partner was cheating.

Hardware imaging devices have also been used for a number of years but were not originally used for investigations. Cellebrite sold its hardware to cellphone retailers who needed a device to copy the contents of a customer's cellphone and its SIM card to another cellphone, usually when the customer wanted to upgrade to a new phone. When law enforcement became involved in cellphone investigations, Cellebrite made some minor modifications and began selling many more devices.

Cellphone forensics was always important, but not many people realized its importance. This is not surprising: The available cellphone forensic software could not work with the vast majority of cellphones. After Internet capabilities were added to cellphones, their importance to investigations grew. With this demand came better forensic software. Suddenly, more evidence was available, including email, Internet searches, and social networking activity. Today just about every computer forensics laboratory has cellphone forensic capabilities. Additionally, there has been a separation of duties in larger laboratories. For example, one investigator may be responsible for extracting evidence from the cellphone, while another investigator might be responsible for much of the paperwork, including subpoenas to cellphone carriers. Yet another investigator may be responsible for gathering and analyzing data from base transceiver stations. A **base transceiver station (BTS)** is the equipment found at a cell site that facilitates the communication of cellphone users across a cellular network.

Cellphone forensics has tremendous challenges, however. A huge number of cellphones still cannot be imaged. Forensic software and hardware supports only the most popular cellphones—more than a hundred new cellphones come to market each year, but many will never be supported by forensic tools. Some of the most problematic cellphones to examine are the inexpensive pay-as-you-go phones from companies like TracFone. Issues also exist with some cellphones from the other smaller cellular companies, like Virgin Mobile, Boost, and MetroPCS.

The issue of encrypted mobile platforms and applications for mobile devices developed by companies like Silent Circle is also relevant. The Blackphone is another challenge for investigators because the developers claim to protect the user's privacy through advanced encryption. Investigators also face a plethora of operating systems running on cellphones today. An investigator working with a laptop will generally encounter a Microsoft Windows operating system or Apple's Mac OS X (operating system). An investigator who obtains a cellphone, on the other hand, could encounter a Symbian, RIM, Windows, iOS, Android, or other mobile device operating system.

In looking to the future, our dependency on cellphone forensics will only increase, and the number of vendor-supported cellphones and tablets will expand. The vociferous market for Android and iOS devices means that the investigator must look outside the device more—to the synced computer, to the synced devices in the home and at work, and to the cloud. Cellphones continue to have a growing dependence on cloud computing, which means that investigators will increasingly rely on evidence that goes beyond the scope of the network carrier. Integrated user applications found on the cellphone, like Facebook and Gmail, are important and will increase in importance. Moreover, we should continually think outside the box as good investigators do. For example, many smartphone users with newer

cars can pair their device to their automobile to play music and accept calls. These dashboard systems will also often attempt to download the user's contacts, which the investigator can later retrieve.

This chapter is called "Mobile Forensics" instead of "Cellphone Forensics" because it discusses other mobile devices that can hold incriminating evidence, including tablets, personal media players, and GPS devices. As always, a good digital forensics investigator needs to think beyond the obvious.

# The Cellular Network

A cellular network is a group of cells. A cell refers to a geographic area within a cellular network. A cell site is a cell tower located in a cell. When you make a call with your cellphone, you connect with a cell tower. The communication is then transmitted to the Mobile Switching Center. The **Mobile Switching Center (MSC)** is responsible for switching data packets from one network path to another on a cellular network. If the user is calling a user on a cellular network managed by another carrier, the call is routed from the MSC to the Public Switched Telephone Network. The **Public Switched Telephone Network (PSTN)** is an aggregate of all circuit-switched telephone networks. The purpose of the PSTN is to connect all telephone networks worldwide; this is where tolls for connecting calls across different networks are calculated. Figure 9.1 details the path of a cellphone call.

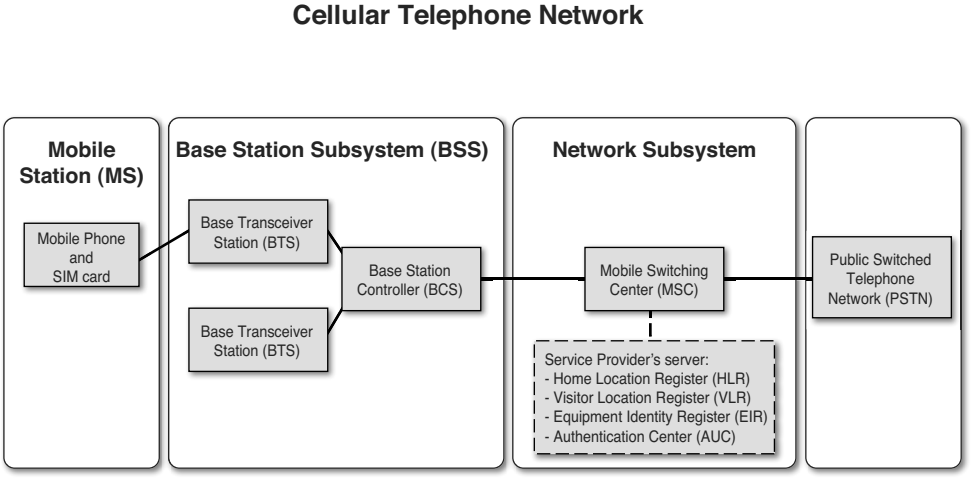



**FIGURE 9.1** Cellular network

## Base Transceiver Station

A cell site, also known as a cell tower, can be a stand-alone tower or can be attached to a building or other structure. The cell tower generally has an antenna with three panels on each side. Typically, each antenna has three sides. Usually the middle panel is a transmitter, and the two outer panels are

receivers. The cell tower is generally over 200 feet high (see Figure 9.2). A tower can contain multiple antennae, which are owned by different carriers. An antenna can be located on a cell tower or placed on the side or top of a building.

**FIGURE 9.2** Cell tower

**Let's Get Practical!**

### Locate Local Cell Towers and Antennae

Understanding the location of cell towers and antennae is helpful, and there are resources to help.

1. Start your web browser and navigate to www.antennasearch.com.
2. In the **Street Address** field, type `1600 Pennsylvania Ave NW`. For **City**, type `Washington`; for **State**, type `DC`; and for **Zip**, type `20006`; then click **Go**.
3. Click **Process** and then compare your screen to Figure 9.3.

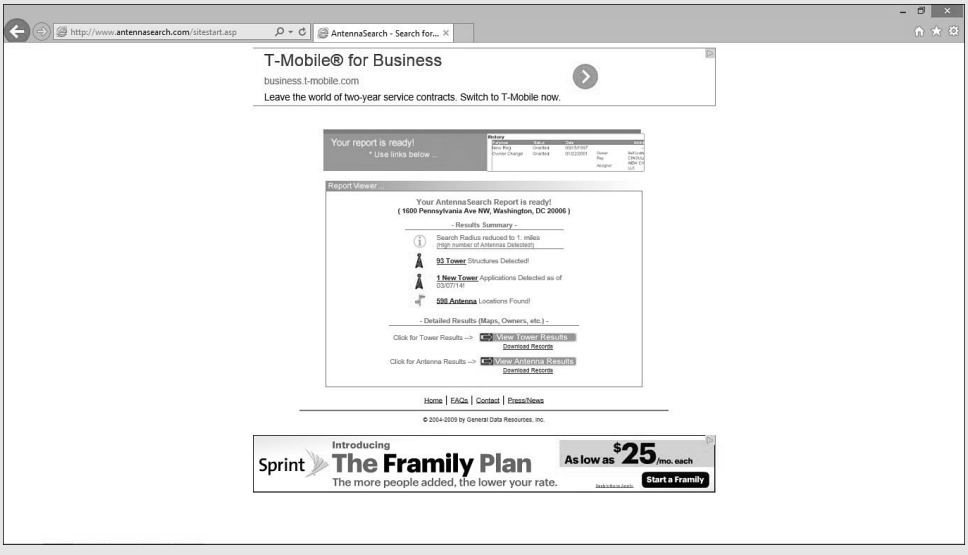



**FIGURE 9.3** Search results

4. Click the **Download Records** link under View Tower Results.
5. In the displayed **File Download** dialog box, click **Open**.

   The unformatted results display in Excel.
6. Save the file as directed by your instructor and then **Exit** Excel.
7. On the antennasearch.com website, click **View Tower Results**.

   A Google map displays. You can also click the **Satellite** button or the **Hybrid** button for a different view. You can also use the control to zoom in on a tower.
8. Click one of the cell tower links, and then compare your screen with Figure 9.4.
9. Close your web browser.


**FIGURE 9.4** Map of cell tower location

As previously noted, the Base Transceiver Station (BTS) is the equipment at the cell site that facilitates communication between the cellphone user and the carrier's network. A **Base Station Controller (BSC)** manages the radio signals for Base Transceiver Stations, in terms of assigning frequencies and handoffs between cell sites. When moving through an area, several Base Transceiver Stations might handle your call—a handoff would occur from one BTS to another. There are two types of handoff. In a **soft handoff**, a cellular communication is conditionally handed off from one base station to another, and the mobile equipment is simultaneously communicating with multiple Base Transceiver Stations. The handoff is conditional because the signal strength on a new BTS are adjudicated. In a **hard handoff**, the communication is handled by one Base Transceiver Station at a time, with no simultaneous communication.

### BTS Evidence

From a computer forensics perspective, it is important to understand how a cellular network is structured so that the investigator can determine the type of evidence that can be retrieved from the carrier's network, even without access to the suspect's handset. Law enforcement can request cell site records from a carrier for a particular cellphone user that indicate where the user was, based on data retrieved from the BTS. It is important for the investigator to specify the desired format for the evidence; getting the information in a spreadsheet is generally more helpful because the data can be easily sorted and analyzed. Figure 9.5 shows sample data from a BTS.

| Call Type | Call Start Date/Time | Duration (Mins: Seconds) | Calling Number | Called Number | First Cell ID | Last Cell ID |
|---|---|---|---|---|---|---|
| PS | 10/2/2014 09:06 | 02:11 | (914) 555-2389 | (9145) 553-4870 | 15678931 | 59487023 |
| PS | 10/2/2014 09:17 | 05:56 | (914) 555-2389 | (212) 555-9020 | 58230944 | 34598723 |
| SMS | 10/2/2014 13:22 | 00:38 | (914) 555-2389 | (516) 555-0012 | 12894232 | 98735834 |
| CS | 10/2/2014 16:01 | 12:29 | (914) 555-2389 | (516) 555-3927 | 58320321 | 35897345 |
| PS | 10/2/2014 21:39 | 01:31 | (914) 555-2389 | (646) 555-8901 | 94899917 | 34589344 |

**FIGURE 9.5** BTS data

To obtain evidence, law enforcement can contact the network carrier and explain the user information that is needed as part of an ongoing investigation. The investigator should also explain to the provider that the customer in question should not be notified about the investigation; this is covered under U.S.C. 2703(f). Law enforcement can request that the suspect's records be preserved for 90 days, pending acquisition of a search warrant. In the aftermath of Edward Snowden, more third-party services have stated that they will inform the customer about these requests unless instructed not to do so by a judge. Under U.S.C. 2307(d), law enforcement can use a court order to obtain cellular tower data.

### Subscriber Evidence

In addition to BTS evidence, law enforcement can obtain subscriber information, call detail records, and PUK codes. **Subscriber records** are personal details the carrier maintains about customers; they can include name, address, alternative phone numbers, Social Security number, and credit card information. **Call detail records (CDRs)** are details used for billing purposes; they can include phone numbers called, duration, dates and times of calls, and cell sites used. The **PIN Unlock Key (PUK)** is an unlock reset code used to bypass the SIM PIN protection.

## Mobile Station

The **mobile station** consists of mobile equipment (handset) and, in the case of a GSM network, a Subscriber Identity Module (SIM). An **International Mobile Equipment Identity (IMEI)** number uniquely identifies the mobile equipment or handset. The initial six or eight digits of the IMEI are the Type Allocation Code. The **Type Allocation Code (TAC)** identifies the type of wireless device. The website www.nobbi.com/tacquery.php allows an investigator to enter a TAC or IMEI to discover details about a specific device.

The IMEI is generally found by removing the back of the cellphone and then looking under the battery, as shown in Figure 9.6.


**FIGURE 9.6** IMEI on the cellphone

## Let's Get Practical!

### Locate the IMEI Through the Keypad

When looking for the IMEI, it is proper procedure to look under the battery. However, the IMEI can be displayed through the keypad:

1. Power on your cellphone.
2. On your keypad, type `*#06#`.

   The IMEI number should display on your GSM cellphone.

