CHAPTER 20

Digital Evidence on Mobile Devices

Eoghan Casey and Benjamin Turnbull

CONTENTS

Mobile devices such as cell phones and smart phones have become an integral part of peoples' daily lives, and as such, they are prone to facilitating criminal activity or otherwise being involved when crimes occur. No other computing device is as personal as the mobile phone, effectively providing a computer in a pocket. Whereas computers, laptops, servers, and game machines might have many users, in the vast majority of cases, mobile devices generally belong to an individual.

Although compact, these handheld devices can contain personal information including call history, text messages, e-mails, digital photographs, videos, calendar items, memos, address books, passwords, and credit card numbers. These devices can be used to communicate, exchange photographs, connect to social networks, blog, take notes, record and consume video and audio, sketch, access the Internet, and much more. As the technology develops, higher data transmission rates are allowing individuals to transfer more data (e.g., digital video), and the computing power in these devices enables us to use them in much the same way as we used laptop systems over the past decade. Because these devices fit in a pocket or bag, they are often carried wherever a person goes and can be used to determine a person's whereabouts at a particular time. This rapid development of mobile computing and communication technology creates opportunities for criminals and investigators alike.

The information stored on and associated with mobile devices can help address the crucial questions in an investigation, revealing whom an individual has been in contact with, what they have been communicating about, and where they have been. Sexual predators can use a mobile device to make initial contact with victims, exchange photographs or videos, and groom victims, creating a vivid cybertrail for digital investigators to follow. Mobile devices have been instrumental in solving homicides, are used by terrorists for reconnaissance and coordination, can be used to smuggle contraband across borders, and are frequently found in prisons despite being prohibited. Members of major criminal organizations and gangs use mobile devices to coordinate activities

Digital Evidence and Computer Crime, Third Edition

and share information, even when they are in prison, and digital investigators can gain significant insights into these groups using information from their mobile devices. Information on mobile devices can also be of use in serious crimes when a person of interest may not realize that they are carrying a mobile device or not thinking of it as a source of incriminating digital evidence.

CASE EXAMPLE: POCKET-DIAL M FOR MURDER

Ronald Williams killed his wife Mariama, apparently in a fit of rage after learning that she had an affair. Unbeknownst to Williams, his cell phone pocket-dialed his wife's cell phone during the crime and the call went to voicemail. The recording on his wife's voicemail captured him stating that he was going to kill her, followed by her screams and their 2-year-old daughter pleading with Williams to stop (Krueger, 2011).

The increasing computational power of mobile devices has afforded even greater uses, and with that, greater potential for misuse. For instance, some mobile devices are optimized for data acquisition such as credit card scanning and scientific measurements (e.g., voltage, temperature, acceleration). This flexibility has ramifications beyond the manufacturer's intentions, and mobile devices have been used to steal credit cards and trigger bombs (van der Knijff, 2009; Wilson, 2006).

This chapter demonstrates how mobile devices can be useful as sources of digital evidence, describes the basic operation of mobile devices, and presents tools and techniques for acquiring and examining digital evidence on these devices. Notably, mobile devices are just one type of embedded system and there are advanced approaches to extracting information from such devices, including JTAG access and chip-off extraction. A more in-depth treatment of embedded systems, including GSM mobile telephones, is provided in the *Handbook of Digital Forensics and Investigation* (Van der Knijff, 2009) and the cmdLabs Web site (http://www.cmdlabs.com).

20.1 MOBILE DEVICE FORENSICS

Mobile devices are dynamic systems that present challenges from a forensic perspective. Additionally, new models of phones are being developed globally, with some experts postulating that five new phone models are released every week (Jones, 2008). The growing number and variety of mobile devices makes it difficult to develop a single process or tool to address all eventualities. In addition to a growing variety of smart phones and platforms including Android systems, Blackberry, Apple iPhone, and Windows Mobile, there are a massive number of low-end phones using legacy OS systems.

Furthermore, there are some unique considerations when preserving mobile devices as a source of evidence. Most mobile devices are networked devices, sending and receiving data through telecommunication systems, WiFi access points, and Bluetooth piconets. Digital evidence in mobile devices can be lost completely as it is susceptible to being overwritten by new data or remote destruction commands it receives over wireless networks. Additionally, in order to extract information, it is necessary to interact with the device, often altering the system's state. As with any computer, interacting with a mobile device can destroy or alter existing evidence. Fortunately, by following the processes outlined in Chapters 3 and 6, it is possible to obtain usable digital evidence from mobile devices in a forensically sound manner acceptable to a court of law.

Mobile devices are challenging from a data recovery and analysis standpoint as well. With their increasing functionality and growing data stores, mobile devices are becoming analogous to computers with specific functions (mainly as a conduit for communications and Internet access). Keeping up with all of the various file systems, data formats, and data sources on mobile devices is an ongoing challenge.

However, a major advantage of mobile devices from a forensic perspective is that they can contain deleted information even after an individual has attempted to render it unrecoverable. The underlying reason for this persistence of deleted data on mobile devices is in the use of Flash memory chips to store data. Flash memory is physically durable against impact, high temperature, and pressure, making it more difficult to destroy. In addition, Flash memory has a limited number of writes and can only be erased block-by-block, and mobile devices generally wait until a block is full before erasing data. Furthermore, mobile devices use proprietary wear leveling algorithms to spread write/erase across Flash memory blocks, which can result in deleted data remaining for some time while new data are written to less used portions of memory. In order to access and recover older/deleted copies of data, it is necessary to acquire a full copy of physical memory as covered later in this chapter.

For all the collection, extraction, and analysis issues mobile devices present, they are an excellent source of digital evidence and can provide insight unavailable from other devices. Additionally, the personal nature of the device makes it easy to establish the last mile evidence required to tie a device to an individual.

20.1.1 Fundamentals of Mobile Device Technology

Mobile devices are simple computers with a CPU, memory, batteries, input interfaces such as a keypad or mouthpiece, and output interfaces such as a screen or earpiece. Data in memory are generally the focus of a forensic examination, but some understanding of the input and output components is needed to access these data. In some instances, it may be sufficient manually to operate a device and read information from the display. However, to recover deleted data or perform more advanced examination, specially designed tools are needed to interface with the device. In some situations, it is sufficient to acquire specific information of interest from a mobile device via a cable connected to the data port, but in other circumstances it is necessary to attach a specialized connector directly to the circuit board in order to acquire all of the information needed in a case. Knowledge of how data are manipulated and stored on handheld devices is sometimes needed to acquire all available digital evidence from handheld devices without altering it and translate it into a human readable form. For instance, placing a mobile device on a cradle and synchronizing it with a computer to obtain information from the device will not copy all data and may even destroy digital evidence.

Mobile devices use radio waves to communicate over networks with various frequencies and standard communication protocols. Two of the most common mobile communication protocols are GSM and CDMA. Another common technology used in the United States and some other countries is iDEN.

As shown in Figure 20.1, mobile devices can have several identifiers, depending on the manufacturer, region, and technology. GSM devices are assigned a unique

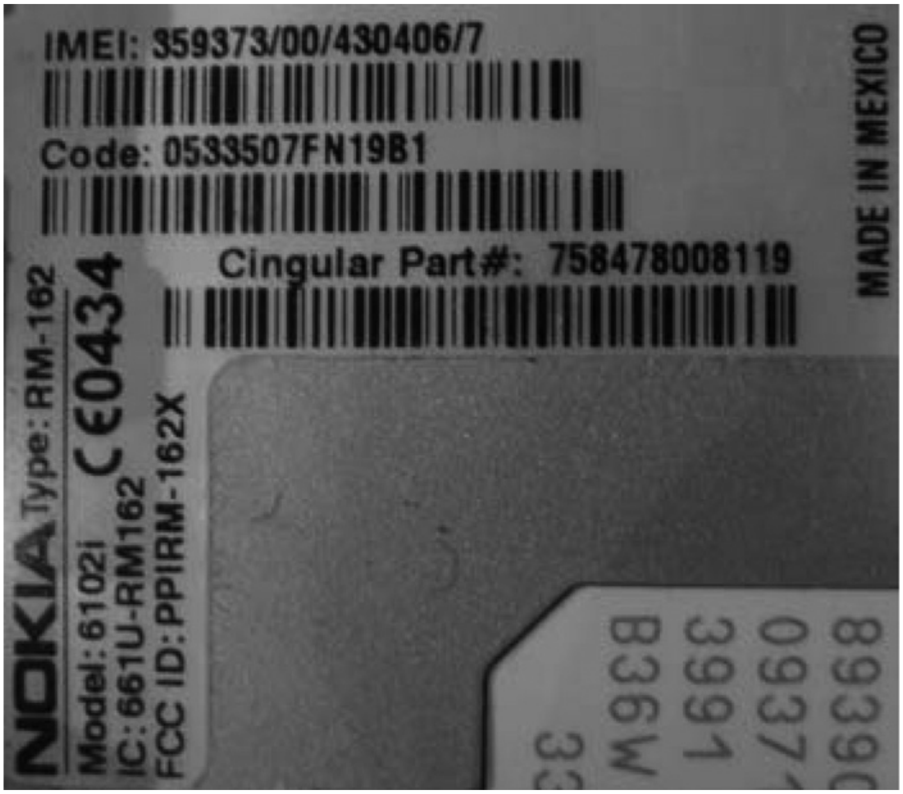


FIGURE 20.1
A Nokia device with various identifiers, including its IMEI and part number. The bottom right shows a SIM card with the ICC-ID.

number called the International Mobile Equipment Identity (IMEI), which includes a serial number for the device. On CDMA phones, the (ESN) is an 11-digit number with the first three digits designating the manufacturer and the remainder unique to the device. The ESN is being replaced with the MEID, which is the CDMA equivalent of the IMEI. There are tools available online that can be used to interpret many of these numbers (e.g., www.numberingplans.com). In addition, some manufacturers assign their own unique serial numbers to mobile devices they make, and Bluetooth-enabled devices also have a unique hardware (MAC) address. Some mobile devices also have an FCC-ID which can be used to search the Web site of the U.S. Federal Communication Commission (http://www.fcc.gov/oet/ea/fccid/) for details about the device, including user manual and photographs.

20.1.2 SIM Cards

GSM devices use SIM cards to authenticate with the network and store various information, including some user-generated activities. SIM cards follow a standard for what information is stored where on the card. However, SIM cards come in slightly different shapes and sizes as shown in Figure 20.2. As a result, a SIM card reader may not be able to accommodate or read data from all SIM cards.

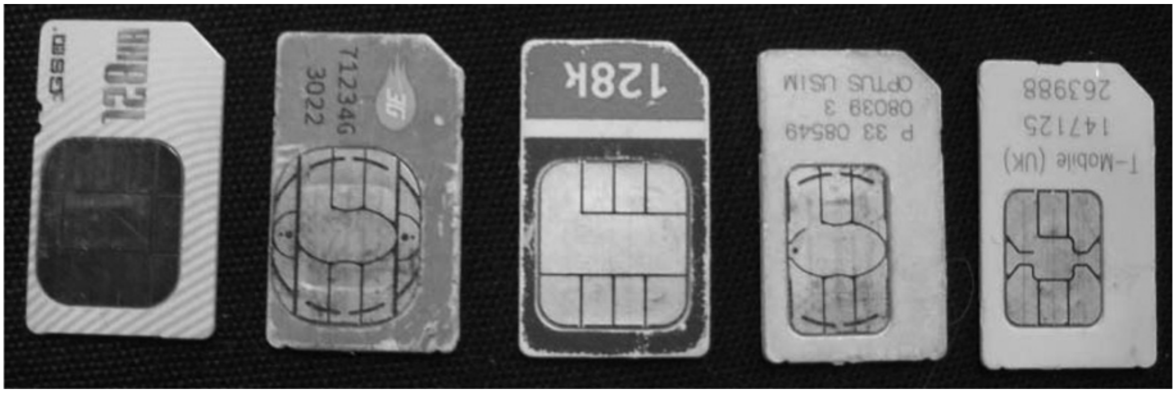


FIGURE 20.2
SIM cards of various sizes.

SIM cards are comprised of a microprocessor, ROM, and RAM, and are assigned a unique Integrated Circuit Card Identifier (ICC-ID). The ICC-ID contains the mobile country code (MCC), mobile network code (MNC), and a serial number of the card. These smart cards are used to authenticate users on GSM and UMTS networks. The SIM card contains information relating to the network and user, including an authentication key (called Ki) needed to establish a connection with the network, the subscriber's personal identification number (PIN) for restricting use of the SIM, and the subscriber's phone number, which is called the Mobile Subscriber ISDN (MSISDN).

The SIM also contains an International Mobile Subscriber Identity (IMSI) that is uniquely associated with the subscriber and is comprised of a country code, a mobile network code, and subscriber identification number. A SIM card may also contain a Temporary Mobile Subscriber Identity (TMSI) and Location Area Identity (LAI). The TMSI is often used over the radio link to avoid revealing the IMSI number to others who may be eavesdropping with radio-related interception equipment. The TMSI and LAI generally change each time a device moves to a new location area within the mobile network.

Not all of the information stored on a SIM card is known or easily accessible by the subscriber. Notice also the separation between the mobile device and the SIM card: a SIM card can easily be transferred to another mobile device.