A **Universal Integrated Circuit Card (UICC)** is a smart card used to uniquely identify a subscriber on a GSM or UMTS network. With a GSM network, the smart card is a SIM; with a UMTS, the smart card is a Universal Subscriber Identity Module (USIM).

A **Mobile Equipment Identifier (MEID)** is an internationally unique number that identifies a CDMA handset (mobile equipment). The MEID was previously referred to as an Electronic Serial Number (ESN) before it was replaced by a global MEID standard around 2005. An **Electronic Serial Number (ESN)** is an 11-digit number used to identify a subscriber on a CDMA cellular network. The ESN contains a manufacturer code and a serial number that identifies a specific handset. Both the ESN and the MEID are noted on the handset in both decimal format and hex format. The website www.meidconverter.com allows users to convert between ESN and MEID and also view both decimal and hex values of an ESN or MEID. Some providers, like Virgin Mobile USA, provide a lookup feature for subscriber details using the MEID.

Many CDMA cellphones have a subsidy lock. A **subsidy lock** confines a subscriber to a certain cellular network so that a cellphone can be sold for free or at a subsidized price. From a forensics perspective, this means that the phone's file system might not be able to be acquired with an active Service Programming Code (SPC). For example, an iPhone may be available for as little as $99, but you are locked into a particular carrier and a specific contract. The unlocked iPhone may actually cost over $700 (depending on the model), but the user can easily switch carriers and is not locked into a two-year agreement. The unlocked iPhone 4S, for example, will not work on a CDMA network, like Sprint or Verizon; it will work only on a GSM network. Prepaid cellphone plans offered by T-Mobile and others in which the subscriber pays full price for the phone can be unlocked. An investigator should understand this because the handset may have been used internationally with a SIM card purchased abroad.

Locked cellphones (with an SPC) are less widely available in Europe, and carrier handset subsidies are frequently offered less. Prepaid and pay-as-you-go plans are generally more popular. In fact, in some countries, it is illegal for a cellphone carrier to sell a locked phone.

All cellphones sold in the United States have an FCC-ID. An **FCC-ID** is a number issued by the Federal Communication Commission (FCC) indicating that the handset is authorized to operate on radio frequencies within FCC control. Figure 9.7 shows a sample FCC-ID on a handset.

The FCC-ID can be viewed by removing the back of a cellphone and taking out the battery. Investigators then can enter the FCC-ID on the FCC website (http://transition.fcc.gov/oet/ea/fccid/). After you enter the FCC-ID, you can download a manual for the cellphone. This is important for an investigator who might need to know about the features of the cellphone and, more importantly, wants to know how to remove the cellphone from all networks and external communications for proper containment.

Additional information about cellphones and cellphone carriers can be obtained from the websites www.phonescoop.com, PDAdb.net, and www.gsmarena.com.


**FIGURE 9.7** FCC-ID

### SIM Card

The **SIM card** identifies a user on a cellular network and contains an IMSI. SIM cards are found in cellphones that operate on GSM cellular networks and usually in iDEN network cellphones. A user can simply add a SIM card to an unlocked cellphone. Not all U.S. cellphone carriers allow a user to purchase a SIM card and use the handset on another network. In the European Union (E.U.), generally all GSM-compatible cellphones can be unlocked. In fact, in some E.U. countries, it is illegal for cellphones to be locked.

The **International Mobile Subscriber Identity (IMSI)** is an internationally unique number on the SIM card that identifies a user on a network. The **Mobile Country Code (MCC)** is the first three digits of the IMSI. The proceeding two to three digits are the Mobile Network Code (MNC). For example, MNC 026 for MCC 310 represents the carrier T-Mobile USA. The final part of the IMSI is the MSIN, which consists of up to 10 digits. A **Mobile Subscriber Identity Number (MSIN)** is created by a

cellular telephone carrier and identifies the subscriber on the network. The **Mobile Subscriber ISDN (MSISDN)** is essentially the phone number for the subscriber. The MSISDN is a maximum of 15 digits and is comprised of the Country Code (CC), the Numbering Plan Area (NPA), and the Subscriber Number (SN). Country Codes are relatively easy to find. For example, in the Americas the CC is 1 because it is in Zone 1. For Trinidad and Tobago, it is 1-868. European countries are in Zone 3 and Zone 4. For example, Ireland, in Zone 3, is 353, and the United Kingdom, in Zone 4, is 44. The Numbering Plan Area for Nassau County, New York, is 516 and is also referred to as the area code.

The SIM card also includes an ICCID. The **Integrated Circuit Card ID (ICCID)** can be a 19- to 20-digit serial number physically located on the SIM card, or it can contain fewer numbers (see Figure 9.8).


**FIGURE 9.8** SIM card

The first two digits of the ICCID are referred to as the Major Industry Identifier (MII). The ICCID can be accessed via the SIM card in the EF_ICCID file.

### International Numbering Plans

The website www.numberingplans.com is a tremendous resource for mobile forensics examiners working with GSM cellphones. The website provides "Number Analysis Tools", which allow the user to conduct an analysis of the following:

- Phone number
- IMSI number

- IMEI number
- SIM number
- ISPC number

An **International Signaling Point Code (ISPC)** is a standardized numbering system used to identify a node on an international telecommunications network.

### Authenticating a Subscriber on a Network

The Mobile Switching Center is where user information passes to the Home Locator Register, Visitor Locator Register, and Authentication Center. The **Home Locator Register (HLR)** is a database of a carrier's subscribers and includes those users' home addresses, IMSI, telephone numbers, SIM card ICCIDs, and services used. The **Visitor Locator Register (VLR)** is a database of information about a roaming subscriber. A subscriber can be found on only one HLR but can exist in multiple VLRs. The current location of a mobile station (handset) can be found on a VLR as well. The VLR also contains the Temporary Mobile Subscriber Identity. The **Temporary Mobile Subscriber Identity (TMSI)** is a randomly generated number that is assigned to a mobile station, by the VLR, when the handset is switched on, and is based on the geographic location.

The **Equipment Identity Register (EIR)** is used to track IMEI numbers and decide whether an IMEI is valid, suspect, or perhaps stolen. The **Authentication Center (AuC)** is a database that contains the subscriber's IMSI, authentication, and encryption algorithms. The Authentication Center issues the subscriber an encryption key that encrypts wireless communications between the mobile equipment and the network.

## Cellular Network Types

There are two types of cellular service carriers. A **Mobile Network Operator (MNO)** owns and operates a cellular network. The following companies are MNOs:

- Verizon
- T-Mobile
- Sprint/Nextel
- AT&T/Cingular

A **Mobile Virtual Network Operator (MVNO)** does not own its own cellular network, but operates on the network of a Mobile Network Operator. For example, Virgin Mobile USA has its own cellular service but operates on the Sprint Network. This means that two warrants may be needed for an investigation: one for Sprint (the MNO) and one for Virgin Mobile USA (the MVNO) to obtain a suspect's records. The following companies are MVNOs:

- Virgin Mobile USA
- Net10
- MetroPCS
- TracFone
- Cricket
- SIMPLE Mobile
- Boost Mobile

### Evolution of Wireless Telecommunications Technologies

Cellular telecommunication technologies include 2G (second-generation), 3G (third-generation), and 4G (fourth-generation) communications. It is important to note that the term *cellular telephone network* is not used here because 3G and 4G cellular networks also support mobile broadband Internet services. Consumers utilizing these services can operate on cellular networks with either a Mi-Fi router or a plug-and-play USB device. **My Wireless Fidelity (Mi-Fi)** is a portable wireless router (see Figure 9.9) that provides Internet access for up to five Internet-enabled devices and communicates via a cellular network.

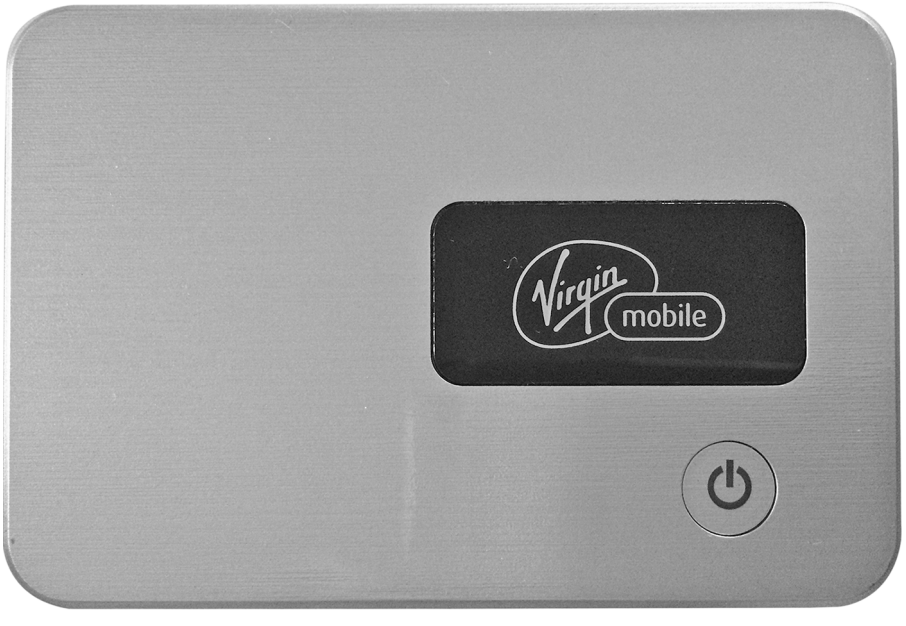



**FIGURE 9.9** Virgin Mobile USA Mi-Fi mobile hotspot

4G is the latest wireless telecommunications standard and supports high-speed large data transmission rates. **4G Long Term Evolution (LTE) Advanced** is a high-mobility broadband communication that is suitable for use on trains and in other vehicles. Motorola Mobility, which was purchased by Google in 2011, holds the patent for this technology. 4G LTE was first implemented in Oslo (Norway) and Stockholm (Sweden).

The **International Telecommunication Union (ITU)** is an agency of the United Nations that produces standards for information and communication technologies. The ITU is comprised of 193 members and more than 700 private sector and academic institutions.

### Time Division Multiple Access (TDMA)

**Time Division Multiple Access (TDMA)** is a radio communication methodology that enables devices to communicate on the same frequency by splitting digital signals into time slots, or bursts. Bursts are data packets that are transmitted on the same frequency. 2G GSM networks use the TDMA method of communication.

### Global System for Mobile Communications (GSM)

**Global System for Mobile Communications (GSM)** is an international standard for signal communications, which uses TDMA and Frequency Division Duplex (FDD) communication methods. Thus, GSM cellular telephones use bursts. GSM was created by the European Telecommunications Standards Institute (ETSI), which was primarily designed by Nokia and Ericsson. The latest and fastest GSM standard is 4G LTE Advanced. 3G GSM networks use Universal Mobile Telecommunications System (UMTS) and Wide Band CDMA (WCDMA) for communication. **WCDMA** is a high-speed signal transmission method based on CDMA and FDD methods. TDMA is often described as the precursor to the GSM protocol, although the two networks are incompatible. T-Mobile and AT&T use GSM networks in the United States.

When unlocked, GSM handsets can be used on international networks by simply purchasing a SIM card locally and activating the SIM card with a local carrier. This is important to know because a suspect could have used a GSM phone internationally, so evidence could have been when the SIM card was switched.

It should be noted that Karsten Nohl, PhD, has written extensively about security vulnerabilities associated with GSM. Nohl has presented a formula for breaking the A5-1 encryption, which GSM cellphones operating on the T-Mobile and AT&T networks use.

**3GP** is an audio/video file format found on mobile phones operating on 3G GSM cellular networks. This standard was developed by the 3rd Generation Partnership Project. **3rd Generation Partnership Project (3GPP)** is a collaboration of six telecommunications standards bodies and a large number of telecommunications corporations worldwide that provide telecommunication standards. The scope of their work includes Global System for Mobile Communication (GSM), General Packet Radio Service (GPRS), and Enhanced Data rates for GSM Evolution (EDGE). More information about 3GPP is available at www.3gpp.org. **General Packet Radio Service (GPRS)** is packet-switching wireless

communication found on 2G and 3G GSM networks. **Enhanced Data rates for GSM Evolution (EDGE)** is a high-data-transfer technology found on GSM networks. EDGE provides up to three times the data capacity of GPRS.

### Universal Mobile Telecommunications System (UMTS)

**Universal Mobile Telecommunications System (UMTS)** is a 3G cellular network standard that is based upon GSM and was developed by 3GPP. As previously noted, UMTS cellphones utilize a USIM smart card to identify the subscriber on a network. From a forensics perspective, a USIM can store more files than a SIM card. Communication across the network is via the wideband WCDMA protocol.