20.2 TYPES OF EVIDENCE ON MOBILE DEVICES

The forensic benefit of mobile devices in an investigation varies, depending on the criminal acts being investigated, the capability of the mobile device, and how it has been used. Data associated with mobile phones is found in a number of locations; embedded memory, attached removable memory, and the Subscriber Identity Module (SIM) card. Not all of these components will be available or necessary for all investigations, but in some cases there may be multiple SIM cards, removable media, or even more than one mobile device.

PRACTITIONER'S TIP

Concealment Behavior of Mobile Criminals

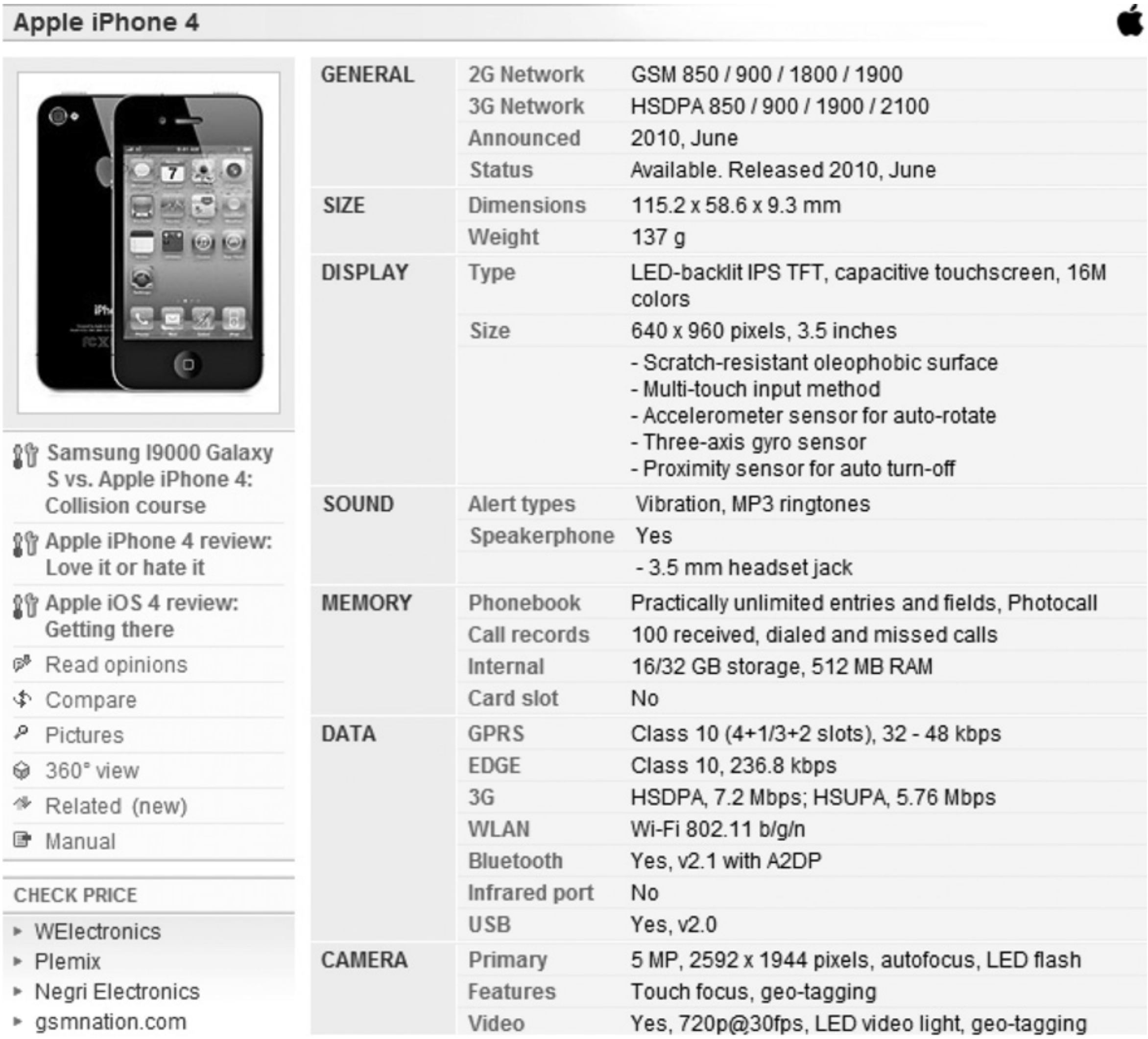
Some criminals are aware of the risks associated with their use of mobile devices. To avoid apprehension, members of certain organized criminal operations will use multiple SIM cards or prepaid mobile devices that are difficult to trace and inexpensive enough to be effectively disposal (a.k.a. burners). After a SIM card or mobile device has been used for a prolonged period, criminals may attempt to destroy them to thwart data recovery. However, useful information may be recoverable from damaged mobile devices or SIM cards. In addition, these people are not immune to technology trends and may also carry high-end personal mobile devices that may provide digital investigators with some insights into the criminals' activities.

Not all phones are created equal, and what is extractable from a device is dependent on its capabilities. Table 20.1 provides a breakdown of phone functionality. The baseline phone information is common across the vast majority of consumer mobile phones, whereas the smart phone evidentiary value extends this basic functionality and associated information.

Table 20.1 Potential Evidence Related to Mobile Devices

Baseline phone	Hardware	Handset date and time; International Mobile Equipment Identity (IMEI)
	User-created information	Address book; SMS; calendar, memos; to-do lists
	Phone-created information	Call register (received, sent, missed)
Smart phone	User-created information	Photographs (including EXIF data); video/audio; maps, MMS; GPS waypoints; stored voicemail; files stored on system; connected computers
	Internet-related information	Online accounts; purchased media (often discoverable in embedded metadata); e-mail; Internet usage; social networking information
	Installed third-party applications	Alternate messaging and communication systems; additional capabilities; malware applications; penetration testing; other applications—anything can help provide alibi or tie to an individual
Local workstation	Transferred information	Tethered mobile devices; backed-up phone data; backed-up third-party applications; store accounts; purchased media
Carrier	Tracking information	Connected cell towers over time; location at different times; current location (inaccurate)
	Usage information	Billing information; call register over time; Internet/data usage; messages not delivered (after radio isolation); be warned—SIM cloning does occur and information is not to be taken at face value
SIM card	Identifiers	Subscriber identifier (IMSI); SIM card identifier (ICC-ID)
SIM card	Usage information	SMS; abbreviated dial names/numbers; last dialed numbers; location areas

Given the wide range of potential functionality, when dealing with a particular mobile device in a case, it is advisable to determine its full functionality to get a better sense of what types of digital evidence it may contain. Manufacturer documentation can provide this information, and there are Web sites that catalog the capabilities of many mobile devices such as phonescoop.com or GSMarena.com as shown in Figure 20.3.



Apple iPhone 4

Samsung I9000 Galaxy S vs. Apple iPhone 4: Collision course

Apple iPhone 4 review: Love it or hate it

Apple iOS 4 review: Getting there

Read opinions

Compare

Pictures

360° view

Related (new)

Manual

CHECK PRICE

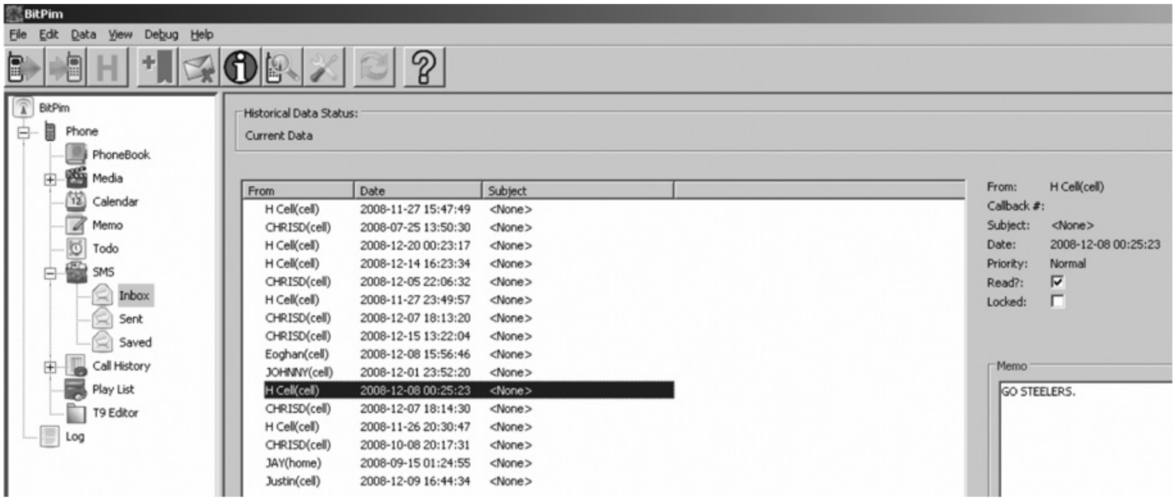
- WElectronics
- Plemix
- Negri Electronics
- gsmnation.com

GENERAL	2G Network	GSM 850 / 900 / 1800 / 1900
	3G Network	HSDPA 850 / 900 / 1900 / 2100
	Announced	2010, June
	Status	Available. Released 2010, June
SIZE	Dimensions	115.2 x 58.6 x 9.3 mm
	Weight	137 g
DISPLAY	Type	LED-backlit IPS TFT, capacitive touchscreen, 16M colors
	Size	640 x 960 pixels, 3.5 inches
		- Scratch-resistant oleophobic surface - Multi-touch input method - Accelerometer sensor for auto-rotate - Three-axis gyro sensor - Proximity sensor for auto turn-off
SOUND	Alert types	Vibration, MP3 ringtones
	Speakerphone	Yes
		- 3.5 mm headset jack
MEMORY	Phonebook	Practically unlimited entries and fields, Photocall
	Call records	100 received, dialed and missed calls
	Internal	16/32 GB storage, 512 MB RAM
	Card slot	No
DATA	GPRS	Class 10 (4+1/3+2 slots), 32 - 48 kbps
	EDGE	Class 10, 236.8 kbps
	3G	HSDPA, 7.2 Mbps; HSUPA, 5.76 Mbps
	WLAN	Wi-Fi 802.11 b/g/n
	Bluetooth	Yes, v2.1 with A2DP
	Infrared port	No
	USB	Yes, v2.0
CAMERA	Primary	5 MP, 2592 x 1944 pixels, autofocus, LED flash
	Features	Touch focus, geo-tagging
	Video	Yes, 720p@30fps, LED video light, geo-tagging

FIGURE 20.3
Details from GSMarena for iPhone 4.

At a minimum, mobile phones can be expected to contain address books, call registers, and Short Messaging Service (SMS) messages, also called *text messages*, as shown in Figure 20.4.

Text messages have the benefit of providing full transcripts, unlike call records, and date-time stamps of received SMS messages are usually accurate because they are inserted by systems operated by the network service provider rather than by the mobile device itself. However, there are investigative disadvantages



Historical Data Status:
Current Data

From	Date	Subject
H Cell(cell)	2008-11-27 15:47:49	<None>
CHRISD(cell)	2008-07-25 13:50:30	<None>
H Cell(cell)	2008-12-20 00:23:17	<None>
H Cell(cell)	2008-12-14 16:23:34	<None>
CHRISD(cell)	2008-12-05 22:06:32	<None>
H Cell(cell)	2008-11-27 23:49:57	<None>
CHRISD(cell)	2008-12-07 18:13:20	<None>
CHRISD(cell)	2008-12-15 13:22:04	<None>
Eoghan(cell)	2008-12-08 15:56:46	<None>
JOHNNY(cell)	2008-12-01 23:52:20	<None>
H Cell(cell)	2008-12-08 00:25:23	<None>
CHRISD(cell)	2008-12-07 18:14:30	<None>
H Cell(cell)	2008-11-26 20:30:47	<None>
CHRISD(cell)	2008-10-08 20:17:31	<None>
JAY(home)	2008-09-15 01:24:55	<None>
Justin(cell)	2008-12-09 16:44:34	<None>

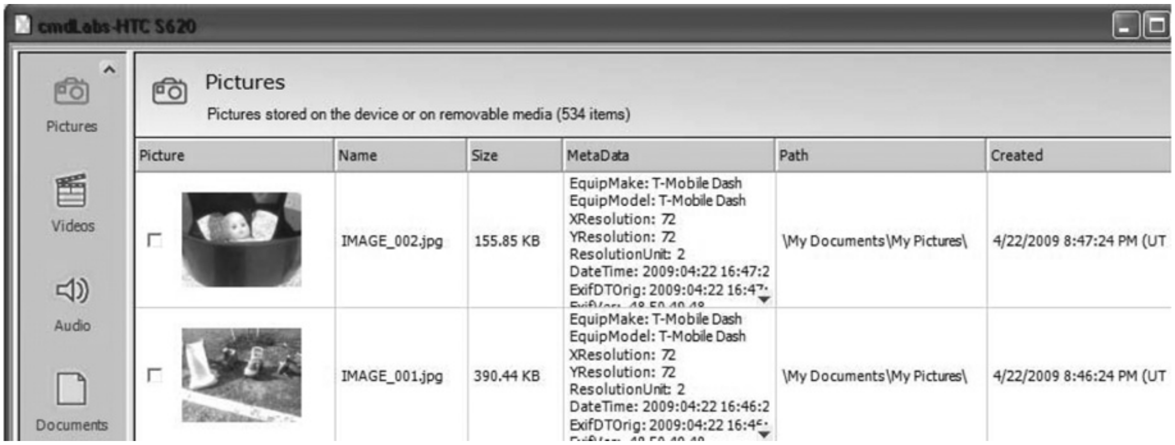
From: H Cell(cell)
Callback #:
Subject: <None>
Date: 2008-12-08 00:25:23
Priority: Normal
Read?: ☑
Locked: ☐

Memo
GO STEELERS.