### Code Division Multiple Access (CDMA)

**Code Division Multiple Access (CDMA)** is a spread-spectrum communication methodology that uses a wide bandwidth for transmitting data. This technology, developed by Qualcomm, does not share channels; it uses multiplexing techniques. **Multiplexing** is where multiple signals are transmitted simultaneously across a shared medium. A fiber optic is an example of a shared medium that can use multiplexing. **CDMA2000** is a 3G technology that uses the CDMA communications protocol. CDMA technology is used by Verizon and Sprint on their U.S. nationwide cellular networks.

**3GP2** is an audio/video file format found on mobile phones operating on 3G CDMA cellular networks. This standard was developed by the 3rd Generation Partnership Project 2. **3rd Generation Partnership Project 2 (3GPP2)** is a partnership of North American and Asian 3G telecommunications companies that develop standards for third-generation mobile networks, including CDMA. For more information about the work of 3GPP2, its partners, and its members, visit www.3gpp2.org.

### Integrated Digital Enhanced Network (iDEN)

**Integrated Digital Enhanced Network (iDEN)** is a wireless technology developed by Motorola that combines two-way radio capabilities with digital cellphone technology. iDEN is based on TDMA. Nextel introduced Push-to-talk, which used iDEN, in 1993, to enable subscribers to use their cellphones like a walkie-talkie (or two-way radio). When using the cellphone with the Push-to-talk feature, cell towers are not used. iDEN is a proprietary protocol, unlike all the other major cellular networks, which use standard open protocols.

## SIM Card Forensics

The two primary functions of a SIM card are to identify the subscriber to a cellular network and to store data. We have already discussed the mechanism by which the IMSI on the SIM identifies a user on a GSM or iDEN network. More important to the investigator is the SIM card's storage of important evidence. A SIM is essentially a smart card that is comprised of a processor and memory.

### SIM Hardware

SIM cards have different form factors. The Mini-SIM is 25mm × 15 mm, and the Micro-SIM is 15mm × 12mm. There are also embedded SIM cards. Printed on the outside is a unique serial number called an ICCID. The serial interface is the area where the SIM card communicates with the handset, as in Figure 9.10.

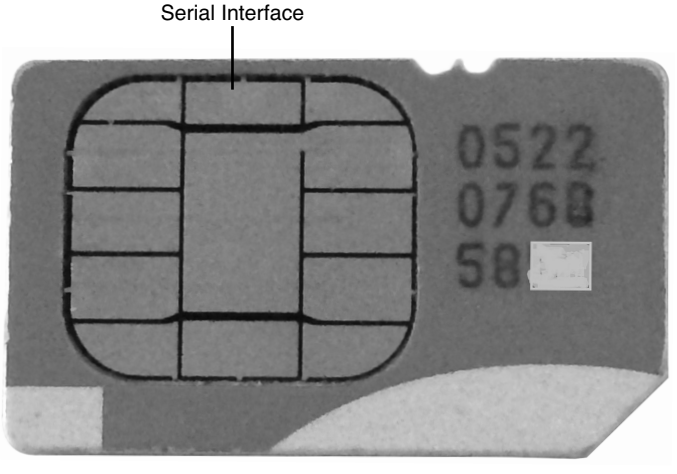



FIGURE 9.10 Serial interface

### SIM File System

The Electronically Erasable Programmable Read Only Memory (EEPROM) is where the hierarchical file system exists. The operating system, user authentication, and encryption algorithms are found on the SIM card's read-only memory (ROM).

There are three primary components of the file system:

1. Master File (MF) that is the root of the file system
2. Dedicated Files (DFs), which are basically directories
3. Elementary Files (EFs), where the data is held

The latter is where investigators can retrieve a tremendous amount of subscriber information. **Abbreviated Dialing Numbers (ADN)** contains the contact names and numbers entered by the subscriber. On the SIM, these contacts are located in the folder `EF_ADN`. **Forbidden Public Land Mobile Network (FPLMN)** refers to cellular networks to which a subscriber attempted to connect but was not authorized to do so. This information can be found in `EF_FPLMN`. This data can assist investigators who want to know where a suspect was located, even if he or she was unsuccessful in connecting to a network. **Last Numbers Dialed (LND)** refers to a list of all outgoing calls made by the subscriber. The

folder `EF_LND` holds this information. `EF_LOCI` contains the Temporary Mobile Subscriber Identity TMSI, which is assigned by the Visitor Locator Register (VLR). The TMSI represents the location where the mobile equipment was last shut down. The TMSI is four octets long and will make no sense to the investigator. However, the investigator could contact the carrier for assistance with determining the location represented by the TMSI. Table 9.1 provides the definitions of the acronyms used in the SIM file system.

**TABLE 9.1** SIM File System Acronyms

| Acronym | Definition |
|---|---|
| EF_ADN | Abbreviated Dialing Numbers (ADN) |
| EF_FPLMN | Forbidden Public Land Mobile Network (FPLMN) |
| EF_LND | Last Numbers Dialed (LND) |
| EF_LOCI | Area where the user last powered down the phone |
| EF_SMS | Short Message Service (SMS) |

Figure 9.11 shows the SIM directory structure.

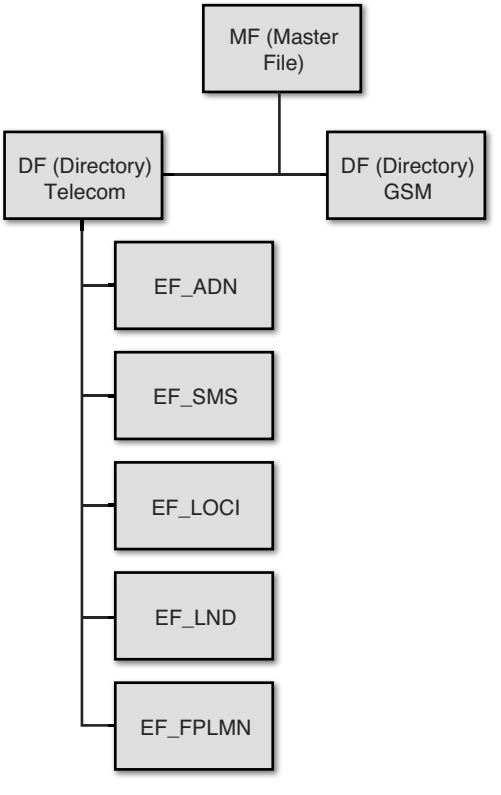



**FIGURE 9.11** SIM directory structure

### Access to the SIM

Gaining access to the data on a SIM is challenging if the SIM card has been PIN protected. A PIN on a SIM is usually four digits long but can be up to eight digits. An investigator has three attempts to get the PIN correct before the SIM is locked. After that, the device prompts for a PUK (Pin Unlock Key) or PUC (Personal Unblocking Code. An investigator can request a PUC from the carrier. A **Personal Unblocking Code (PUC)** is a code that is available from the carrier and allows a user to remove the PIN protection from the SIM card.

> **NOTE**
>
> A user can go online and change the PUK. The investigator then would be unable to access the contents of the SIM without the cooperation from the subscriber.

### SIM Card Clone

Similar to hard disk drive cloning, an investigator often chooses to clone a SIM card instead of examining the original SIM card. As a best practice, a SIM card clone should be used in the investigation in place of the original. Most cellphone forensic tools enable the investigator to clone a SIM card.

## Types of Evidence

The range of evidence available from a cellphone is quite different from what can be acquired from a laptop or desktop. One of the primary differences is the existence of SMS and MMS messages, which the following section explains in detail.

### Short Message Service (SMS)

**Short Message Service (SMS)** is a text message communication service found on mobile devices. These text messages can be found in memory on a mobile handset or on a SIM card in the handset. SMS messages are mostly saved on the handset, but when stored on the SIM card, they can be found in the `DF_TELECOM` file.

An investigator can determine whether an SMS message has been read, deleted, or sent based on the status flag. The byte value changes based on the status of the message. Table 9.2 identifies the values of the status flag and their meanings.

**TABLE 9.2** Values and Descriptions of the Status Flag Value

| Status Flag Value (Binary) | Description |
|---|---|
| 00000000 | Deleted message |
| 00000001 | Read message |
| 00000011 | Unread message |
| 00000101 | Sent message |
| 00000111 | Unsent message |

When viewing the text message with a hex editor, an unread SMS message begins with `11`, a deleted message begins with `00`, and so forth.

### Multimedia Messaging Service (MMS)

**Multimedia Messaging Service (MMS)** is a messaging service found on most cellphones that allows the user to send multimedia content, like audio, video, and images. Using a cellphone forensics tool, the investigator can carve this multimedia content out of the user's messages. MMS can be retrieved from a SIM or from the mobile device.

## Handset Specifications

Knowledge of handset hardware helps an investigator know how to safely secure the device after it has been seized. As previously noted, the investigator can research the FCC-ID on the handset online to identify the features of the mobile device.

### Memory and Processing

Cellphones contain a microprocessor, ROM chip, and random access memory (RAM). The operating system is located in ROM. Secure Digital (SD) cards, particularly microSD cards, are frequently found in smartphones as well. They can contain the following data:

- Photos
- Videos
- Apps
- Maps

Many smartphones today are opting not to use a removable SD card, but instead use an internal Embedded Multimedia Card (eMMC). This memory uses FAT32.

### Battery

Four types of cellphone batteries primarily are used: lithium ion (Li-Ion), lithium polymer (Li-Poly), nickel cadmium (NiCd), and nickel metal hydride (NiMH). The iPhone and BlackBerry Curve use a lithium ion battery, which is lightweight compared to other batteries.

### Other Hardware

Cellphones vary from model to model, but they also generally have a radio module, digital signal processor, liquid crystal display (LCD), microphone, and speaker. Some models also have a built-in keyboard.

### Accelerometer

Another feature that is frequently found on cellphones today is an accelerometer. An **accelerometer** is a hardware device that senses motion or gravity and reacts to these changes. For example, the accelerometer facilitates a screen flip when the device is turned sideways or upside-down. Moreover, the accelerometer enhances the gamer's experience by allowing the user to turn and move by changing the angle of the device. The accelerometer has become popular since its integration into the iPad and iPhone.

### Camera

Most cellphones today come with a digital camera that has still photo and video capabilities. Most smartphones possess features that allow the user to take a photo and quickly upload that picture to a social networking site like Facebook. In terms of video, many smartphones enable the user to upload content directly to sites like YouTube. Many smartphones also embed the latitude and longitude of where the photograph was taken: Most Android cellphones do this by default.

## Mobile Operating Systems

As noted in earlier chapters, the purpose of an operating system (OS) is to manage the resources of an electronic device—usually, a computer. A cellphone's OS is found in a ROM chip on the phone. From a computer forensics perspective, knowledge of an OS helps an investigator understand what type of evidence can be retrieved, the tools required to retrieve the evidence, and where to find the evidence. The problem for investigators is that mobile devices have so many different operating systems than do traditional computers. It is helpful to have at least one investigator in your lab become a registered app developer so that you can access the beta version of the latest mobile operating system version. This gives you more time to plan and adjust for new security enhancements and changes to system files.

### Android OS

**Android** is an open source operating system based on the Linux 2.6 kernel. In 2005, Google acquired Android. Android is maintained by the Open Handset Alliance (OHA), a collaborative group of telecom companies, mobile phone manufacturers, semiconductor, and software companies.

The Android OS is found on smartphones, tablets, and many other consumer electronics. Smartphones running on the Android platform can be found on the GSM, CDMA, and iDEN cellular networks. Android phones have tremendous capabilities, thanks to the numerous apps available from the Android market. However, this wealth of functionality comes at a price when it comes to battery life, and an investigator should be aware of this. Also bear in mind that a tablet could also have cellular capabilities. Numerous tablets run on Android OS, including Samsung's popular Galaxy Tab and eReaders, such as Amazon's Kindle.

Android is widely found in the auto industry. The Shanghai Automotive Industry Corporation (SAIC) now runs its media entertainment on the Android platform. The Audi 8 uses both Google Maps navigation and Google Earth. The Nevada Department of Vehicles has approved Android for use in its self-driving cars. Ford Motor Company and General Motors have also adopted Android for use in their cars, and the Renault Clio and Zoe have a 7-inch touch-screen dashboard device running on Android.

Android can also be found in home appliances. Dacor has an Android-powered oven, for example, that operates based on recipes from a tablet. Android has been integrated into refrigerators, which can scan the barcode on food labels and monitor the freshness of items left in the refrigerator; these refrigerators also assist consumers with a diet application and help complete a grocery list. Some air conditioners run on the Android OS and allow for remote control and operation, and a certain LG washer and dryer appliances runs on Android. In the future, we are likely to see what amounts to an Android ecosystem.

### Android File System

An Android device has two types of memory: RAM and NAND. As on a regular computer, RAM is volatile memory and may contain evidence that includes the user's passwords. NAND is nonvolatile flash memory. A page or a chunk on NAND can be anywhere from 512K to 2048K. Android supports a number of file systems, including Ext4, FAT32, and YAFFS2 (Yet Another Flash File System 2). The Ext4 file system can be found on the Google Nexus S and appears to be supplanting the YAFFS2 file system. YAFFS2 is an open source file system that was developed for use with NAND flash memory. Currently, a forensic analyst must download the YAFFS2 source code and review the files in a hex editor.

Microsoft's FAT32 file system resides on Android devices; the FAT32 file system is found on microSD cards, which are common in many Android handsets. The Linux file system driver for FAT32 is called VFAT. Android apps also often are run from the microSD card.

The most valuable evidence on an Android is in the libraries, especially the SQLite databases. A **SQLite database** is an open source relational database standard, which is frequently found on mobile devices. The development and maintenance of SQLite is sponsored by the SQLite Consortium, which includes Oracle, Nokia, Mozilla, Adobe, and Bloomberg.

### Samsung Galaxy

Apple may have the lion's share of the tablet market, but the Samsung Galaxy is the top-selling smartphone. The company has sold well more than 100 million units. Less than a month after its release, Galaxy S4 sales surpassed the 10 million units sold marker, which translates to 4 units sold every second. The S4 includes a new feature called Dual Shot that enables the user to simultaneously take a picture with the front and rear cameras on the device. Users can also add sound to a photo. A feature known as Group Play allows multiple owners of the S4 to share music, photos, and documents, and also play games together. The user can also create special albums with a narration to go with the pictures,

called Story Album. S Voice is a voice-activated artificial intelligence that comes with Samsung Galaxy S3, the S4, and certain Galaxy Note tablets. The feature is similar to Apple's Siri.

Released in September 2013, the Samsung Galaxy Gear is a watch that connects to the Galaxy smartphone. The watch comes complete with a 1.9-megapixel camera, allows 720p video recording, contains 4GB of memory, and supports Bluetooth. This smart watch allows the user to place and answer calls directly through the watch. Therefore, when seizing a Samsung Galaxy smartphone or tablet, the investigator must be aware that a paired watch may also need to be seized.

Spring 2014 saw the release of the Samsung S5. The impressive part of this device is its 16-megapixel camera with UHD 4K video recording at 30 fps. The device also comes with a fingerprint scanner, which can pose accessibility issues for investigators. The device has a heart rate monitor as well, to help with personalization and prove ownership of the smartphone. The S5 runs on Android 4.4.2 KitKat. Like its predecessor, this device also syncs to a smart watch called Gear 2 Neo.

### Android Evidence

Investigators can extract evidence from an Android smartphone in four ways:

1. Logical (hardware/software)
2. Physical (hardware/software)
3. Joint Test Action Group (JTAG)
4. Chip-off

Some mobile forensic software supports logical acquisition of a smartphone, which means that only user data can be recovered, not system files. Optimally, the investigator should acquire a physical image when possible. A physical image is generally acquired from a backup or by pushing an exploit to the device. To retrieve the user files on an Android, the Data Partition must be accessed by rooting the device.

#### Joint Test Action Group (JTAG)

**Joint Test Action Group (JTAG)** is an IEEE standard (IEEE 1149.1) for testing, maintenance, and support of assembled circuit boards. JTAG has become increasingly important as a way to bypass security and encryption on a smartphone to obtain a physical dump of the phone's data.

The RIFF box in Figure 9.12 is used to acquire the data from the circuit board on the cellphone. A full dump of NAND memory can be obtained. The connectors are carefully soldered onto the JTAG points on the circuit board. Voltage can be applied to the circuit board using a cellphone battery and can be monitored using a voltmeter.

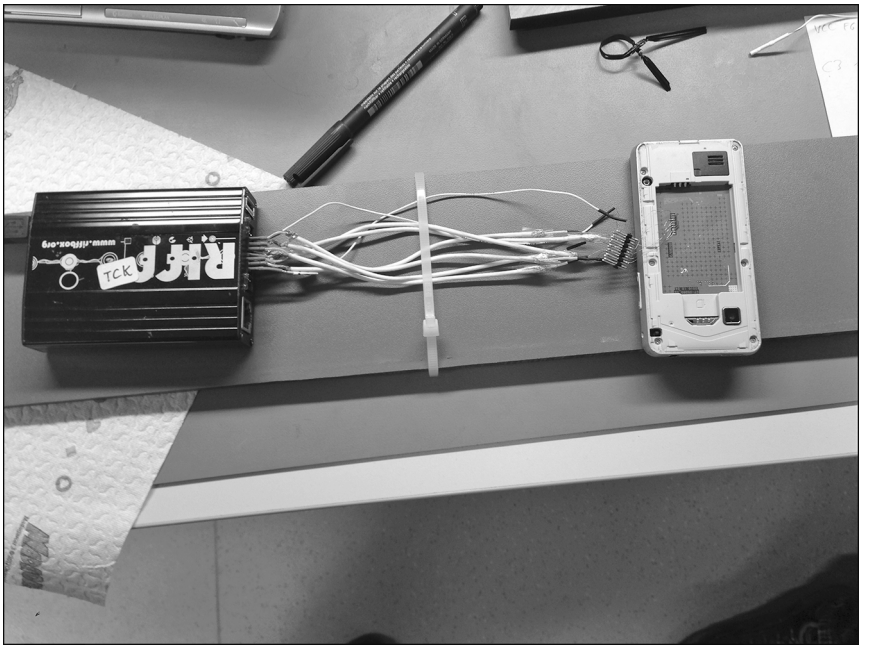



**FIGURE 9.12** JTAG acquisition with a RIFF box

### Chip-Off

When mobile forensics software or a UFED Touch cannot be used, JTAG is the next course of action. The last resort available to the investigator, when all else fails, is chip-off. Very few computer forensics labs conduct chip-off because of the high costs involved and because the skills required create a significant barrier to entry; this method is also not always successful. Chip-off can be used to circumvent encryption on many different circuit boards or be used to access data on a chip when the circuit board has been damaged. The chip can be removed from the board by applying hot air or infrared to the soldered pins. The chip can then be added to an adapter (see Figure 9.13) and read.

**FIGURE 9.13** Chip adaptors

### Android Security

Users can secure their Android smartphone in these ways:

- PIN-protection (a numeric PIN number);
- Password (alpha-numeric);
- Pattern lock, where a finger is used to secure the device with gestures (swiping motion); and
- Biometrics (an iris or retina scan, or perhaps facial recognition).

The pattern lock is also referred to as a *gesture*. The user swipes a 3×3 grid (9 dots) on the smartphone screen, and no dot can be swiped more than once. This means that working out the user's gesture is not too difficult. The 20-byte hex value found in `gesture.key` file can be added to a free tool produced by viaForensics, called viaExtract, to determine the pattern lock. The path to this gesture file is `data/system/gesture.key`. The file is encrypted with a SHA-1 hash algorithm. To obtain the gesture, a physical image of the device is conducted.

Password protection can be the most difficult to crack. The file where the password is stored can be found here: *data/system/pc.key*. An investigator can attempt to crack the password using brute force or can use a dictionary attack.

A PIN on an Android has a maximum of eight digits. After the user unsuccessfully enters the PIN a number of times, then the user is requested to enter the Gmail login and password.

Some biometric, third-party solutions rely on facial recognition. Interestingly, this type of security can be bypassed by using a photo of the suspect's face to unlock the device.

An investigator should also consider searching for the latest security vulnerabilities associated with Android and other mobile device platforms. Security flaws, as well as application vulnerabilities, are regularly uncovered and made public online and may provide an opportunity to gain access to valuable evidence. Of course, investigators must decide whether an approach is forensically sound.

### Android Forensics Tools

Many different Android forensics tools are available. viaForensics is one organization that produces free tools, such as Santoku, which enables the examiner to image an Android device. The company also produces AFLogical, which performs a logical acquisition of Android 1.5 or higher. The data acquired is stored on a blank SD card.

### Android Applications (Apps)

Android applications (apps) are developed in Java and have an `.apk` file extension. For Google Play to accept an Android application, a signed certificate must be associated with the application. Applications run in a Dalvik Virtual Machine (DVM) and have a unique user ID and process. This enforces application security and prevents data sharing with other apps. Especially helpful for the investigator is the fact that the date and time when an app is executed are stored on the device. It is the developer that decides what data will be shared, and therefore the data that the examiner can retrieve is only as good as what the developer has made available.

The developer has four choices for data storage:

1. Preference
2. Files
3. SQLite database
4. Cloud

SQLite databases can be a great source of evidence for the investigator. The following tools retrieve data from these relational databases:

- SQLite Database Browser (http://sqlitebrowser.sourceforge.net/)
- SQLite Viewer (www.oxygen-forensic.com/en/features/sqliteviewer/)
- SQLite Analyzer (www.kraslabs.com/sqlite_analyzer.php)

Every time an Android user walks past a Wi-Fi hotspot, that hotspot is recorded on that device, regardless of whether the user attempted to connect to that device. This information can be retrieved from `Cache.WiFi`. The data retrieved from this file can be used to map out where a user was moving from and to. Third-party applications have used this locational information to track where users go and as a basis for other applications, like traffic alert services. Therefore, an investigator should also consider the locational data being recorded by third-party apps.

Facebook is one of the most popular apps found on smartphones. It is important to know that just about all the information stored in a user's online profile can be found in that user's smartphone or tablet. `Fb.db` is the SQLite database that contains a user's Facebook contacts, chat logs, messages, photos, and searches.

A user's login and password for Exchange can be found in plain text at the following path: `/data/data/com.android.email/databases/EmailProvider.db`. A user's Gmail login and password can also be found in plain text at `com.google.android.gm`.

Android smartphones come with a GPS application for turn-by-turn directions, called Navigation. The SQLite database associated with Navigation is `Da_destination.db`. This file contains the sound files (WAV) that can be played to determine the directions a suspect took.

Of course, there is also cellular telephone evidence. SMS and MMS can be found at `/data/data/com.android.providers.telephony`. This file includes the sender, recipient, read status, pictures, and audio/video files. MMS can be found at `/data/data/com.android.mms`.

### Symbian OS

**Symbian** is a mobile device operating system developed by Nokia and currently maintained by Accenture. Symbian was the most popular mobile operating system as of 2012, although Android was the fastest-growing OS. Symbian OS can be found on Nokia, Sony Ericsson, Samsung, and Hitachi handsets, to name but a few. However, Nokia has been moving away from Symbian OS, in favor of Windows OS. Nokia has transferred support for Symbian OS to Accenture.

### Research in Motion (RIM)

**RIM OS** is the operating system developed by Research in Motion (RIM) for use on BlackBerry smartphones and tablets. Although they are limited, BlackBerry APIs are available to allow for third-party development. The BlackBerry OS is now open source system, however.

Because many organizations issue their employers BlackBerry devices, these smartphones can provide a wealth of evidence. The BlackBerry was developed with corporate productivity in mind, so this device can attain Internet access through a carrier's data plan but can also work in Wi-Fi hotspots. In fact, with BlackBerry 7.1 OS, the device can connect to a hotspot and then become a mobile hotspot for up to five devices. BlackBerry Tablet OS is an operating system developed for the BlackBerry PlayBook tablet computer. Unlike Google's Android OS, which runs on handsets manufactured by a wide variety of providers, RIM OS works only on BlackBerry devices.

It is important for an investigator to understand that, even without access to the BlackBerry handset, the investigator can access a wealth of handset evidence from the computer that a suspect or victim synced to. An IPD Backup File is file backup from a BlackBerry that is found on a synced computer or medium. The files can be recognized by their `.ipd` file extension. More importantly, these IPD files are unencrypted and might be more accessible from a computer than from the device itself (which could be PIN protected).

Many tools available allow an investigator to parse, view, and search through these files. One tool is Elcomsoft Blackberry Backup Explorer. The software works with the IPD files on a Mac or Windows computer and can extract email, SMS, MMS, call logs, Internet activity, appointments, photos, and other user-created files. Elcomsoft also produces a password recovery utility for purchase. Figure 9.14 shows an image of the BlackBerry Curve, which is still a popular smartphone.