FIGURE 20.4
SMS messages and other items from a Motorola V3 Razr acquired using BitPim.

with messages; there is no record of when messages were first read (only if they have been accessed), and messages may be incomplete if they have been erased from the handset. Some acquisition methods may recover deleted messages, but this is dependent on the extraction method as discussed later in this chapter.

Smart phones have baseline phone functionality but are vastly more powerful and extendable, and hence have greater evidentiary value. Figure 20.5 shows digital photographs and other information acquired from a Windows Mobile device.



Pictures
Pictures stored on the device or on removable media (534 items)

Picture	Name	Size	MetaData	Path	Created
☐	IMAGE_002.jpg	155.85 KB	EquipMake: T-Mobile Dash EquipModel: T-Mobile Dash XResolution: 72 YResolution: 72 ResolutionUnit: 2 DateTime: 2009:04:22 16:47:2 ExifDTOrig: 2009:04:22 16:47	\My Documents\My Pictures\	4/22/2009 8:47:24 PM (UT
☐	IMAGE_001.jpg	390.44 KB	EquipMake: T-Mobile Dash EquipModel: T-Mobile Dash XResolution: 72 YResolution: 72 ResolutionUnit: 2 DateTime: 2009:04:22 16:46:2 ExifDTOrig: 2009:04:22 16:46	\My Documents\My Pictures\	4/22/2009 8:46:24 PM (UT

FIGURE 20.5
Photographs acquired from a Windows Mobile device using XRY showing EXIF header information.

Photographs, audio, and video can provide some of the most compelling digital evidence in a case. Recall the case of Gaumer described in Chapter 10 involving an accidental voicemail that apparently captured the sounds of the victim being physically assaulted. In some cases accomplices use mobile devices to record a crime, as occurred in the UK when a 15-year-old girl who was found guilty of aiding and abetting manslaughter after she recorded the fatal beating of a man (Borland, 2008). In other cases, perpetrators themselves have filmed their crime.

CASE EXAMPLE (MANCHESTER, UK, 2010)

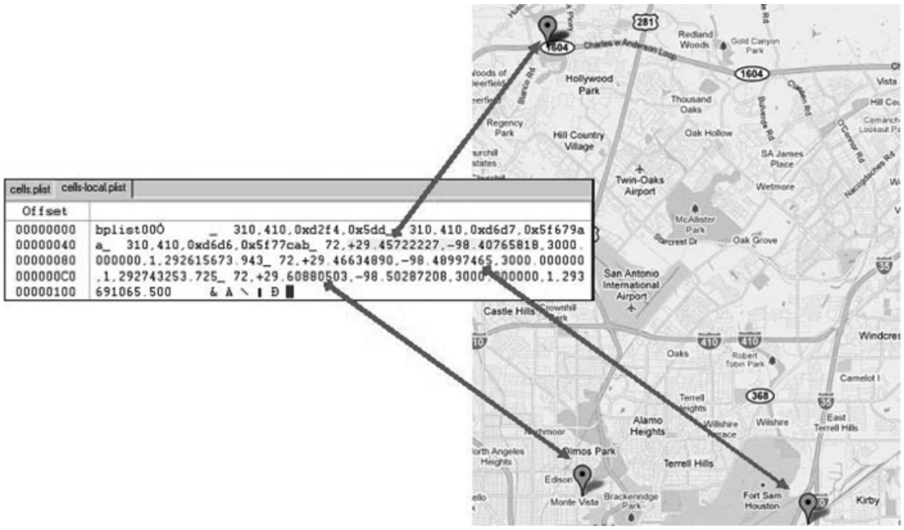
Investigation into the death of 15-month-old Charlie Hunt revealed that he had been beaten by his mother's boyfriend, Darren Newton, over several months (Williams, 2010). Incriminating evidence was found in the form of videos that Newton had taken using his mobile device of himself assaulting the child. The videos, apparently taken over a period of months, showed Newton repeatedly slapping the child on the head for extended periods. On November 19, the final time that Newton assaulted Charlie Hunt, the child died. Newton was sentenced to life in prison for murder.

Smart phones have Internet capability rivalling that on many computers. A more advanced smart phone will additionally store an Internet history, Internet cache, Internet bookmarks, MMS, e-mail, photographs, videos, and installed third-party applications and may be used for transferring computer files. Email and Internet browser history and bookmarks can provide great forensic insight, and phones provide another source of this data. There is also a wealth of information in third-party installed applications. Although online application marketplaces have existed for several years, they are now playing an increasing part of the user experience in mobile devices and greatly augment the capability of individual mobile phones.

20.2.1 Location Information

The ability to determine the location of mobile devices during a period of interest is a powerful investigative capability. Some mobile devices record the location of cellular towers they contacted, potentially providing a historical record of the user's whereabouts over a given period. For instance, iPhones store the locations of recently used cellular towers in a file as shown in Figure 20.6.

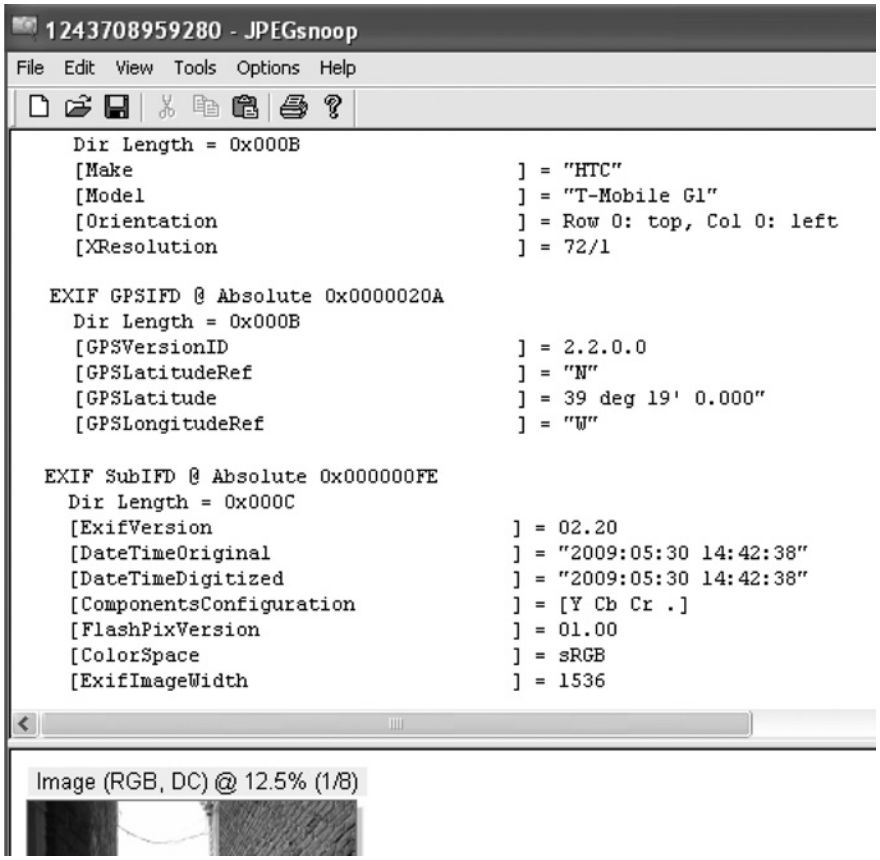
GPS-enabled devices may also contain remnants of past locations and maps that can be useful in an investigation. Additionally, EXIF data embedded in digital photographs can add additional evidentiary value, providing the date and time the photograph was created, the device type used to create it, and potentially the GPS coordinates of where the photograph was taken as shown in Figure 20.7. Onboard GPS may also provide the user with mapping functionality, and hence provide forensic investigators with waypoints, plotted destinations, and routes taken.



cells.plist cells-local.plist

```
Offset
00000000  bplist00Ó       _   310,410,0xd2f4,0x5dd_  310,410,0xd6d7,0x5f679a
00000040  a_  310,410,0xd6d6,0x5f77cab_ 72,+29.45722227,-98.40765818,3000.
00000080  000000,1,292615673.943_ 72,+29.46634890,-98.48997465,3000.000000
000000C0  ,1,292743253.725_ 72,+29.60880503,-98.50287208,3000.000000,1.293
00000100  691065.500     & Λ \ ı Ð █
```

FIGURE 20.6
A file from an iPhone containing longitude and latitude of cellular tower locations used by the device.



1243708959280 - JPEGsnoop

```
    Dir Length = 0x000B
    [Make                              ] = "HTC"
    [Model                             ] = "T-Mobile G1"
    [Orientation                       ] = Row 0: top, Col 0: left
    [XResolution                       ] = 72/1

  EXIF GPSIFD @ Absolute 0x0000020A
    Dir Length = 0x000B
    [GPSVersionID                      ] = 2.2.0.0
    [GPSLatitudeRef                    ] = "N"
    [GPSLatitude                       ] = 39 deg 19' 0.000"
    [GPSLongitudeRef                   ] = "W"

  EXIF SubIFD @ Absolute 0x000000FE
    Dir Length = 0x000C
    [ExifVersion                       ] = 02.20
    [DateTimeOriginal                  ] = "2009:05:30 14:42:38"
    [DateTimeDigitized                 ] = "2009:05:30 14:42:38"
    [ComponentsConfiguration           ] = [Y Cb Cr .]
    [FlashPixVersion                   ] = 01.00
    [ColorSpace                        ] = sRGB
    [ExifImageWidth                    ] = 1536
```

Image (RGB, DC) @ 12.5% (1/8)

FIGURE 20.7
An EXIF header from a digital photograph showing the GPS coordinates of the originating device at the time the photograph was taken.

20.2.2 Malicious Code on Mobile Devices

As mobile devices are being used more to conduct online banking and shopping, they are becoming prime targets for computer criminals to steal money or valuable information. For instance, a fake banking application for Android devices was disseminated to unsuspecting users and sent information to a third party without their consent (2010, Rogue phishing app smuggled onto Android marketplace, John Leyden, http://www.theregister.co.uk/2010/01/11/android_phishing_app/). More sophisticated malware allows criminals to intercept SMS messages associated with online banking transactions, enabling them to steal money directly from a victim's bank account.

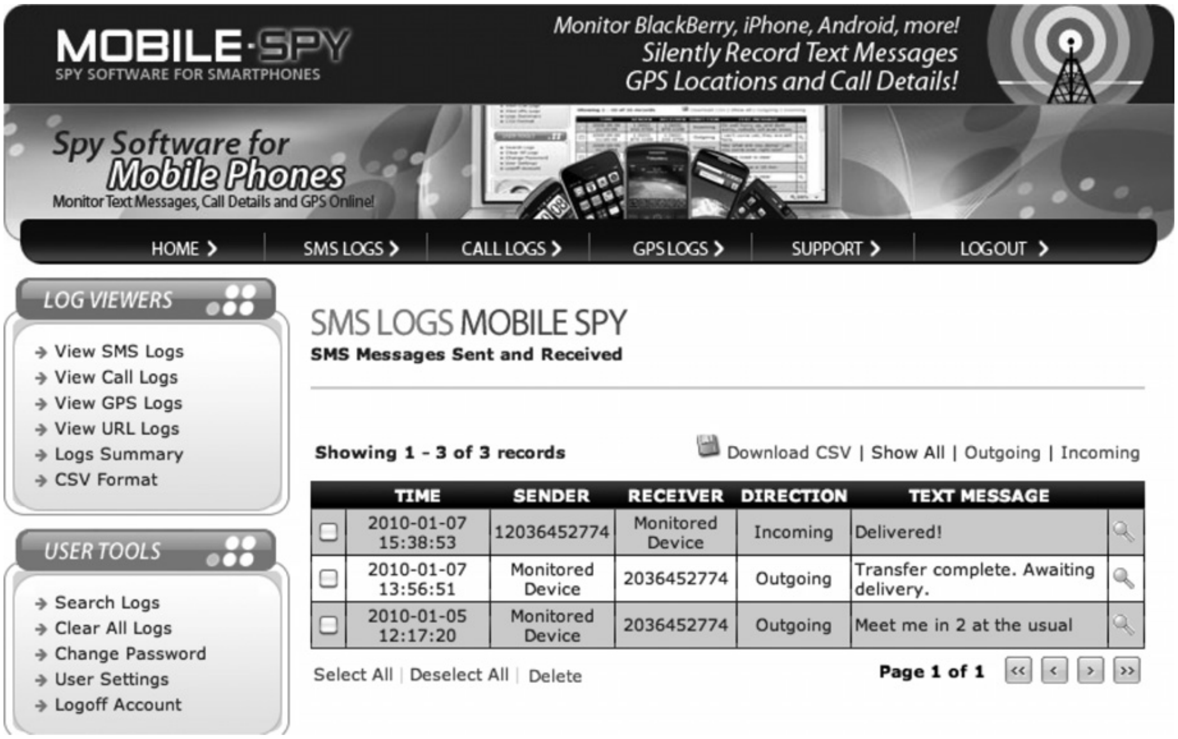
CASE EXAMPLE: ZEUS IN THE MOBILE

A malicious Trojan program called ZeuS was designed to monitor activities of the users on a computer and steal their online banking information. A variant of this program tricked computer users to provide information about their mobile device. This information was then used to intercept SMS messages associated with online banking, and to capture mobile transaction authentication numbers used to approve unauthorized bank transactions.