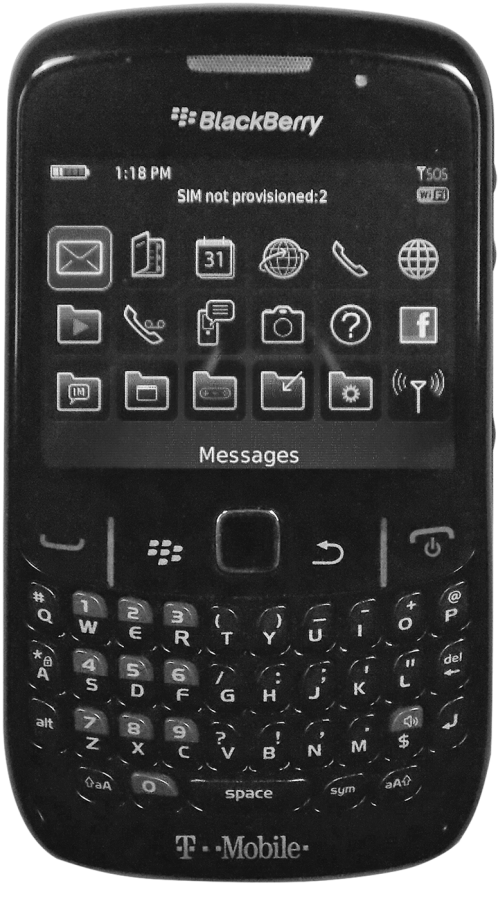



**FIGURE 9.14** BlackBerry Curve

## Windows Phone

**Windows Phone** is a Microsoft operating system that can be found on personal computers, mobile phones, and tablets. It resides on mobile phones manufactured by HTC, Samsung, Nokia, and others. Examining Windows smartphones can be problematic and often requires JTAG to download data from the handset. The good news is that the files downloaded using JTAG are NTFS and do not need to be converted. **Internet Explorer Mobile** is the web browser, based on Internet Explorer 9, found on Windows Phone devices. **People Hub** is an address book tool found on Windows Phone devices that can synchronize contacts from social networking sites like Facebook, Twitter, and LinkedIn. Windows Phone supports POP and IMAP email protocols, including Hotmail, Gmail, and Yahoo! Mail, and can sync contacts and calendars from these services. Zune is the application used for managing multimedia files on Windows Phone devices. As one would expect, .WMV files are supported, but so too are AVI, MP4, MOV, and 3GP/3G2 file formats.

### Windows Phone Applications

**Bing Mobile** is the search engine included with Windows Phone. **Tellme** is a Microsoft tool found on Windows Phone, which is used for voice recognition commands for Bing searches, to call contacts or to activate applications. **Bing Maps** is a vehicle navigation system that comes with Windows Phone.

**Office Hub** coordinates Microsoft Office applications and documents. Microsoft Office Mobile includes Excel Mobile, Word Mobile, PowerPoint Mobile, and SharePoint Workspace Mobile, all of which are compatible with the desktop versions of Microsoft Office.

### Other Mobile Operating Systems

There are some other operating systems that an investigator may encounter. Bada is an operating system that was developed by Samsung Electronics. Handsets that run Bada OS usually have "Wave" in the name. Some mobile phones also run Linux OS. For example, the Nokia N900 smartphone's operating system is Maemo 5, which is Linux based, but it can run full Linux OS. Some people refer to this device as a "hacker phone."

# Standard Operating Procedures for Handling Handset Evidence

Laboratories and their investigators must use best practices for cellphone examinations. Luckily, guidelines are available to use as the basis for the laboratory's standard operating procedures (SOP). An organization's SOP varies from place to place primarily as a result of differences in organizational budgets; this then impacts the resources (equipment, personnel, training, and so on) the lab has available.

When documenting the examination of a cellphone, it is important to document every person who came in contact with the device. For example, some onsite police are instructed to place a handset into

Airplane Mode when it is seized, and that needs to be documented; if the device was dusted for fingerprints before its arrival at the computer forensics lab, that also should be a part of the investigative report.

## National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) provides standard operating procedures for a variety of scientific practices, including cellphone forensics. NIST Special Publication 800-101 Revision 1 (final) issued guidelines on cellphone forensics in 2014. NIST is a well-recognized organization, and computer forensics investigators should be familiar with its guidelines.

Four steps are involved in a forensic examination:

1. Preservation
2. Acquisition
3. Examination and analysis
4. Reporting

### NIST Resources for Tool Validation

The first point to make is that, as with every other forensic tool in a computer forensics lab, all tools should be validated prior to their use in investigations. It is essential to use test data and follow a set of investigative protocols to determine the data that can be extracted. Comparisons also should be made with other cellphone tools. Questions about this validation process may arise during a court trial. Validation also incorporates the use of cryptographic hashes, like MD5 or a SHA1 or a SHA2 hash, to ensure that the results from using a particular tool can be reproduced with the exact same outcome. During the validation process, error rates should be clearly documented.

NIST provides examiners with tremendous resources to assist with testing tools. The Computer Forensic Tool Testing (CFTT) project provides guidelines for testing computer forensics tools, including test criteria, test sets, and test hardware. More information can be found at www.cftt.nist.gov/.

The National Software Reference Library (NSRL) provides guidance on effectively using technology in investigations that require the examination of digital evidence. More information can be found at www.nsrl.nist.gov/.

NIST has provided test datasets of digital evidence. The Computer Forensic Reference Data Sets (CFReDS) for digital evidence are test data that can be used to validate forensic tools, test equipment, and train investigators. More information is available at www.cfreds.nist.gov/.

Computer forensics investigators should also be familiar with the U.S. Department of Justice's NIJ report *Electronic Crime Scene Investigation: A Guide to First Responders*. This is a general guide to computer forensic investigations.

The Association of Chief Police Officers (ACPO) and other standards have noted the importance of making sure evidence is not changed after it is subjected to an examination. According to the ACPO:

> No actions performed by investigators should change data contained on digital devices or storage media that may subsequently be relied upon in court.

With cellphones, a fundamental problem arises when it comes to a forensics. Cellphones generally have small onboard memory capacity, so memory utilization and compression is essential. This, coupled with the fact that these devices are continually connected to a cellular network, means that the data on a cellphone is continually changing. When a computer forensics examiner attempts to extract evidence from a cellphone, changes can be made to the cellphone. What is important to remember is that the user-created data can remain unaltered when using best practices. Therefore, the evidence is admissible when the process is documented appropriately. Some investigators still contend that "cellphone forensics" does not exist and that there are only "cellphone examinations."

## Preparation and Containment

Containing a cellphone should be a careful but expeditious process. According to the U.S. Department of Justice (NIJ) guidelines, in the *Electronic Crime Scene Investigation—A Guide for First Responders* book, investigators should follow these steps:

- **Securing and evaluating the scene**—Steps should be taken to ensure the safety of individuals and to identify and protect the integrity of potential evidence.
- **Documenting the scene**—Investigators should create a permanent record of the scene, accurately recording both digital-related and conventional evidence.
- **Evidence collection**—Traditional and digital evidence should be collected in a manner that preserves its evidentiary value.
- **Packaging, transportation, and storage**—Investigators should take adequate precautions when packaging, transporting, and storing evidence, to maintain the chain of custody.

Therefore, the investigator should first document the crime scene, including making notes and taking photographs. The investigator should then properly contain the cellphone. Proper containment means removing the device from the network. The following containers can be used to remove the device from wireless networks:

- Faraday box
- RF Shield box
- MFI Shielding Cloth (see Figure 9.15)

- Paraben StrongHold bag (see Figure 9.16)
- Arson can

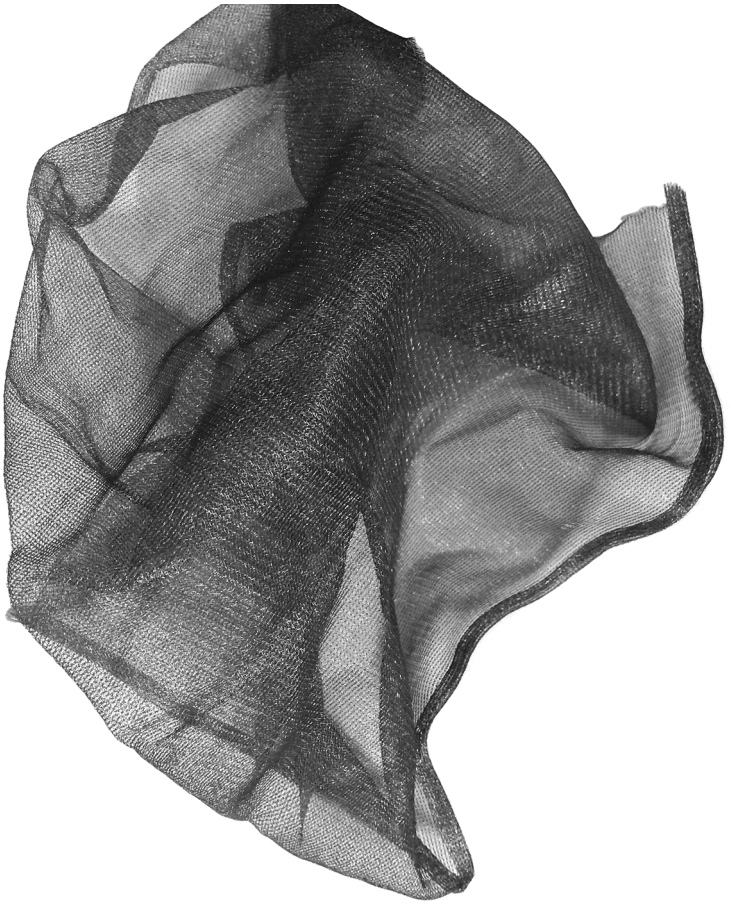


**FIGURE 9.15** MFI Shielding Cloth

A Faraday box can be expensive, whereas an arson can may serve as a cheaper option and still be very effective. An even cheaper alternative is tin foil. Some investigators place a cellphone in a Faraday box but leave a cable hanging out, to continue charging the phone. The problem is that a charging cable can actually work like an aerial. The issue with containment of a cellphone is that the device will boost the signal in an attempt to connect to the cellular network, which drains the battery faster. Smartphones, like the iPhone and Android phones, will require frequent charging because of the number of applications that simply drain the battery faster. Once the phone shuts down, there is the risk of encountering a user's handset PIN or a SIM card PIN (or both).

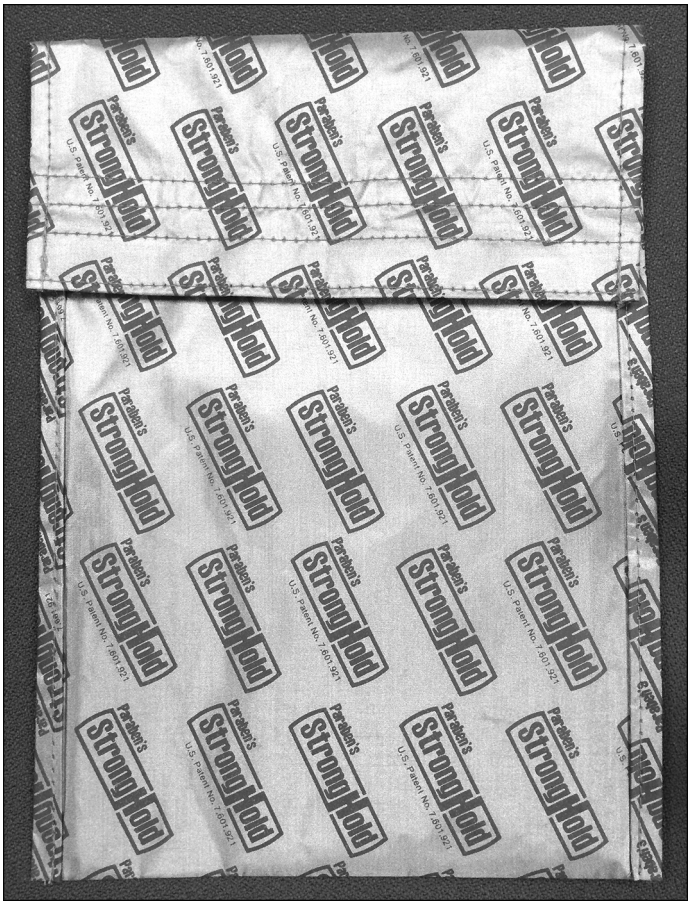



**FIGURE 9.16** Paraben StrongHold bag

### Forensic Shield Box

Concentric Technology Solutions produces a series of RF Shield Boxes for securing cellphones and blocking external signals (ramseyforensicbox.com). These Shielded Test Enclosures not only prevent wireless signals from being received by the device, but also include a power source for the devices housed in the box. The boxes can be padlocked for additional security. The box is also illuminated and fitted with gloves so that the investigator can examine the cellphone in the box. Ports can also be added to the box so that they can be imaged without removing the device. Additionally, investigators can use a feature that allows them to record video and audio of the examination of the device in the box.