In addition, programs are available to monitor activities on mobile devices, including Windows Mobile, Blackberry, and iPhone. These programs are sometimes called *spouseware*, effectively eavesdropping on the user of the device. Details about text messages, calls, Internet browsing, and GPS coordinates are recorded and can be viewed via a Web site by a person with the associated credentials. For instance, Figure 20.8 list text messages on a Windows Mobile device running MobileSpy. This information is only viewable by someone with a username and password associated with that specific installation of MobileSpy. These programs leave traces on mobile devices that can be found through forensic examination.

As people and organizations become more reliant on mobile devices, computer criminals will devote more attention to exploiting these devices to victimize individuals and break into corporate networks.

Mobile devices can also be used as a platform to launch attacks against other systems. Several computer and network security tools have been ported to mobile devices. Port scanners, wireless network security analyzers, and penetration testing frameworks such as Metasploit have all been ported or developed for Apple iPhone and Android devices. Although not official, these application types do exist and may be used for crime. The presence of such applications is of interest in computer misuse investigations (Moore, 2007).



SMS LOGS MOBILE SPY

SMS Messages Sent and Received

Showing 1 - 3 of 3 records

	TIME	SENDER	RECEIVER	DIRECTION	TEXT MESSAGE	
□	2010-01-07 15:38:53	12036452774	Monitored Device	Incoming	Delivered!	🔍
□	2010-01-07 13:56:51	Monitored Device	2036452774	Outgoing	Transfer complete. Awaiting delivery.	🔍
□	2010-01-05 12:17:20	Monitored Device	2036452774	Outgoing	Meet me in 2 at the usual	🔍

Page 1 of 1

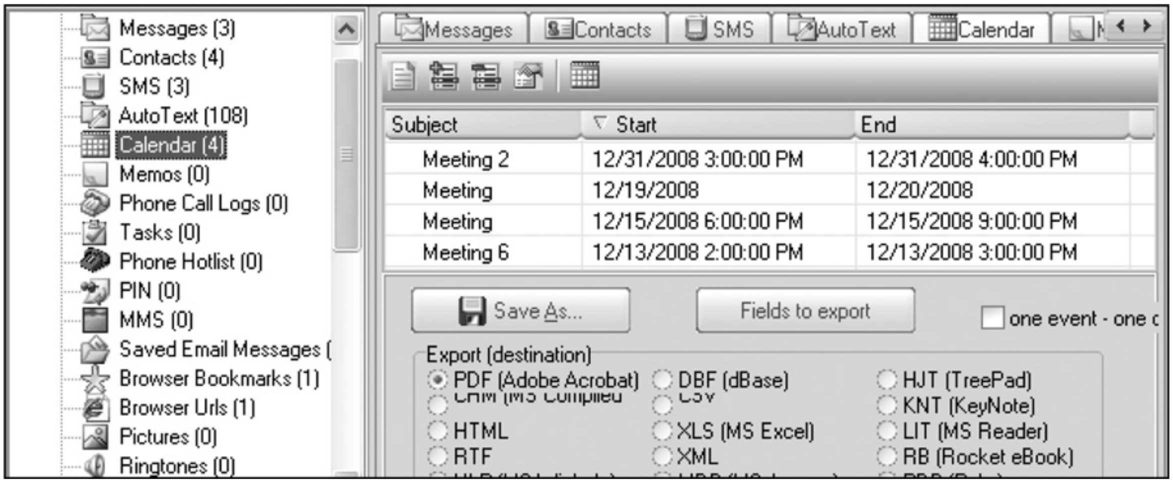
FIGURE 20.8
MobileSpy used to intercept text messages on a mobile device and post them to a Web server.

20.2.3 Thinking Outside of the Device

Digital investigators must always keep in mind that mobile devices can connect to various networks via cellular towers, WiFi access points, and Bluetooth. The networked nature of mobile devices creates opportunities and dangers from a forensic standpoint. Connected networks can contain investigatively useful information related to mobile devices, but can also enable offenders to obliterate incriminating evidence remotely. For instance, Apple provides a Web-based service to remotely wipe a lost or stolen iPhone, and organizations that centrally manage Blackberry devices can remotely wipe a specific device from Blackberry Enterprise Server.

Network service providers may provide information for consistency with the data extracted from the phone, or may be additional to what can be recovered from the device. Billing records are maintained by network service providers for many subscribers. Customers that have a monthly usage plan will receive an itemized bill showing the calls, messages, and data activities associated with their mobile device. Once subscriber information is retrieved by digital investigators, a carrier may provide additional historical call records, unretrieved SMS messages, billing information, and cell towers the device has connected to over time, the latter providing an inexact method of physically determining where a phone has been. These records can provide useful historical details that are no longer recoverable from the mobile device itself. For example, the numbers dialed may connect a suspect with a victim. In addition, network service providers generally maintain call detail records that can provide specific details about each call and message pertaining to a mobile device. For more in-depth coverage of the types of information that are available from network service providers that can be useful in an investigation, see the "Wireless Networks" in *Digital Forensics and Investigation* (Dario Forte, 2009).

Data relating to a handheld device can often be found on associated desktop computers. For example, when a mobile device is synchronized with a desktop computer, data are stored in backup files indefinitely. Items that have been erased from the device may still exist on the desktop including e-mail messages and private data. These files may be stored in a proprietary format and it may be necessary to obtain specialized tools to interpret these backup files on the desktop. For instance, Blackberry backup files are stored in an IPD format that can be viewed using Amber ABC Converter as shown in Figure 20.9.



Subject	Start	End
Meeting 2	12/31/2008 3:00:00 PM	12/31/2008 4:00:00 PM
Meeting	12/19/2008	12/20/2008
Meeting	12/15/2008 6:00:00 PM	12/15/2008 9:00:00 PM
Meeting 6	12/13/2008 2:00:00 PM	12/13/2008 3:00:00 PM

□ one event - one c

Export (destination)

● PDF (Adobe Acrobat) ○ DBF (dBase) ○ HJT (TreePad)
○ CHM (MS Compiled ○ CSV ○ KNT (KeyNote)
○ HTML ○ XLS (MS Excel) ○ LIT (MS Reader)
○ RTF ○ XML ○ RB (Rocket eBook)

FIGURE 20.9
Amber ABC Converter used to view a Blackberry IPD file.

Digital investigators can obtain information about online accounts that have been used on mobile devices to connect with cloud-based services such as Gmail. For instance, the following user account information was extracted from a keychain database on an iPhone, including accounts on Yahoo, Hotmail, and Windows Live.

```
F:\tools>sqlite3.exe “iPhone2\Keychains\keychain-2.db”
SQLite version 3.6.16
Enter “.help” for instructions
Enter SQL statements terminated with a “;”
sqlite> select labl,acct,svce from genp;
|eric.rooster@yahoo.com|Yahoo-token
|erooster@live.com|
|erikroost@hotmail.com|
|therooster@hotmail.com|
|therooster@hotmail.com|com.apple.itunesstored.keychain
erooster|MMODBracketsAccount|
LumosityBrainTrainer|erooster|LumosityBrainTrainer
```

Communications, documents, and multimedia created using a mobile device may be transferred to cloud-based services for long-term storage. Mobile devices that are capable of accessing the Internet can provide further linkage to online social networks such as Facebook, which can provide digital investigators with further information about who an individual is associated with. Therefore, digital investigators may find a treasure trove of data on these servers that is no longer available on the mobile device itself.

Digital investigators can also use information from mobile devices to learn more about the user’s social network. Even a basic mobile phone can provide digital investigators with a wealth of information about the user’s social network—analysis of contacts and address books provides an indication of an individual’s social, work, and family networks. The ability to reconstruct social networks using information from mobile devices is a powerful tool for investigating any criminal organizations including drug dealers, gangs, human traffickers, and terrorists (Koschade, 2006).

CASE EXAMPLE: CLEANING THE STREETS

Although drug dealers were using cheap, disposable mobile devices to conduct their criminal enterprise, digital investigators were able to use information from these devices to apprehend over 20 drug dealers in Medford, Oregon. In addition to linking drug dealers based on call history recovered from mobile devices, digital investigators recovered photographs of individuals doing or selling drugs (Conrad, 2010).

For a single mobile device it is often useful to know whom someone knows, but there is additional benefit for large investigations. Where multiple devices are involved, analysis of overlapping networks can provide leads on common friends or acquaintances and how communication occurs between otherwise unrelated groups. Analysis of the call register will add greater insight into the strength of the connections between individuals and can provide a timeline of communication. Both the call register and address book on a mobile device can also be used as a way of corroborating or refuting testimony from the phone’s primary user.

20.3 HANDLING MOBILE DEVICES AS SOURCES OF EVIDENCE

In general, the same forensic principles that apply to any computing device also apply to mobile devices in order to enable others to authenticate acquired digital evidence. Recall that the purpose of a forensically sound process is to document that the evidence is what you claim and has not been altered or substituted since collection. At a minimum, all steps taken to extract data should be recorded to support transparency and repeatability, enabling others to assess and repeat your work. In addition, the MD5 hash of acquired data should be calculated and documented, allowing others to verify that nothing has been altered since the data were acquired. Any issues encountered during the acquisition process should also be noted, even when they are embarrassing or the cause is unknown. Documentation must also show continuous possession and control throughout its lifetime. Therefore, it is necessary not only to record details about the collection process, but also every time it is transported or transferred and who was responsible.

Keep in mind that some devices can receive data through wireless networks that might bring new evidence but might overwrite existing data. Therefore, an investigator must make a calculated decision to either prevent or allow the device to receive new data over wireless networks as depicted in Figure 20.10. Removing the battery from a mobile device will prevent it from communicating but may also activate security measures such as lock codes and encryption that could prevent further access to data on the device. In addition, when using acquisition methods that require the mobile device to be powered on, it is necessary to isolate the mobile device from networks.

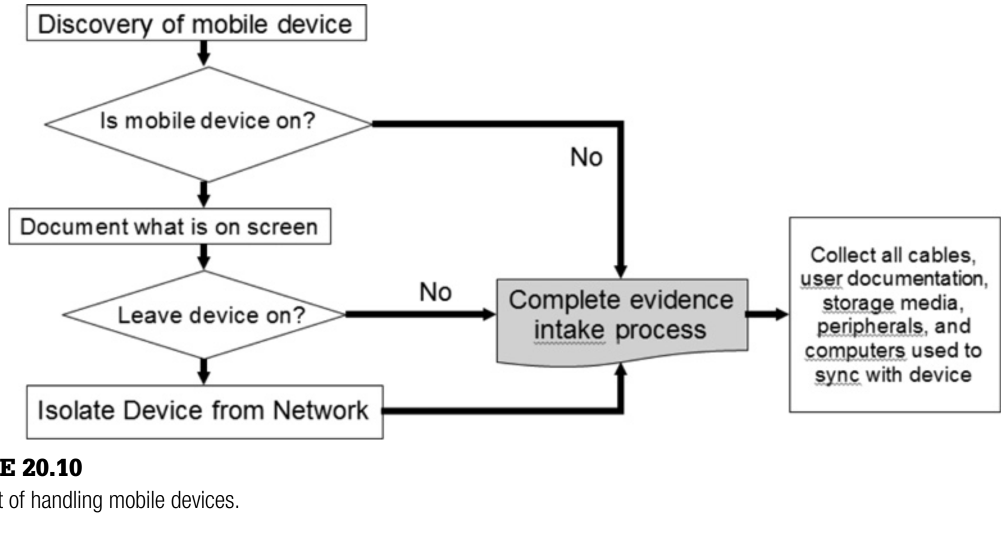

Discovery of mobile device
Is mobile device on?
No
Document what is on screen
Leave device on?
No
Complete evidence intake process
Collect all cables, user documentation, storage media, peripherals, and computers used to sync with device
Isolate Device from Network

FIGURE 20.10

Flowchart of handling mobile devices.

Network isolation ensures that the contents of a phone reflect the time at which it was seized, disallowing changes that may occur to it after it has been seized. Actions over the network that can alter content include receiving phone calls, messages, network polling activity, and the use of remote erasure systems; the latter being an enterprise feature designed for corporate smart phones. Such network activities can alter the contents of a mobile device, potentially adding new data, overwriting existing data or unallocated space, or erasing the phone contents remotely.

Some devices can be reconfigured to prevent communication with the network. Devices that do not have such a feature can be isolated from radio waves by placing them in Faraday isolation, such as radio-frequency shielded evidence containers, which block network communications. Signal jamming systems provide another means for preventing mobile devices from communicating with a network but this type of equipment is illegal in some jurisdictions. Network isolation practices must be maintained during forensic analysis, and this is achieved with shielded mobile phone examination rooms or extraction cases. To protect the device against damage or accidental activation, package it in an envelope or bag.

PRACTITIONER'S TIP

Mobile Device Triage

Given the dynamic and rapidly evolving nature of mobile device forensics, it is sometimes necessary to acquire data the moment it is observed and available. In some situations, such as military operations or bomb threats, there is neither the time nor resources to isolate the device from the network prior to extracting information. Furthermore, any delays could allow timed security locks to activate or provide a window for remote wiping. Effective on-scene triage processes and tools may preserve evidence that would otherwise be lost, and can make the difference between life and death in certain situations (Mislan, Casey, & Kessler 2010).

After taking precautions to protect data on the device, examine it for physical damage or suspicious modifications. In most cases, a cursory examination of the exterior of the device will suffice. However, when dealing with a very technically savvy or dangerous offender, some investigative agencies use X-ray or high-resolution microscopes to detect physical damage or modifications.

With the decreasing size of memory modules, they can be easily overlooked, hidden, destroyed, or swallowed. The microSD card in Figure 20.11 can store 256 MB of data, and much larger capacity cards are emerging. These storage modules can contain multimedia files, SMS/MMS messages, as well as backups of data from the mobile device.

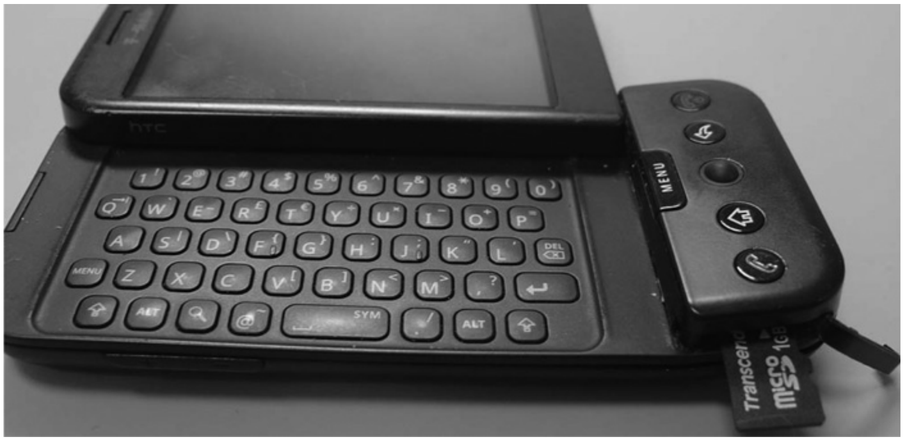


FIGURE 20.11
A 1-GB removable storage media card in a G1 mobile device that has a small enough form factor to be overlooked but large enough storage capacity to contain useful digital evidence.

Even experienced forensic practitioners sometimes overlook these small-scale storage modules. The slot for these storage modules is very difficult to find on some mobile devices like the G1. If, while assessing the capabilities of a mobile device, you find that the device supports a removable storage card check for the presence of such a card in the evidentiary device right away. When you find a removable storage module in a mobile device, remove it immediately to preserve the information that it contains.

These storage media are generally FAT formatted and can be handled in a forensic manner in the same way as other storage media. Specifically, document the serial number and any other identifying details, examine the media for damage, activate write protection switches if present, and then create a forensic duplicate of the contents via a suitable adapter. The resulting forensic duplicate can be examined using your forensic software of choice, enabling exploration of the file system and recovery of deleted files.

PRACTITIONER'S TIP

Evidence Contamination

When certain mobile devices are powered on without their SIM card, they instruct the user to insert a SIM card. Do not insert your personal SIM card since data transfer or data loss may occur. For example, Windows Mobile devices automatically import the contents of an inserted SIM card. So, if you were to insert your own SIM card, the device will be contaminated with your personal data from the SIM card.

In addition to collecting a mobile device itself, it is important to look for associated items that might contain data or help extract data from the device. Removable memory and SIM cards can contain more data than the device itself and interface cables and cradles may be needed to connect the device to an evidence collection system. As with any other computer, document the types of hardware and their serial numbers, taking photographs and notes as appropriate. If a device is on when it is found, leave it on if possible because turning it off may activate password protection, making it more difficult to extract data from the device later. Also, document any information visible on the display including the date and time of the system clock.

20.4 FORENSIC PRESERVATION OF MOBILE DEVICES

Given the variety of mobile devices, it should come as no surprise that there is no single, standardized method of accessing all of them to extract data using software or hardware. This is one of the first major hurdles of mobile device forensics, because without any means of accessing the data on a device, you are left with only one option: manual examination. When acquiring data from mobile devices, there are a variety of options and the specifics of a case and the mobile device will dictate which approach is most suitable. A corollary of this fact is that no single tool will cover all mobile devices nor will a single tool cover all situations. The current available methods for extracting data from mobile devices are summarized in Table 20.2.

Table 20.2 Methods of Extracting Information from Mobile Devices

Method	Description
Manual operation via user interface	Examiner manually accesses the phone through the user interface. To ensure that all details are documented and the chain of custody is preserved, this process is normally photographed or videotaped. Only data accessible through the operating system is retrievable. The most basic process.
Logical acquisition via communication port	Logical acquisition methods interact with mobile devices using protocols such as AT commands and OBEX (OBject Exchange), and only extracts data that is accessible through the operating system.
Physical acquisition via communication port or proprietary interface (e.g., Nokia FBUS)	Extracts the memory contents in their entirety through the communications port. Interpreting the extracted binary is dependent on understanding how the phone stores data in memory structures.

(*Continued*)

Table 20.2 Methods of Extracting Information from Mobile Devices (*Continued*)

Method	Description
Physical acquisition via JTAG	Uses the JTAG interface to extract the memory contents of the device. Allows the extraction of full binaries. Acquiring digital evidence via the JTAG is less intrusive than relying on the device operating system, but interpreting the extracted binary requires in-depth knowledge of the device.
Physical acquisition via direct memory chip access	The most low-level and potentially complex acquisition method for mobile devices. Involves extracting memory chips from the device and reading the memory structures. Can provide access to all device content, but requires knowledge of interpreting the raw structures. This technique should not be used for cases when the original device must remain operable.

It is generally advisable to acquire data from a mobile device using two or more of the methods in Table 20.2 in order to compare the results to ensure the information that you are basing your work on is correct.

A manual examination is sometimes sufficient if investigators only need a particular piece of information from the device. Before performing a manual examination of a device, it is advisable to become familiar with its operation using an identical test device. For this reason, and to enable tool testing and tool development, forensic laboratories that specialize in this type of examination maintain an extensive collection of mobile devices. When performing a manual examination, it is important to record all actions taken with device to enable others to assess whether the examination was performed satisfactorily.

PRACTITIONER'S TIP

Overlooking Evidence

During a manual examination of a mobile device, it is easy to overlook areas of digital evidence because they are new, novel, or simply unfamiliar. For instance, a digital investigator might not realize the significance of an application such as Tigertext (www.tigertext.com) that is designed to exchange secret messages via mobile devices. As a result, the digital investigator might not open the application and review its contents, thus missing digital evidence that could be crucial to the case. To reduce the risk of overlooking evidence on a mobile device, it is important to explore each screen and application methodically and to document the results carefully.

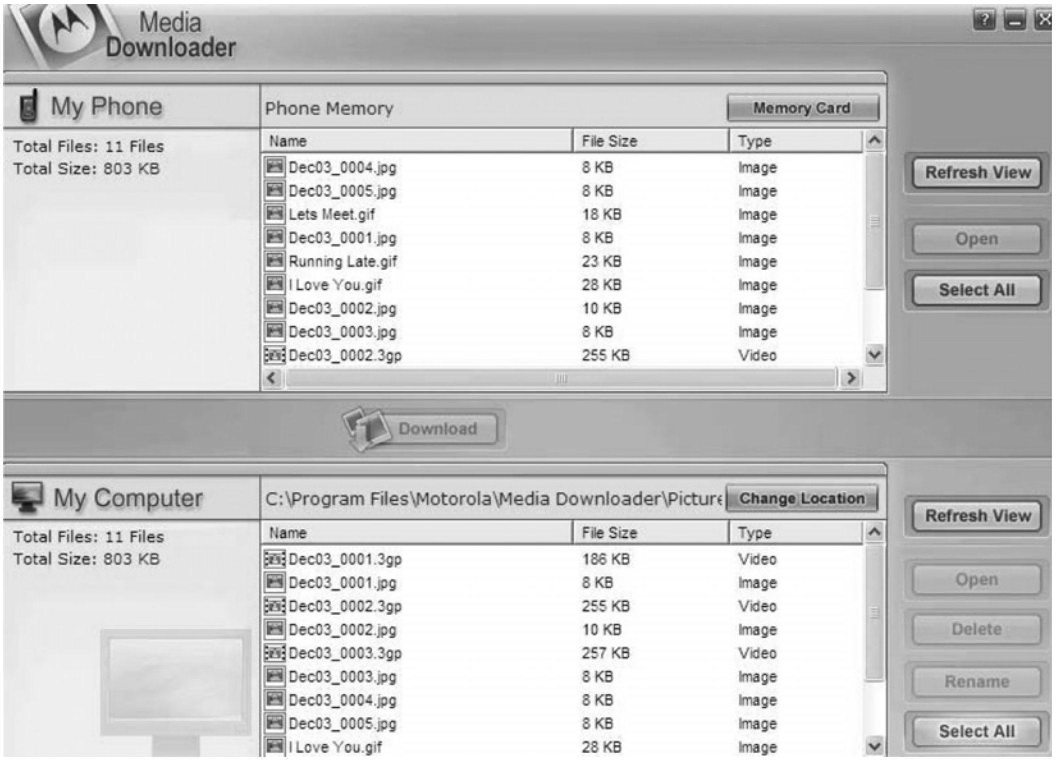
The most common automated method of accessing devices is using a data cable, followed by a wireless means such as Bluetooth. Once you have such access to the device, the next major hurdle is determining the most effective means of extracting data from the device. Some mobile devices support standard AT command access, but this usually only provides access to a limited selection of data. Many mobile devices have proprietary protocols and require manufacturer/developer tools to execute. Logical acquisition provides context for items such as date-time stamps and location within the file system on a mobile device. In some instances, the information retrievable from a data cable is different from the information extractable via Bluetooth, so it may be beneficial to perform logical extraction in different ways to ensure all possible content has been extracted.

The main benefit of acquiring physical memory is that a more complete capture of data is obtained, including deleted items. In addition, physical acquisition methods can work with damaged mobile devices and generally make fewer alterations to the original device while data are being acquired. There are several approaches to acquiring a forensic duplicate of mobile devices at a physical level. Some forensic tools transfer and run an executable commonly called a *software agent* on the mobile device. Alternately, the boot process of some mobile devices can be interrupted, giving access to the system before the main operating system loads and enabling you to interact with the device at a low level via a boot loader. More advanced methods of acquiring physical memory involve accessing mobile devices at a hardware level, either through the JTAG interface or by reading the Flash memory chips directly. However, extracting a full dump of physical memory does not provide the logical structure of the file system, making it necessary to either extract unstructured data or interpret file system information in a raw form.

Best practice guidelines from the 2000 International Organization on Computer Evidence conference (IOCE, 2000) state that phones and other electronic devices should be examined with "methods that minimise loss/change of data." However, acquisition of mobile devices may require some interaction, depending on the type of extraction method used. Manual and logical acquisition methods require some degree of interaction, and physical acquisition methods require either interaction or physical deconstruction. JTAG access may be the best middle ground but requires knowledge of the integrated circuit, which is generally only known to manufacturers. There is no single best method to forensically acquire data from mobile phones.

While logical and physical acquisition methods require the least interaction with the target device, it is often not practical to obtain an exact memory image of a device, both for logistical and technical reasons. Therefore, the phone's (and SIM card's) operating system must be trusted not to alter the memory when read commands are executed. If, in the course of an examination an analyst finds that an acquisition technique has altered data, this must be noted.

Ideally, it would be possible to first acquire the full contents of physical memory from a mobile device. This gives access to deleted data, including SMS data, earlier call logs, and IMSI numbers from SIM cards that were previously inserted in the mobile device. In addition, if the user sets a customized lock code for a mobile device, this information can be extracted from a full memory dump and then used to acquire the device logically. Unfortunately, current forensic tools are not able to acquire physical memory from every type of mobile device, and hardware access methods require specialized knowledge and equipment that are not available in many cases. Fortunately, the unlock code for some mobile devices can be obtained or bypassed using forensic tools that acquire logical data from mobile devices. The benefit of acquiring a device logically is that it provides you with additional context of data (i.e., which filename it was associated with) and associated metadata (e.g., when the data were created). For some devices, only the manufacturer's backup utility is currently capable of extracting certain items. For instance, Figure 20.12 shows the Motorola backup utility of iDEN phones obtaining files from a mobile device that could not be acquired using any forensic tools.