## Wireless Capabilities

Today's cellphones have many wireless capabilities. Apart from cellular communications, many cellphones have infrared (IrDA), Wi-Fi, or Bluetooth wireless capabilities built in. This is important to remember when containing a cellphone device.

A cellphone can also be properly contained by doing the following:

- Remove the SIM card (if it has one)
- Change setting to Airplane Mode
- Disable the wireless connection
- Disable the Bluetooth connection

Using the FCC-ID and finding the cellphone's manual can help with finding the wireless capabilities of the device and removing the device from all potential wireless connections.

**Let's Get Practical!**

### Identify the Features of a Cellular Phone

Detailed information about all devices operating on frequencies controlled by the FCC is available online. You will need Adobe Reader installed to complete this practical.

1. Start your web browser and navigate to http://transition.fcc.gov/oet/ea/fccid/.

   Ensure that any Pop-Up Blocker feature on your web browser is disabled.

2. Using your own cellphone, remove the back of the device and then remove the battery so that the FCC-ID on the device is displayed.
3. Enter the FCC-ID in the **Grantee Code** box and in the **Product Code** box, as shown in Figure 9.17.
4. Click the **Search** button.
5. Review the displayed documents, and then document the features of the device, including wireless features and the type of network it operates on (for example, CDMA or GSM).
6. Submit the report as directed by your instructor.


**FIGURE 9.17** FCC-ID lookup page

Some organizations use signal jammers in their computer forensics labs to block all radio transmissions and interference with cellphones. However, the FCC has reiterated that these devices are illegal to use, even for law enforcement, because in an emergency situation, a person in distress might not be able to contact emergency services. A signal jammer can be used if a license is obtained officially from the FCC. For example, a bomb disposal squad might get permission to use a signal jammer to prevent the remote detonation of a bomb; terrorists often use a cellphone to detonate a bomb.

The cellphone carrier can also be contacted to ensure that the phone is removed from the network. Criminals often report a cellphone lost to erase the contents of the cellphone, so moving fast to remove the device from the network rapidly is critical.

### Charging the Device

Keeping a cellphone's battery charged is critical. Smartphones, especially Android and iPhones, have notoriously poor battery life because of the many applications that quickly consume the phone's charge. Given that many smartphones are PIN protected and that containing a phone in a Faraday box will boost the signal and battery usage, finding a charger quickly is vital.

**NOTE**

Never keep a cellphone in a container like a Faraday box with a charging cable sticking out: A charging cable can act as an aerial. Never charge a seized cellphone via a computer, or you are likely to change evidence on the phone.

### Documenting the Investigation

Most forensic tools, like Paraben's Device Seizure AccessData's MPE+, have a built-in report feature. The investigator's report should ultimately include the following details:

Device specifications, including details about the SIM card

- Where the device was seized
- How the device was seized (copies of consent form or warrant)
- Preparation techniques, including removing the device from the network
- Forensic tools used to acquire the evidence
- Evidence acquired (SMS, MMS, images, video, contacts, call history, etc.)
- Carrier evidence (subscriber details and call detail records)
- Application service evidence (e.g. Gmail from Google's e-mail servers)

Naturally, photographs of the location where the device was seized, the device itself and all relevant numbers (ICCID, IMEI, etc.) should be taken.

## Handset Forensics

A SIM card provides a tremendous amount of evidence, as does an SD card. However, examining the onboard memory on the handset itself is equally important. Both software and hardware forensics solutions are available.

### Cellphone Forensic Software

Several innovative software programs can effectively perform cellphone forensics, including these:

- BitPim
- Mobile Phone Examiner (MPE+)
- MOBILedit! Forensic
- Device Seizure
- SIMcon
- XAMN

Each is described in greater detail here.

### BitPim

BitPim is an open source tool that allows you to view and manipulate files on a many CDMA phones. Mobile phones supported by BitPim include Samsung, LG, Sanyo, and many other cellphones that contain Qualcomm CDMA chipsets. The software can be downloaded for free from www.bitpim.org.

### Mobile Phone Examiner (MPE+)

This tool enables the investigator to examine a wide range of cellular handsets and SIM (or USIM) cards. The tool enables the examiner to carve data. In other words, it separates images and video and audio files that are embedded in MMS files. MPE+ enables the user to enter a PIN for PIN-protected handsets and SIM cards. Moreover, the tool enables the user to enter a PUK code to bypass the PIN on a SIM card.

The files acquired by MPE+ can be exported as a PDF or exported in Microsoft Excel (CSV file). Image files of the handset or SIM card are in an AD1 format, which can be opened in either MPE+ or AccessData's FTK.

An academic version of MPE+ comes with instructor and student manuals, the software, and mobile phone files for practical classroom labs.

### MOBILedit! Forensic

MOBILedit is an organizational tool for a smartphone user's contacts, messages, media, and other files that is installed on the user's computer. A forensic edition can be used to extract cellphone files and generate investigation reports.

### Device Seizure

Developed and distributed by Paraben Corporation, Device Seizure is well known by mobile forensic examiners because the software supports more devices than many software tools. The tool's capabilities include mobile phones, tablets, iPhones, PDAs, and GPS devices. Figure 9.18 displays Device Seizure's user interface.

Paraben also supplies device containment supplies, such as its StrongHold Bag, StrongHold Box (Faraday box), and Project-A-Phone for manual examinations.

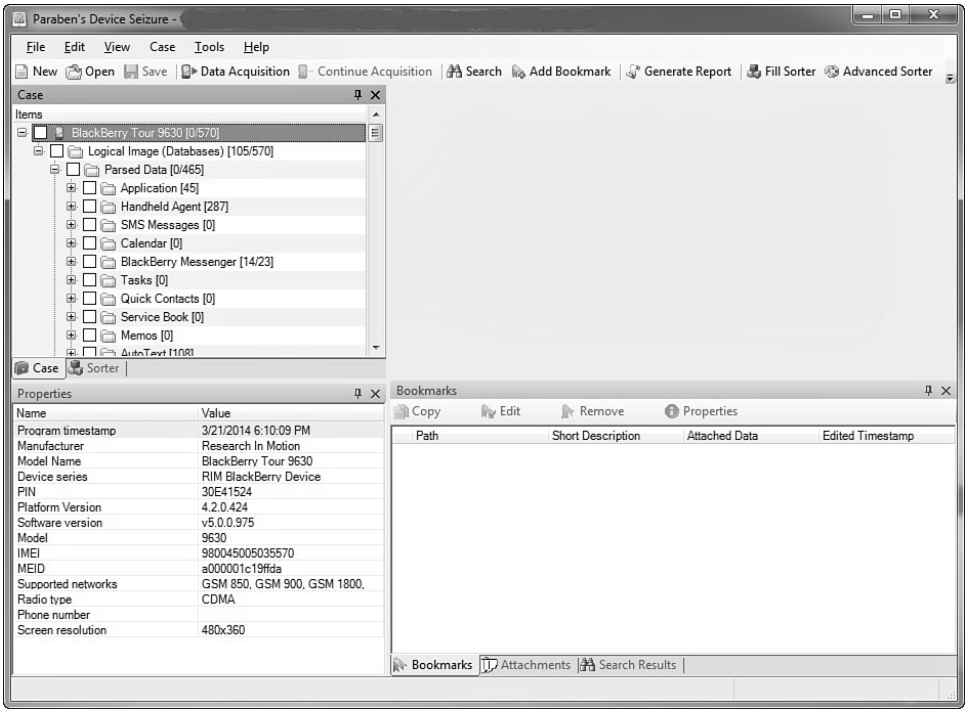



**FIGURE 9.18** Device Seizure user interface

### SIMcon

SIMcon is an application that works with a SIM card reader to recover deleted messages, contacts, call logs, and other user files. Similar to other cellphone forensic tools, it does produce MD5 and SHA-1 hash values of evidence. Although the tool works only with SIM cards, it is a low-cost forensic tool used by many in law enforcement.

### XAMN

Micro Systemation produces software and a hardware field kit for forensics examiners. The company also provides a helpful link analysis tool that some other vendors provide. XAMN is a link analysis tool. Link analysis allows an investigator to add the images from multiple smartphones and quickly identify commonalities between the phones, including contacts. Link analysis can detail accomplices or victims that suspects may have in common. The tool can also map out where a suspect or victim was traveling, based on cellular tower, Wi-Fi hotspot, or photo geotag data. In addition, XAMN has a timeline and calendar function. As you can imagine, a tool that graphically represents how suspects are linked through data retrieved from their cellphones and maps out where they have been not only saves time, but also can be invaluable to determine what transpired when a crime was committed.

**NOTE**

Other reputable cellphone forensic tools are available, all with their unique strengths and features:

- BKForensics: Cell Phone Analyzer
- Katana Forensics: Lantern
- Oxygen: Oxygen Forensic Suite
- CDMA SoftWare: CDMAWorkshop
- Motorola-Tools.com: Flash&Backup
- MediaFire: Nokia Flash Tool
- Susteen: Secure-View

## Cellphone Forensics Hardware

Investigators have numerous software solutions for imaging cellphones and tablets, but they also can use hardware devices for this. Some of these hardware devices are helpful when examining cellphones in the field because they can be charged and have write-blocking capabilities built in.

### CellDEK

CellDEK is a mobile forensics hardware device manufactured by Logicube. The CellDEK is a device that can be used in the field for imaging mobile phones and navigation systems, like Garmin and TomTom. The device supports iOS devices, like the iTouch and iPhone and numerous smartphones.

### Cellebrite

Cellebrite's Universal Forensics Extraction Device (UFED) is a hardware device that can be used for logical and physical extractions from cellphones and GPS devices. UFED is very well regarded in the industry, and many law enforcement computer forensics laboratories have the device. Part of UFED's success stems from the wide range of phones supported by Cellebrite, including iOS, Android, and RIM devices. The UFED Touch can be used in a laboratory or in the field, which appeals to law enforcement. Figure 9.19 shows a UFED Touch.


**FIGURE 9.19** UFED Touch from Cellebrite

### Logical versus Physical Examination

Mobile forensic tools provide a logical or physical extraction of evidence from a cellphone—or sometimes both. Similar to examining a personal computer, a logical examination of a cellphone provides a traditional view of the directories, files, and folders, and it can be compared to the interface we see with Windows File Explorer on a PC or Finder on a Mac. The physical view refers to the actual location and size of files in memory. Only a physical examination can retrieve deleted messages and other deleted files.

A major difference with computer forensics and mobile forensics is that, with a physical view of files on a computer, we can find file fragments. However, when an SMS text message is deleted, you can typically be certain that the message has been removed and no message fragments exist. A physical extraction can resurrect some deleted files, however.

## Manual Cellphone Examinations

In the absence of a mobile forensic imaging tool, the investigator is forced to manually examine the cellphone. This happens frequently, especially with lower-end prepaid phones offered by companies, like TracFone. Tools for these phones are generally nonexistent. This is especially a problem when there is no data port on the handset. Sometimes data can be downloaded from the device through Bluetooth. When traditional imaging is not an option, the investigator acts as a "field jockey" and

thumbs through the phone's contents, taking photos along the way. Project-a-Phone and Fernico ZRT are two tools designed for photographing cellphone screens, although using a regular digital camera can suffice. Documenting the process in detail is critical nevertheless. The reason for using a solution, like Project-a-Phone (see Figure 9.20) is that the tool comes with a reporting tool to make the process easier.