Total Files: 11 Files
Total Size: 803 KB

Name	File Size	Type
Dec03_0004.jpg	8 KB	Image
Dec03_0005.jpg	8 KB	Image
Lets Meet.gif	18 KB	Image
Dec03_0001.jpg	8 KB	Image
Running Late.gif	23 KB	Image
I Love You.gif	28 KB	Image
Dec03_0002.jpg	10 KB	Image
Dec03_0003.jpg	8 KB	Image
Dec03_0002.3gp	255 KB	Video

C:\Program Files\Motorola\Media Downloader\Pictur

Total Files: 11 Files
Total Size: 803 KB

Name	File Size	Type
Dec03_0001.3gp	186 KB	Video
Dec03_0001.jpg	8 KB	Image
Dec03_0002.3gp	255 KB	Video
Dec03_0002.jpg	10 KB	Image
Dec03_0003.3gp	257 KB	Video
Dec03_0003.jpg	8 KB	Image
Dec03_0004.jpg	8 KB	Image
Dec03_0005.jpg	8 KB	Image
I Love You.gif	28 KB	Image

FIGURE 20.12
iDEN backup.

PRACTITIONER'S TIP

Dealing with Password Protection

Many mobile devices permit users to set a password to restrict access to the device. For certain devices, it is possible to bypass or recover such protection. It is generally inadvisable to guess a lock code or passphrase because some mobile devices will wipe their contents after too many failed attempts. Some jurisdictions also provide legislative recourse to acquire passphrases and lock codes from suspects when technical methods are not effective or feasible. Such recourse often requires a court order or warrant.

Be aware that a blank or broken display may simply indicate that the screen is damaged and it may still be possible to extract evidence via cable as shown in Figure 20.13.

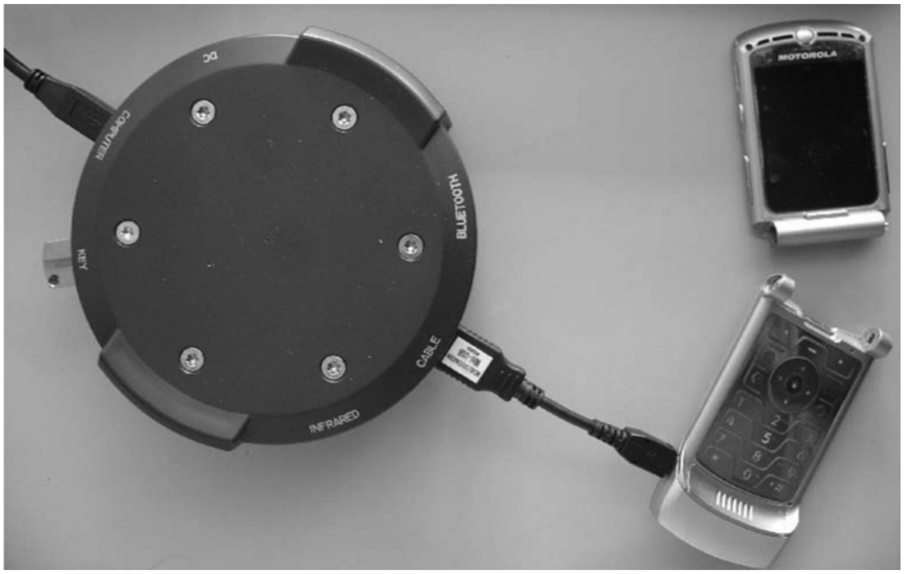


FIGURE 20.13
Physical acquisition of broken mobile device using XACT.

20.4.1 Mobile Device Forensics Tools

Forensic tools are in constant development to provide a convenient means of extracting specific data from various mobile devices, typically logically via cable, infrared, and Bluetooth or physically via cable or JTAG. All of these tools function in a similar way, sending commands to the phone and recording responses that contain information stored in the phone's memory. The information that can be extracted using these methods depends on both the connection mechanism and model of the phone.

Logical mobile phone acquisition systems interact with the phone operating system to extract data, much in the same way the vendor synchronization systems do. As such, there are limitations to the information retrievable, and only information relevant to the Operating System is available. As such, information potentially relevant in a forensic investigation might not be acquired; information such as deleted items won't be extracted. Mobile phones generally have a baseline of extractable data from such tools; phone address book, call register, SMS and photographs, but additional information is not guaranteed.

The limitation to these forms of applications is that it relies on the assumption that the desktop application and the investigator are assuming that the phone's logic is not making any changes to other areas of the phone's memory. However, this assumption cannot be verified without the source code and circuit schematics of the phone's software and hardware, which are rarely, if ever, publicly available.

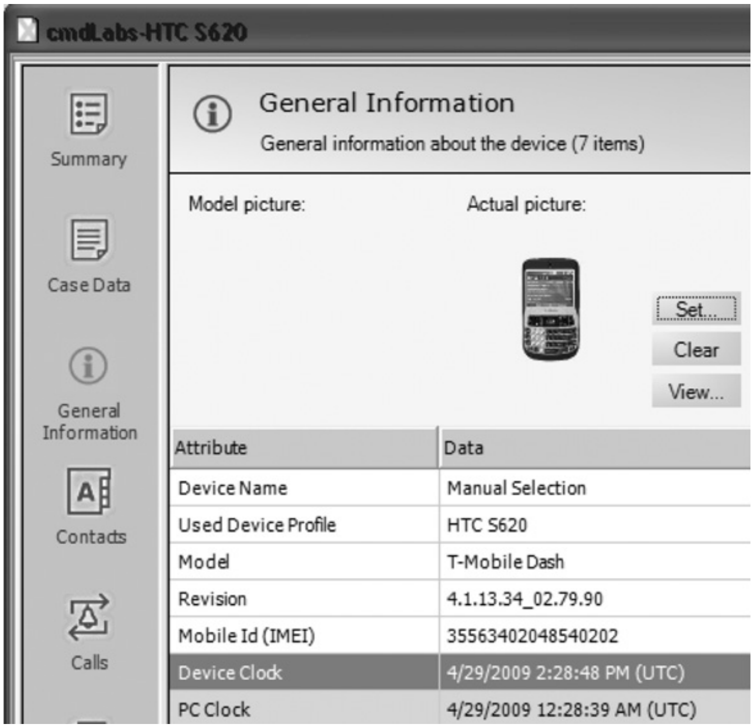
There are several commercial forensic tools specifically designed to acquire data from mobile phones. This section introduces some of the more popular commercial tools.

MicroSystemation XRY (http://www.msab.com) is one of the market leaders in mobile device acquisition. MicroSystemation sell products to capture mobile phones and other small-scale devices logically via USB, infrared, and Bluetooth. XRY also has an additional component, XACT, that expands capability by performing physical acquisition via the JTAG interface. XACT also allows for the acquisition of specific models of GPS receiver. Figure 20.14 shows the XRY acquisition interface.

Cellebrite Universal Forensic Extraction Device (UFED) (http://www.cellebrite.com) is a self-contained, portable mobile phone logical acquisition device. The system is self-powered and copies data to a USB disk or to a second phone. Cellebrite UFED was designed in Israel. The Cellebrite UFED is shown in Figure 20.15. Cellebrite also have an additional component, UFED Physical Pro, that allows physical acquisition of mobile phones and other small-scale devices. UFED systems are also available in a field-ready ruggedized form.

Logicube CellDEK (http://www.logicubeforensics.com) is a system designed to acquire data from mobile phones and other small-scale devices such as GPS receivers. CellDEK conducts logical extraction of data via USB, infrared, and Bluetooth.

MOBILedit! Forensic (http://mobiledit.com) is another logical data acquisition tool. MOBILedit! Forensic can be purchased as a software-only tool or as part of a kit including cables and infrared reader.



cmdLabs-HTC S620

General Information

General information about the device (7 items)

Attribute	Data
Device Name	Manual Selection
Used Device Profile	HTC S620
Model	T-Mobile Dash
Revision	4.1.13.34_02.79.90
Mobile Id (IMEI)	35563402048540202
Device Clock	4/29/2009 2:28:48 PM (UTC)
PC Clock	4/29/2009 12:28:39 AM (UTC)

FIGURE 20.14
XRY Interface showing data acquired from a mobile device.

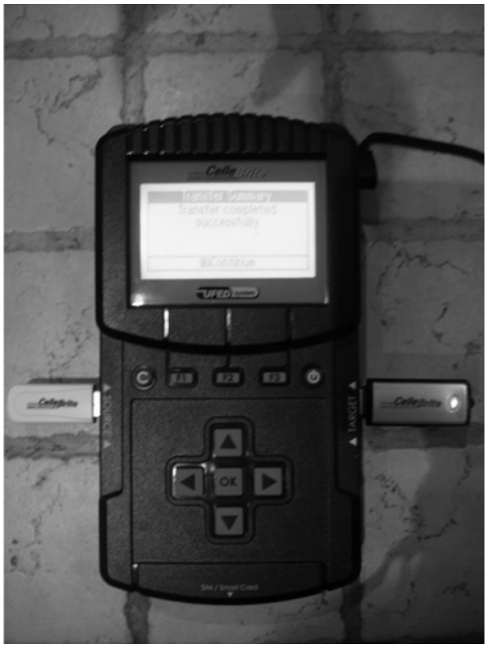
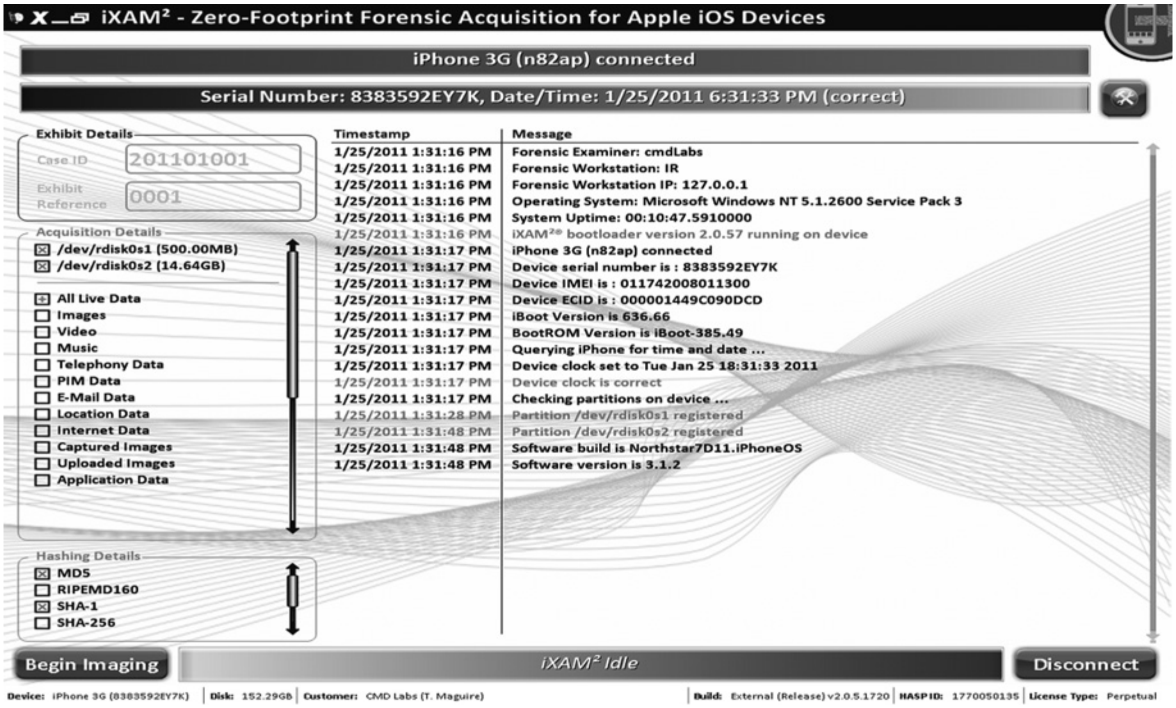


FIGURE 20.15
Cellebrite UFED device.

iXAM (http://www.ixam-forensics.com) is a forensic acquisition system specifically for the Apple iPhone and Apple iPod Touch. iXAM acquires data via the USB interface, but has full physical extraction of data. iXAM is a niche system, only providing acquisition of a small number of devices from a single manufacturer. Figure 20.16 shows iXAM acquiring an Apple iPhone.



iXAM² - Zero-Footprint Forensic Acquisition for Apple iOS Devices

iPhone 3G (n82ap) connected

Serial Number: 8383592EY7K, Date/Time: 1/25/2011 6:31:33 PM (correct)

Exhibit Details

Case ID: 201101001

Exhibit Reference: 0001

Acquisition Details

- ☒ /dev/rdisk0s1 (500.00MB)
- ☒ /dev/rdisk0s2 (14.64GB)

- ⊞ All Live Data
- □ Images
- □ Video
- □ Music
- □ Telephony Data
- □ PIM Data
- □ E-Mail Data
- □ Location Data
- □ Internet Data
- □ Captured Images
- □ Uploaded Images
- □ Application Data

Hashing Details

- ☒ MD5
- □ RIPEMD160
- ☒ SHA-1
- □ SHA-256

```
Timestamp              | Message
1/25/2011 1:31:16 PM   | Forensic Examiner: cmdLabs
1/25/2011 1:31:16 PM   | Forensic Workstation: IR
1/25/2011 1:31:16 PM   | Forensic Workstation IP: 127.0.0.1
1/25/2011 1:31:16 PM   | Operating System: Microsoft Windows NT 5.1.2600 Service Pack 3
1/25/2011 1:31:16 PM   | System Uptime: 00:10:47.5910000
1/25/2011 1:31:16 PM   | iXAM²® bootloader version 2.0.57 running on device
1/25/2011 1:31:17 PM   | iPhone 3G (n82ap) connected
1/25/2011 1:31:17 PM   | Device serial number is : 8383592EY7K
1/25/2011 1:31:17 PM   | Device IMEI is : 011742008011300
1/25/2011 1:31:17 PM   | Device ECID is : 000001449C090DCD
1/25/2011 1:31:17 PM   | iBoot Version is 636.66
1/25/2011 1:31:17 PM   | BootROM Version is iBoot-385.49
1/25/2011 1:31:17 PM   | Querying iPhone for time and date ...
1/25/2011 1:31:17 PM   | Device clock set to Tue Jan 25 18:31:33 2011
1/25/2011 1:31:17 PM   | Device clock is correct
1/25/2011 1:31:17 PM   | Checking partitions on device ...
1/25/2011 1:31:28 PM   | Partition /dev/rdisk0s1 registered
1/25/2011 1:31:48 PM   | Partition /dev/rdisk0s2 registered
1/25/2011 1:31:48 PM   | Software build is Northstar7D11.iPhoneOS
1/25/2011 1:31:48 PM   | Software version is 3.1.2
```

Device: iPhone 3G (8383592EY7K) | Disk: 152.29GB | Customer: CMD Labs (T. Maguire) | Build: External (Release) v2.0.5.1720 | HASP ID: 1770050135 | License Type: Perpetual

FIGURE 20.16

Acquisition of iPhone using IXam.

20.4.2 Software Agents

Some forensic tools transfer and run an executable commonly called a *software agent* on the mobile device in order to acquire data from the device. Using a software agent has advantages from a forensic perspective because it provides a degree of trust and control over the process. However, if the software agent associated with a forensic tool cannot run on the evidential device, no data will be acquired. If specific files on a mobile device are inaccessible through the operating system, some important information will not be acquired. Finally, running a software agent on the device necessarily alters the device, potentially overwriting some data. However, in certain cases, the only available option may be to run a software agent in order to acquire data from a specific mobile device. Digital investigators must weigh these issues against the benefits of acquiring some information from a device. In addition, it may be necessary to explain that the acquired digital evidence is trustworthy despite any concerns raised by the use of a software agent on the device.

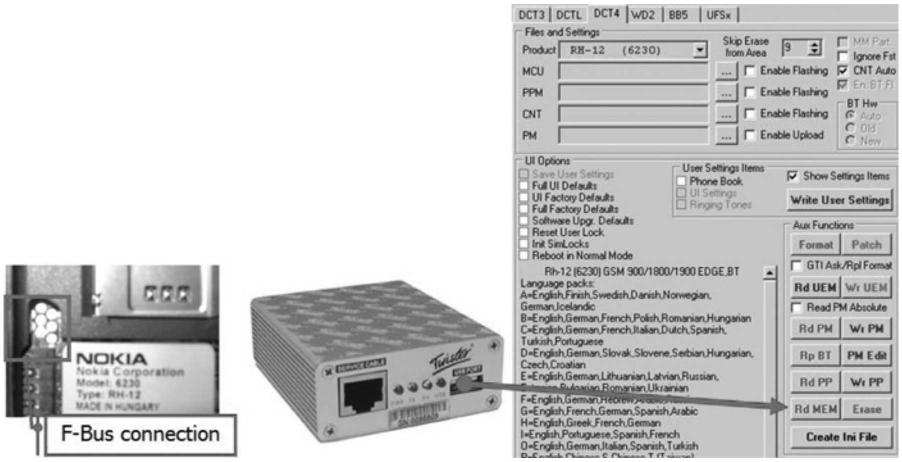
20.4.3 Bootloaders

When a mobile device is powered on, the first code it executes is called a *boot loader*. This code has very basic functionality and is comparable to the BIOS on Intel computers. During normal use of a mobile device, the boot loader simply launches the operating system to enable the user to interact with the device. However, the boot loader can be interrupted during the startup process to prevent the operating system from launching and can then be instructed to execute custom operations. In this way, forensic tools can use the boot loader to gain access to memory on a mobile device.

20.4.4 Flasher Boxes

Flasher boxes are devices originally designed to customize the appearance and operation of the operating system on mobile devices. However, by design, Flasher boxes can also dump the contents of physical memory from mobile devices.

The Twister Flasher box shown in Figure 20.17 can read the physical memory from a variety of mobile devices, including many Nokia models. The Twister box interfaces with many Nokia devices via gold-colored contacts on the circuit board, shown above left. Once the correct data cable is connected between the mobile device and Twister box, the Sarasoft software program shown in part above is used to read data from memory using the proprietary Nokia F-Bus protocol.



Product: RH-12 (6230)
Skip Erase from Area: 9
☐ MM Part
☐ Ignore Fst
☑ CNT Auto
☑ En. BT Fl.
BT Hw: ● Auto ○ Old ○ New
MCU ☐ Enable Flashing
PPM ☐ Enable Flashing
CNT ☐ Enable Flashing
PM ☐ Enable Upload
UI Options: ☐ Save User Settings ☐ Full UI Defaults ☐ UI Factory Defaults ☐ Full Factory Defaults ☐ Software Upgr. Defaults ☐ Reset User Lock ☐ Init SimLocks ☐ Reboot in Normal Mode
User Settings Items: ☐ Phone Book ☐ UI Settings ☐ Ringing Tones
☑ Show Settings Items
☐ GTI Ask/Rpl Format
☐ Read PM Absolute

Rh-12 (6230) GSM 900/1800/1900 EDGE,BT
Language packs:
A=English,Finish,Swedish,Danish,Norwegian,
German,Icelandic
B=English,German,French,Polish,Romanian,Hungarian
C=English,German,French,Italian,Dutch,Spanish,
Turkish,Portuguese
D=English,German,Slovak,Slovene,Serbian,Hungarian,
Czech,Croatian
E=English,German,Lithuanian,Latvian,Russian,
Estonian,Bulgarian,Romanian,Ukrainian
F=English,German,Hebrew,Arabic,
G=English,French,German,Spanish,Arabic
H=English,Greek,French,German
I=English,Portuguese,Spanish,French
O=English,German,Italian,Spanish,Turkish

FIGURE 20.17
Twister Flasher box can connect to FBUS interface on Nokia device to acquire data using the Sarasoft program.

20.4.5 JTAG

JTAG (Joint Action Test Group) refers to the IEEE 1149.1 standard (http://grouper.ieee.org/groups/1149/1/). The JTAG standard specifies an interface for standardized approaches to test integrated circuits, interconnections between components, and a means of observing and modifying circuit activity during a component's operation (Breeuwsma, 2006). It is a standard feature found in many mobile phones, as it provides manufacturers a low-level interface to the device that is not dependent on the operating system. However, the JTAG specifications for individual phones are not available outside the manufacturer. JTAG is of interest to forensic investigators and analysts, as it can theoretically provide direct access to a mobile phone's memory without any chance of altering it. However, the time and knowledge required to achieve this is substantial—not only requiring an understanding of JTAG for the specific model of phone, but also to reconstruct the resulting binary comprised of the device's memory structures. Despite the limitations in using JTAG as a forensic extraction mechanism, it provides the most common method of physical extraction. JTAG is common across multiple device manufacturers and there are multiple devices that extract memory structures through JTAG.

20.4.6 Chip off Extraction

Extracting the memory chips from a phone and reading them directly is by far the most exacting extraction method, but has the advantage of interfacing data in the most direct method. Chip extraction is the most low-level physical extraction method (Breeuwsma et al., 2007).

The output from chip extraction is forensically the cleanest, relying on no intermediate communications systems or on the device in any way. Reading the chip directly returns the memory structures for analysis. However, this approach suffers from the same issues as JTAG extraction, and will return only raw memory structures. Additionally, this is the most complex extraction method and has a failure rate associated. This approach is considered impractical in many situations where evidence may be returned, in cases where there is no guilt established or when prosecution does not occur.

Once extracted, extracted flash chips must be read to extract data. Device programmers are designed to write data to memory chips but can be used to extract data from the chips for forensic purposes. This acquisition method requires the mobile device to be dismantled and chip to be removed and is sometimes referred to as *chip off* processing. It is generally necessary to obtain a socket designed to connect a particular make of chip to the device programmer. There are several commercial device programmers available: Data I/O FlashPAK II (www.dataio.com), Xeltek SuperPro 5000 (http://www.xeltek.com), and BPM Microsystems (http://www.bpmmicro.com).

20.5 FORENSIC EXAMINATION AND ANALYSIS OF MOBILE DEVICES

The purpose of performing a forensic examination is to find and extract information related to an investigation, including deleted data. Whether data from a mobile device was acquired logically or physically, the general examination approach is the same as outlined in Chapter 6.

- Survey the available items to become familiar with the main sources of information on the mobile device.
- Recover any deleted items including files, SMS messages, call logs, and multimedia.
- Harvest metadata from active and recovered items such as date-time stamps, file names, and whether messages were read and calls were incoming, outgoing, or missed.
- Conduct a search and methodical inspection of the evidence, including keyword searches for any specific, known details related to the investigation.
- Perform temporal and relational analysis of information extracted from memory, including a timeline of events and link chart.
- Validate important results because even forensic tools have bugs.

When dealing with active data on a baseline mobile device, it may be possible to examine all of the acquired messages, call logs, calendar entries, and other items stored on the device. However, when the complete file system or a full physical memory dump was acquired from a mobile device, it is generally infeasible to examine every file or data fragment stored on the device. In such cases, digital investigators must develop a strategy to find relevant digital evidence. Surveying the acquired data by looking through folders and viewing the contents of files on a mobile device can lead to some useful items and may help with the development of a strategy, but this process is not a substitute for a methodical forensic examination. A strong forensic examination strategy should take into account what is known about the crime and the types of information that are being sought. For example, when there is a specific time period of interest in a case, examining all activities on the mobile device and reconstructing a timeline of events may be an effective strategy. As another example, when digital photographs are of interest in a case, an effective strategy to findings all relevant items on a mobile device may be to employ a combination of file system examination, keyword searching, and file carving.

20.5.1 File System Examination on Mobile Devices

All mobile devices have some form of file system, ranging from simple, proprietary one to more complex, standard ones. For instance, some Motorola and LG devices run the BREW (Binary Runtime Environment for Wireless) operating system developed by Qualcomm, which has its own file system. The file system on many CDMA devices can be viewed using BitPim as shown in Figure 20.18. However, using BitPim it may not be possible to view date-time stamps associated with files or acquire the entire file system for later examination using other tools. Commercial forensic tools such as Cellebrite can acquire the full logical file system from many mobile devices, including metadata such as date-time stamps.