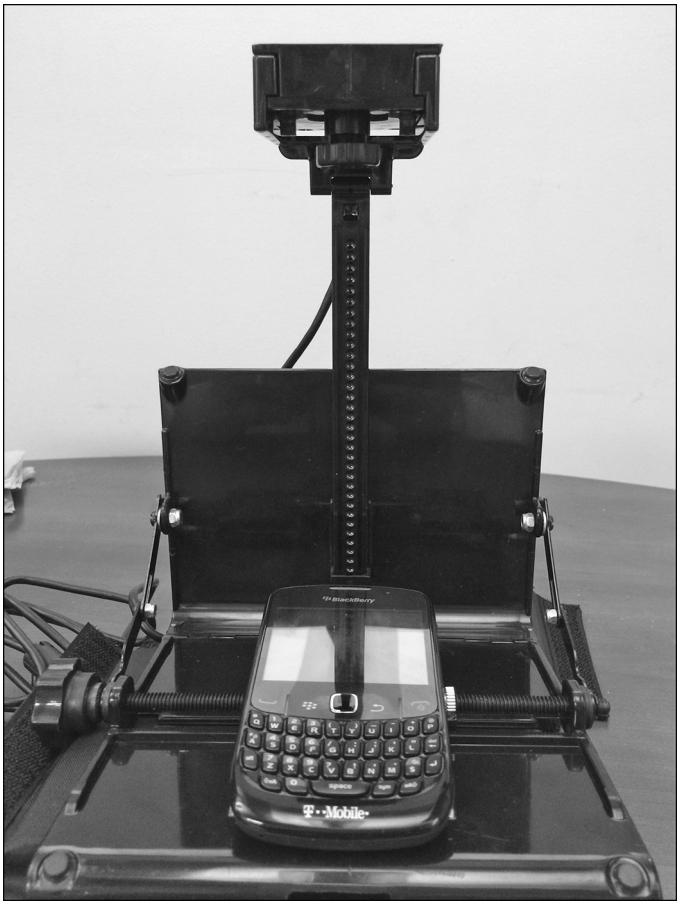



**FIGURE 9.20** Project-a-Phone

## Flasher Box

In the absence of a cellphone forensic imaging solution, one might expect to perform a manual examination using Project-A-Phone or a similar device. Consider what happens when an examiner cannot bypass the cellphone's PIN or if the phone is damaged. As a last resort, some investigators will use a flasher box. A **flasher box** is a device used to make a physical dump of a cellphone.

There are disadvantages, though, to using a flasher box. Using the device may change the data on the cellphone. Additionally, an examiner using such a device should have proper training. The device does not create a helpful MD5 hash for you. Nevertheless, NIJ and ACPO discuss the use of flasher boxes in their standard operating procedures. Moreover, flasher boxes were initially a solution before advanced cellphone forensic tools became available.

# Global Satellite Service Providers

Wireless telephones do not always operate on a cellular network. In fact, most of the world's surface area does not have cellular service. Thus, a ship in the middle of the ocean or an expedition to the Antarctic cannot rely on a local cell site to route calls. Instead, these telephones communicate with other telephones through satellites. Emergency personnel can also use these telephones during a crisis situation, like an earthquake.

## Satellite Communication Services

Iridium Communications maintains a group of 66 satellites called the Iridium Satellite Constellation. These satellites operate in a low orbit approximately 485 miles into the Earth's atmosphere. The company also provides global satellite phones that go beyond traditional terrestrial cellphones. These cellphones can provide direct communications via satellite linkages in areas without cell site coverage, such as in the middle of the Atlantic Ocean or in the Arctic. Globestar is a similar satellite phone provider. SkyWave Mobile Communications provides satellite and General Packet Radio Service for transportation, mining (oil and gas), heavy equipment, and utility companies.

Inmarsat PLC, a British satellite company, provides similar phone service through 11 geostationary telecommunications satellites. The company provides Global Maritime Distress & Safety Services (GMDSS).

# Legal Considerations

As noted in Chapter 7, "Admissibility of Digital Evidence," under the Fourth Amendment, a government agent must obtain a warrant to conduct a search. This is true in the case of cellphones. However, there are exceptions to this rule, including consent, incident to arrest, or exigent circumstances. Exigent circumstances imply that a warrantless search was required to save a life (for example, in the case of a kidnapping).

When applying for a search warrant, the investigator should describe the cellphone and include the following details:

- Make
- Model

- Serial number (if available)
- Manufacturer
- Telephone number
- Location of the device (address and specific location)

If available, the investigator should also include the IMEI or MEID of the phone. In addition, the investigator should detail the type of evidence he or she wants to acquire (SMS, MMS, contacts, and so forth).

### Carrier Records

The investigator can also obtain corroborating evidence from the cellular carrier, in the form of subscriber records and call detail records. The carrier uses subscriber records for billing, and the call detail records provide information about the location and time a cellphone was used to make calls. Remember, a call can be traced to multiple cell sites and can identify a route taken by the suspect. Call detail records identify the location of the handset at a particular location; it is up to the investigator to link the suspect to that handset. When obtaining call detail records, the investigator should request the data in a particular format (such as CSV) and also request information about how to interpret cell site codes that are provided. The carrier can send the investigator a voicemail reset code when requested.

## Other Mobile Devices

Numerous other devices can be of evidentiary value to investigations. These devices include tablets, GPS devices, and personal media devices.

### Tablets

As with cellphones, many different types of tablets are on the market. The software and operating systems running on these devices are very similar. iOS and Android are the most widely found operating systems running on tablets. Some tablets also come with a data plan that runs on a cellular network. Computer forensic tools like Device Seizure, Cellebrite, and BlackLight support a number of tablets. Figure 9.21 shows Amazon's Kindle, which runs on Android OS.

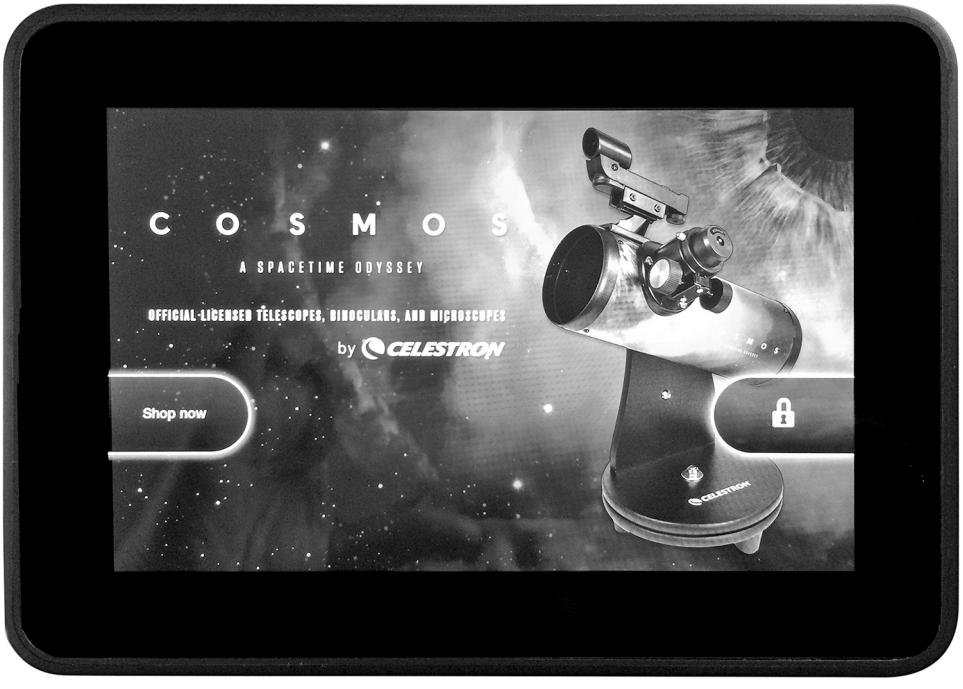



**FIGURE 9.21** Amazon Kindle

## GPS Devices

GPS devices can be used for maritime navigation, driving, and aviation. Handheld devices are used for recreation, like biking and hiking, or can be used by emergency services during disasters. Many of these devices, like TomTom, can be imaged by forensic tools like Cellebrite and Paraben's Device Seizure. Many of these devices come with an SD card, which can be valuable to an investigator. An investigator may also find evidence on a user's synced computer.

Four primary sources of evidence are available from a GPS device: trackpoints, track log, waypoint, and route. More recent GPS devices also contain data about cellphones that were connected via Bluetooth or even Internet searches. Motonav is one example of the expanded services now available. Devices like Motonav, may possess data from the synced cellphone like the user contacts. General Motors (GM) OnStar service is another potential source of data for investigators. GM stores GPS data from vehicles with the built-in OnStar service. GM's monitoring has sparked controversy because the company can disclose this information to third parties, even after the subscriber has terminated services. The TomTom satnav navigation system also caused controversy when it was discovered that the company was sending historical driver GPS routing data to police in the Netherlands. The user data from the TomTom helped police set up speed traps, based on driver habits.

A **trackpoint** is a geo-locational record that is automatically captured and stored by a GPS device. Trackpoints are not created by the user. For example, when a GPS device is turned on, a trackpoint,

recording the current location is made, and then subsequent trackpoints are created at predetermined intervals. A **track log** is a list of trackpoints that can be used to re-create a route.

A **waypoint** is a geo-locational point of interest created by a user. Waypoints are often created to note places of interest, like a restaurant or a hotel, as part of a longer route. Finally, a **route** is a series of user-created waypoints on a trip.

### GPS Tracking

Since 2009, all cellphones are federally mandated to have a GPS chip embedded in the device. In 2003, the U.S. Federal Communications Commission's E-911 Mandate was introduced. **Enhanced 911** is a federal mandate that stipulates that all handset manufacturers must ensure that caller ID and locational data can be obtained from a cellphone subscriber making a 911 call. Therefore, the police can locate a person in distress using **Assisted GPS**, which uses the GPS chip in your cellphone and triangulation rather than simply relying on cell site data. Interestingly, the infamous hacker Kevin Mitnick eluded law enforcement for many years, yet it was his cellphone that led the FBI to discover his whereabouts using triangulation. A **Public Safety Access Point (PSAP)** is a call center that receives emergency requests from the public for police, medical, or firefighter services.

Case Study

#### To Catch a Murderer: A Case Study

A Public Safety Access Point can assist police by tracking a subscriber's cellphone in real time. In October 2004, Fred Jablin was found dead in his home on Hearthglow Lane in Richmond, Virginia. Detective Coby Kelley quickly suspected Jablin's ex-wife, Piper Rountree, and quickly obtained a warrant for Rountree's cellphone records. Fred Jablin, distinguished chair at the University of Richmond, had suffered a very nasty divorce and custody battle with Rountree, and Jablin had won sole custody. By September 2004, Rountree was in trouble: She owed $10,000 in back alimony.

Detective Kelley obtained the cellphone records for Piper Rountree's cellphone, which placed the phone at the scene of the crime. Kelley tracked the cellphone going east on I-64 toward Norfolk Airport. A brief interruption in signal location occurred before the phone could be tracked again in Baltimore, Maryland. Of course, Rountree stated that she had not been in Virginia at the time of the murder, but was actually in Houston, Texas. She also stated that her sister, Tina Rountree, often used her cellphone.

Piper Rountree called her son 14 hours prior to the murder and mentioned that she was in Texas, although her cellphone was pinging towers in Virginia. On October 21 (a few days prior to the murder), Rountree purchased a wig on the Internet, using her own account, but the wig was delivered to her former boyfriend's P.O. Box in Houston. Piper Rountree was attempting to use the wig to pose as her sister, Tina. A Southwest Airlines employee later testified that he had witnessed Piper Rountree boarding a plane to Virginia. On May 6, 2005, Piper Roundtree was sentenced to life in prison plus three years for use of a firearm in a crime. This case clearly illustrates how important cellphone evidence was in corroborating evidence used at trial.

# Summary

Mobile forensics has become extremely important for investigations because of the wealth of evidence it can provide. This type of information can even be more important than the evidence gleaned from a traditional computer because cellphones are always on and we carry them everywhere. Forensic tools have improved over the past five years, but we still have many devices that are not supported. With the growing importance of cellphone forensics, investigators are reaching out beyond the cellphone to the cellular carrier and cloud computing service providers.

Cellphones are problematic to analyze because so many different operating systems and device models are available, and the data on these devices continually changes because of network connections and their small onboard memory. The contents of a smartphone cannot be analyzed as one mass media device because of removable memory and SIM cards (GSM phones).

A variety of cellular networks exist, with GSM and CDMA being the predominant network protocols. Understanding these networks helps investigators understand where the evidence is located. Mobile Network Operators, like Sprint and Verizon, own and operate networks; a Mobile Virtual Network Operator provides service but does not own the cellular network infrastructure.

Other mobile devices, like tablets and GPS electronics, also are important to investigators. A tablet can have Internet service through a cellular network. Broadband USB and Mi-Fi cards also use cellular networks.

Investigators should always test forensic tools prior to their use. Many cellphones are not supported by forensic tools, so a manual investigation must be conducted. Investigators should also be aware of NIST, NIJ, and ACPO standard operating procedures for investigating digital devices. Proper care should be afforded when containing the device, charging the device, and ensuring isolation from a variety of wireless networks.

## KEY TERMS

**3GP:** An audio/video file format found on mobile phones operating on 3G GSM cellular networks.

**3GP2:** An audio/video file format found on mobile phones operating on 3G CDMA cellular networks.

**3rd Generation Partnership Project (3GPP):** A collaboration of six telecommunications standards bodies and a large number of telecommunications corporations worldwide that provides telecommunication standards.

**3rd Generation Partnership Project 2 (3GPP2):** A partnership of North American and Asian 3G telecommunications companies that develop standards for third-generation mobile networks, including CDMA.

**4G Long Term Evolution (LTE) Advanced:** A high-mobility broadband communication that is suitable for use on trains and in other vehicles.

**abbreviated dialing numbers (ADN):** Contains the contact names and numbers entered by the subscriber.

**accelerometer:** A hardware device that senses motion or gravity and reacts to these changes.

**Android:** An open source operating system based on the Linux 2.6 kernel.

**Assisted GPS:** Uses the GPS chip in your cellphone and triangulation simply relying on cell site data.

**Authentication Center (AuC):** A database that contains the subscriber's IMSI, authentication, and encryption algorithms.

**base station controller (BSC):** Manages the radio signals for base transceiver stations, assigning frequencies and handoffs between cell sites.

**base transceiver station (BTS):** The equipment found at a cell site that facilitates the communication of a cellphone user across a cellular network.

**Bing Maps:** A vehicle navigation system that comes with Windows Phone.

**Bing Mobile:** The search engine included with Windows Phone.

**call detail records (CDR):** Details used for billing purposes; these can include phone numbers called, duration of calls, dates and times of calls, and cell sites used.

**CDMA2000:** A 3G technology that uses the CDMA communications protocol.

**cell:** A geographic area within a cellular network.

**cell site:** A cell tower located in a cell.

**cellular network:** A group of cells.

**Code Division Multiple Access (CDMA):** A spread-spectrum communication methodology that uses a wide bandwidth for transmitting data.

**Electronic Serial Number (ESN):** An 11-digit number used to identify a subscriber on a CDMA cellular network.

**Enhanced 911:** A federal mandate that stipulates that all handset manufacturers must ensure that caller ID and locational data can be obtained from a cellphone subscriber making a 911 call.

**Enhanced Data rates for GSM Evolution (EDGE):** A high-data-transfer technology found on GSM networks. EDGE provides up to three times the data capacity of GPRS.

**Equipment Identity Register (EIR):** Used to track IMEI numbers and decide whether an IMEI is valid, suspect, or perhaps stolen.

**FCC-ID:** A number issued by the Federal Communication Commission (FCC) that indicates the handset is authorized to operate on radio frequencies within the FCC's control.

**flasher box:** A device used to make a physical dump of a cellphone.

**Forbidden Public Land Mobile Network (FPLMN):** Cellular networks that a subscriber attempted to connect to but was not authorized for.

**General Packet Radio Service (GPRS):** Packet-switching wireless communication found on 2G and 3G GSM networks.

**Global System for Mobile Communications (GSM):** An international standard for signal communications that uses TDMA and Frequency Division Duplex communication methods.

**hard handoff:** Communication handled by one only base transceiver station at a time, with no simultaneous communication.

**Home Locator Register (HLR):** A database of a carrier's subscribers, including their home addresses, IMSI, telephone numbers, SIM card ICCIDs, and services used.

**Integrated Circuit Card ID (ICCID):** Usually, a 19-digit serial number physically located on the SIM card.

**Integrated Digital Enhanced Network (iDEN):** A wireless technology developed by Motorola that combines two-way radio capabilities with digital cellphone technology.

**International Mobile Equipment Identity (IMEI):** Number that uniquely identifies the mobile equipment or handset.

**International Mobile Subscriber Identity (IMSI):** An internationally unique number on the SIM card that identifies a user on a network.

**International Signaling Point Code (ISPC):** A standardized numbering system used to identify a node on an international telecommunications network.

**International Telecommunication Union (ITU):** An agency of the United Nations that produces standards for information and communication technologies.

**Internet Explorer Mobile:** The web browser, based on Internet Explorer 9, found on Windows Phone devices.

**IPD Backup File:** A file backup from a BlackBerry that is found on a synced computer or medium.

**Joint Test Action Group (JTAG):** An IEEE standard (IEEE 1149.1) for testing, maintenance, and support of assembled circuit boards.

**Last Numbers Dialed (LND):** A list of all outgoing calls made by the subscriber.

**Mobile Country Code (MCC):** The first three digits of the IMSI.

**Mobile Equipment Identifier (MEID):** An internationally unique number that identifies a CDMA handset (Mobile Equipment).

**Mobile Network Operator (MNO):** Owns and operates a cellular network.

**Mobile Station:** Consists of Mobile Equipment (handset) and a Subscriber Identity Module (SIM).

**Mobile Subscriber Identity Number (MSIN):** Created by a cellular telephone carrier, and identifies the subscriber on the network.

**Mobile Subscriber ISDN (MSISDN):** Essentially, the phone number for the subscriber.

**Mobile Switching Center (MSC):** Responsible for switching data packets from one network path to another on a cellular network.

**Mobile Virtual Network Operator (MVNO):** Does not own its own cellular network, but operates on the network of a Mobile Network Operator.

**Multimedia Messaging Service (MMS):** A messaging service found on most cellphones that allows the user to send multimedia content such as audio, video, and images.

**multiplexing:** Multiple signals transmitted simultaneously across a shared medium.

**My Wireless Fidelity (Mi-Fi):** A portable wireless router that provides Internet access for up to five Internet-enabled devices and communicates via a cellular network.

**Office hub:** Coordinates Microsoft Office applications and documents.

**People Hub:** An address book tool found on Windows Phone devices that has the ability to synchronize contacts from social networking sites like Facebook, Twitter, and LinkedIn.

**PIN Unlock Key (PUK):** An unlock reset code used to bypass the SIM PIN protection.

**Public Safety Access Point (PSAP):** A call center that receives emergency requests from the public for police, medical, or firefighter services.

**Public Switched Telephone Network (PSTN):** An aggregate of all circuit-switched telephone networks.

**RIM OS:** Operating system developed by Research in Motion for use on BlackBerry smartphones and tablets.

**Route:** A series of user-created waypoints on a trip.

**Short Message Service (SMS):** A text message communication service found on mobile devices.

**SIM card:** Identifies a user on a cellular network and contains an IMSI.

**soft handoff:** Cellular communication conditionally handed off from one base station to another, with the mobile equipment simultaneously communicating with multiple base transceiver stations.

**SQLite database:** An open source relational database standard that is frequently found on mobile devices.

**subscriber records:** Personal details maintained by the carrier about its customers, including their names, addresses, alternative phone numbers, Social Security numbers, and credit card information.

**subsidy lock:** Confines a subscriber to a certain cellular network so that a cellphone can be sold for free or at a subsidized price.

**Symbian:** A mobile device operating system developed by Nokia and currently maintained by Accenture.

**Tellme:** A Microsoft tool found on Windows Phone that is used for voice recognition commands for Bing searches, to call contacts or to activate applications.

**Temporary Mobile Subscriber Identity (TMSI):** A randomly generated number that the VLR assigns to a mobile station when the handset is switched, based on the geographic location.

**Time Division Multiple Access (TDMA):** A radio communication methodology that enables devices to communicate on the same frequency by splitting digital signals into time slots, or bursts.

**track log:** A list of trackpoints that can be used to re-create a route.

**trackpoint:** A geolocational record that is automatically captured and stored by a GPS device.

**Type Allocation Code (TAC):** Identifies the type of wireless device.

**Universal Integrated Circuit Card (UICC):** A smart card used to uniquely identify a subscriber on a GSM or UMTS network.

**Universal Mobile Telecommunications System (UMTS):** A 3G cellular network standard based on GSM and developed by 3GPP.

**Visitor Locator Register (VLR):** A database of information about a roaming subscriber.

**waypoint:** A geolocational point of interest created by a user.

**Wide Band CDMA (WCDMA):** A high-speed signal transmission method based on CDMA and FDD methods.

**Windows Phone:** A Microsoft operating system that can be found on personal computers, mobile phones, and tablets.

## Assessment

### CLASSROOM DISCUSSIONS

1. You have just received a mobile device with an FCC-ID of BEJVM670. You have been told that the cellphone has an MEID. Using this information, answer the following questions:
   - **A.** What U.S. cellular carrier(s) could be providing service for the cellphone?
   - **B.** Does this cellphone have Bluetooth?
   - **C.** Could this cellphone have been used to take photographs? If so, could the photos have GPS data associated with them?
   - **D.** Where on this device could there be potential evidence? For example, in addition to the handset, is there a SIM or SD card?

2. Detail best practices for containing and analyzing a cellular telephone.
3. In what ways could the cellphone carrier assist you in your investigation?
4. Describe how cellphone forensics differs from traditional computer forensics.

## MULTIPLE-CHOICE QUESTIONS

1. The equipment found at a cell site that facilitates the communication of a cellphone user across a cellular network is best described as which of the following?
   - A. Cellular network
   - B. Base Transceiver Station
   - C. Public Switched Telephone Network
   - D. Home Locator Register
2. Which of the following best describes the role of the Base Station Controller?
   - A. Manages the radio signals for Base Transceiver Stations.
   - B. Assigns frequencies and handoffs between cell sites.
   - C. Both A and B are correct.
   - D. Neither A or B is correct.
3. Which of the following are details used by telecommunications carriers for billing purposes and can include phone numbers called, duration of calls, dates and times of calls, and cell sites used?
   - A. Equipment Identity Register
   - B. Mobile Network Operator
   - C. Temporary Mobile Subscriber Identity
   - D. Call detail records
4. Which of the following typically is not be found on a GSM cellphone?
   - A. SIM
   - B. IMEI
   - C. FCC-ID
   - D. MEID
5. The first three digits of the IMSI are referred to as which of the following?
   - A. Mobile Country Code
   - B. Mobile Subscriber Identity Number
   - C. Mobile Network Operator
   - D. Integrated Circuit Card ID

6. Which of the following is a portable wireless router that provides Internet access for up to five Internet-enabled devices and communicates via a cellular network?

   **A.** Office hub
   **B.** Public Safety Access Point
   **C.** Mobile station
   **D.** Mi-Fi

7. Which of the following is a high-mobility broadband communication that is suitable for use on trains and in other vehicles?

   **A.** 2G
   **B.** 3G
   **C.** 3GPP
   **D.** 4G LTE

8. Which of the following is an international standard for signal communications that uses TDMA and FDD (Frequency Division Duplex) communication methods?

   **A.** GSM
   **B.** CDMA
   **C.** UMTS
   **D.** WCDMA

9. Which one of the following directories contains a list of contacts (names and telephone numbers) saved by a subscriber on a SIM card?

   **A.** EF_SMS
   **B.** EF_LOCI
   **C.** EF_LND
   **D.** EF_ADN

10. Which of the following mobile operating systems is an open source operating system based on the Linux 2.6 kernel and is owned by Google?

    **A.** Symbian
    **B.** Android
    **C.** RIM
    **D.** Windows

## FILL IN THE BLANKS

1. A(n) _____ is the geographic area within a cellular network.
2. A Mobile _____ Center is responsible for switching data packets from one network path to another on a cellular network.
3. A(n) _____ handoff occurs when a cellular communication is conditionally handed off from one base station to another and the mobile equipment is simultaneously communicating with multiple Base Transceiver Stations.
4. A(n) _____ Mobile Equipment Identity number uniquely identifies the Mobile Equipment or handset.
5. The database that contains information about a roaming subscriber is referred to as a(n) _____ Locator Register.
6. The _____ Identity Register is used to track IMEI numbers and decide whether an IMEI is valid, suspect, or perhaps stolen.
7. Integrated _____ Enhanced Network is a wireless technology developed by Motorola that combines two-way radio capabilities with digital cellphone technology.
8. _____ Public Land Mobile Network refers to cellular networks that a subscriber attempted to connect to but was not authorized for.
9. A Personal Unlock _____ (PUK) is a code that is available from the carrier and allows a user to remove the PIN protection from the SIM card.
10. A Public Safety _____ Point is a call center that receives emergency requests from the public for police, medical, or firefighter services.

## PROJECTS

### Write an Essay about Cellphone Forensics

Find an example of cellphone forensics used in a criminal investigation, and write an essay about its importance in successfully convicting a suspect.

### Write Standard Operating Procedures for Examining a Cellphone

Find a smartphone and then write standard operating procedures for examining that cellphone. Include in your essay forensic tools that will work with that particular model.

### Describe a Forensic Examiner's Guide to Working with a Mobile Operating System

Select a mobile operating system and then describe a forensic examiner's guide to working with that operating system.

### Write an Essay Describing the Differences in Examining Two Different Cellphones

Write an essay describing the differences from an examination of a CDMA cellphone and a GSM cellphone.

# Index

## Numerics



## A

# B

# C

# D

# E

# F

# G

# H

# I

## J



## K



## L

# M

# N

## O

# P

# Q



# R

# S

# T

# U

# V

# W



# X

# Y



# Z