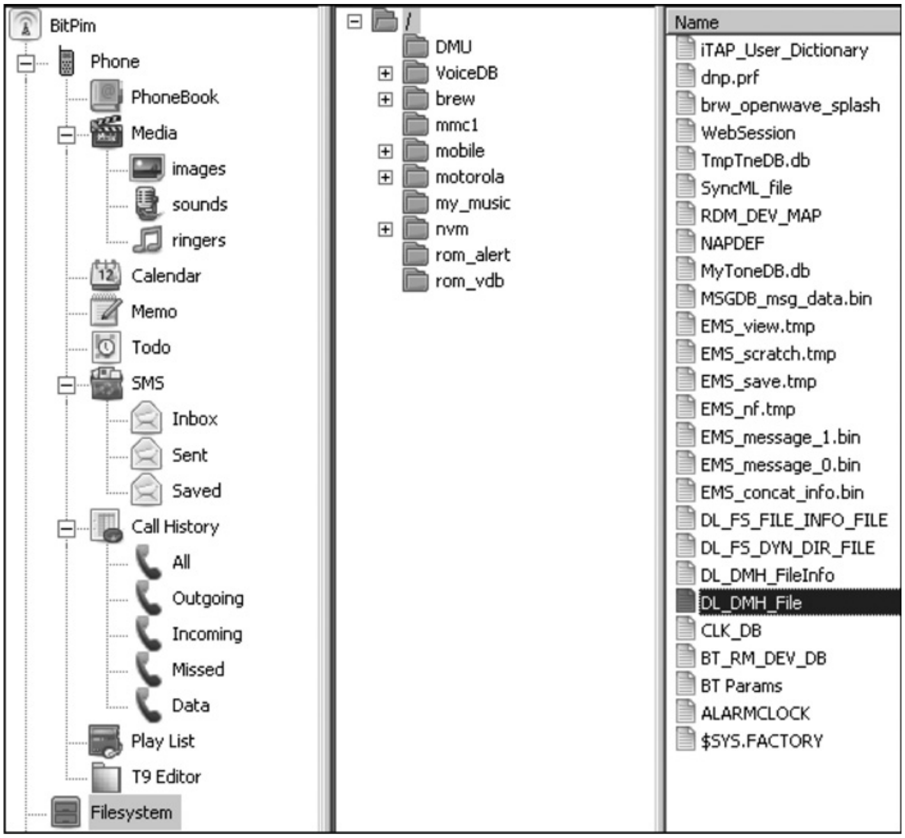
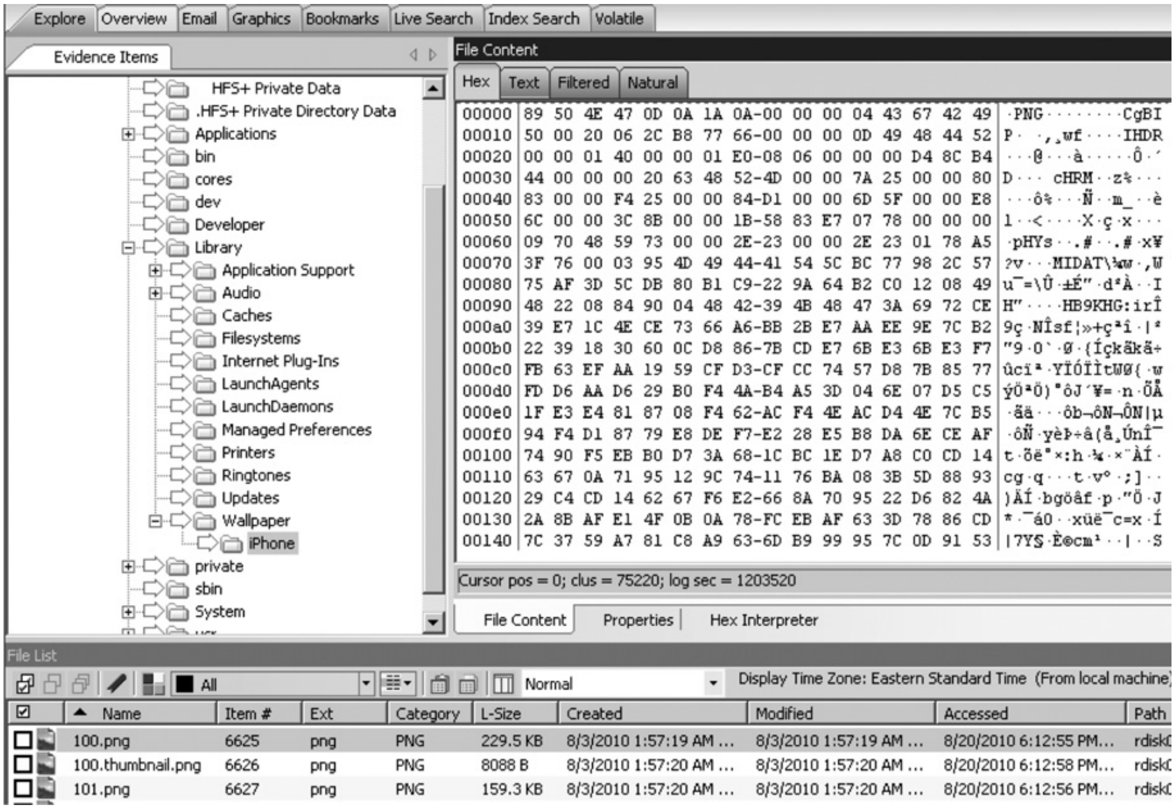


FIGURE 20.18
BitPim used to browse the file system on a Motorola CDMA device.

Some mobile devices use the FAT file system to arrange data in memory, others use Linux ext2/ext3 file systems, and iPhones use HFSX which is unique to Apple computer systems. As a result, it is often possible to perform a forensic analysis of a physical forensic duplicate of mobile devices using file system forensic tools such as those covered in Chapters 17, 18, and 19. Figure 20.19 shows a forensic duplicate of an iPhone being examined using FTK.



```
00000 89 50 4E 47 0D 0A 1A 0A-00 00 00 04 43 67 42 49 ·PNG········CgBI
00010 50 00 20 06 2C B8 77 66-00 00 00 0D 49 48 44 52 P· ·,¸wf····IHDR
00020 00 00 01 40 00 00 01 E0-08 06 00 00 00 D4 8C B4 ···@···à·····Ô·´
00030 44 00 00 00 20 63 48 52-4D 00 00 7A 25 00 00 80 D··· cHRM··z%···
00040 83 00 00 F4 25 00 00 84-D1 00 00 6D 5F 00 00 E8 ···ô%···Ñ··m_··è
00050 6C 00 00 3C 8B 00 00 1B-58 83 E7 07 78 00 00 00 l··<····X·ç·x···
00060 09 70 48 59 73 00 00 2E-23 00 00 2E 23 01 78 A5 ·pHYs··.#··.#·x¥
00070 3F 76 00 03 95 4D 49 44-41 54 5C BC 77 98 2C 57 ?v···MIDAT\¼w·,W
00080 75 AF 3D 5C DB 80 B1 C9-22 9A 64 B2 C0 12 08 49 u¯=\Û·±É"·d²À··I
00090 48 22 08 84 90 04 48 42-39 4B 48 47 3A 69 72 CE H"····HB9KHG:irÎ
000a0 39 E7 1C 4E CE 73 66 A6-BB 2B E7 AA EE 9E 7C B2 9ç·NÎsf¦»+çªî·|²
000b0 22 39 18 30 60 0C D8 86-7B CD E7 6B E3 6B E3 F7 "9·0`·Ø·{Íçkãkã÷
000c0 FB 63 EF AA 19 59 CF D3-CF CC 74 57 D8 7B 85 77 ûcïª·YÏÓÏÌtWØ{·w
000d0 FD D6 AA D6 29 B0 F4 4A-B4 A5 3D 04 6E 07 D5 C5 ýÖªÖ)°ôJ´¥=·n·ÕÅ
000e0 1F E3 E4 81 87 08 F4 62-AC F4 4E AC D4 4E 7C B5 ·ãä···ôb¬ôN¬ÔN|µ
000f0 94 F4 D1 87 79 E8 DE F7-E2 28 E5 B8 DA 6E CE AF ·ôÑ·yèÞ÷â(å¸ÚnÎ¯
00100 74 90 F5 EB B0 D7 3A 68-1C BC 1E D7 A8 C0 CD 14 t·õë°×:h·¼·×¨ÀÍ·
00110 63 67 0A 71 95 12 9C 74-11 76 BA 08 3B 5D 88 93 cg·q···t·vº·;]··
00120 29 C4 CD 14 62 67 F6 E2-66 8A 70 95 22 D6 82 4A )ÄÍ·bgöâf·p·"Ö·J
00130 2A 8B AF E1 4F 0B 0A 78-FC EB AF 63 3D 78 86 CD *·¯áO··xüë¯c=x·Í
00140 7C 37 59 A7 81 C8 A9 63-6D B9 99 95 7C 0D 91 53 |7Y§·È©cm¹··|··S
```

Cursor pos = 0; clus = 75220; log sec = 1203520

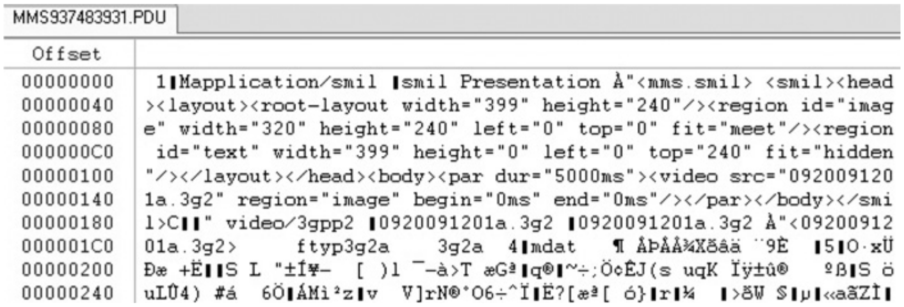
Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Item #	Ext	Category	L-Size	Created	Modified	Accessed	Path
□	100.png	6625	png	PNG	229.5 KB	8/3/2010 1:57:19 AM ...	8/3/2010 1:57:19 AM ...	8/20/2010 6:12:55 PM...	rdisk(
□	100.thumbnail.png	6626	png	PNG	8088 B	8/3/2010 1:57:20 AM ...	8/3/2010 1:57:20 AM ...	8/20/2010 6:12:58 PM...	rdisk(
□	101.png	6627	png	PNG	159.3 KB	8/3/2010 1:57:20 AM ...	8/3/2010 1:57:20 AM ...	8/20/2010 6:12:56 PM...	rdisk(

FIGURE 20.19
Examination of iPhone physical forensic duplicate using FTK.

Even when a full copy of physical memory is not possible, for many devices the complete logical file system can be acquired. Although this generally does not include deleted items, it can still provide access to substantial digital evidence including MMS messages, IM fragments, and Web browsing history that are not displayed automatically by forensic tools. In such situations, the forensic examiners must locate the desired information within the file system and interpret it themselves. This is one of the main reasons why it is important for practitioners to have an understanding of the underlying technology and not be overly reliant on automated tools.

As an example, Figure 20.20 shows a file named "MMS937483931.PDU" that was extracted from the file system of an LG mobile device. This file contains an MMS message with a video that can be recovered even after the original video file was deleted from the device. These MMS files start with an SMIL header that includes the name of the attached file, followed by the actual content of the attachment (Casey, 2009).



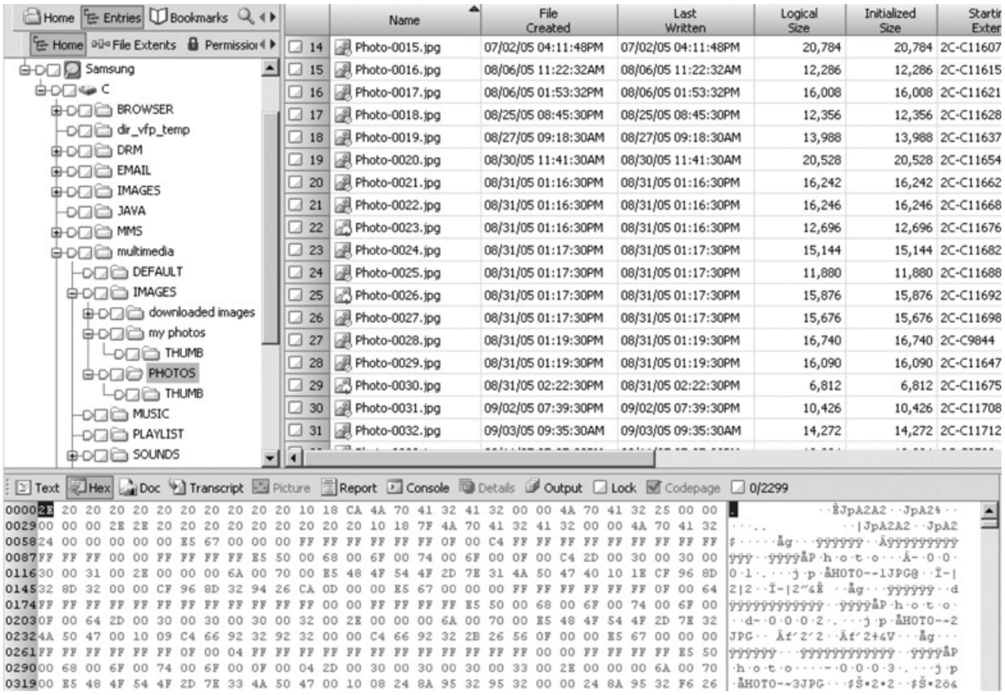
```
MMS937483931.PDU

 Offset
00000000   1▮Mapplication/smil ▮smil Presentation Å"<mms.smil> <smil><head
00000040  ><layout><root-layout width="399" height="240"/><region id="imag
00000080  e" width="320" height="240" left="0" top="0" fit="meet"/><region
000000C0   id="text" width="399" height="0" left="0" top="240" fit="hidden
00000100  "/></layout></head><body><par dur="5000ms"><video src="092009120
00000140  1a.3g2" region="image" begin="0ms" end="0ms"/></par></body></smi
00000180  l>C▮▮" video/3gpp2 ▮0920091201a.3g2 ▮0920091201a.3g2 Å"<09200912
000001C0  01a.3g2>     ftyp3g2a    3g2a  4▮mdat   ¶ ÅÞÅÅ¾Xõåä ¨9È  ▮5▮O·xÛ
00000200  Ðæ +Ë▮▮S L "±Î¥–  [ )l ¯–à>T æGª▮q®▮~÷;Ö¢ÊJ(s uqK Ïý±û®   ºß▮S ö
00000240  uLÛ4) #á  6Ö▮ÁMì²z▮v  V]rN®˚O6÷^Ï▮Ë?[æª[ ó}▮r▮¼  ▮>õW S▮µ▮«aãZÌ▮
```

FIGURE 20.20

File from an LG mobile device containing an MMS message with a video attachment that can be recovered even after the original video has been deleted from the file system.

20.5.2 Data Recovery on Mobile Devices

When common file systems are used such as FAT, HFS, and ext2/3, it may be possible to recover deleted files using file system forensic tools as discussed in Chapters 17, 18, and 19. For instance, Figure 20.21 shows EnCase being used to recover deleted photographs from a FAT file system on a Samsung mobile device.



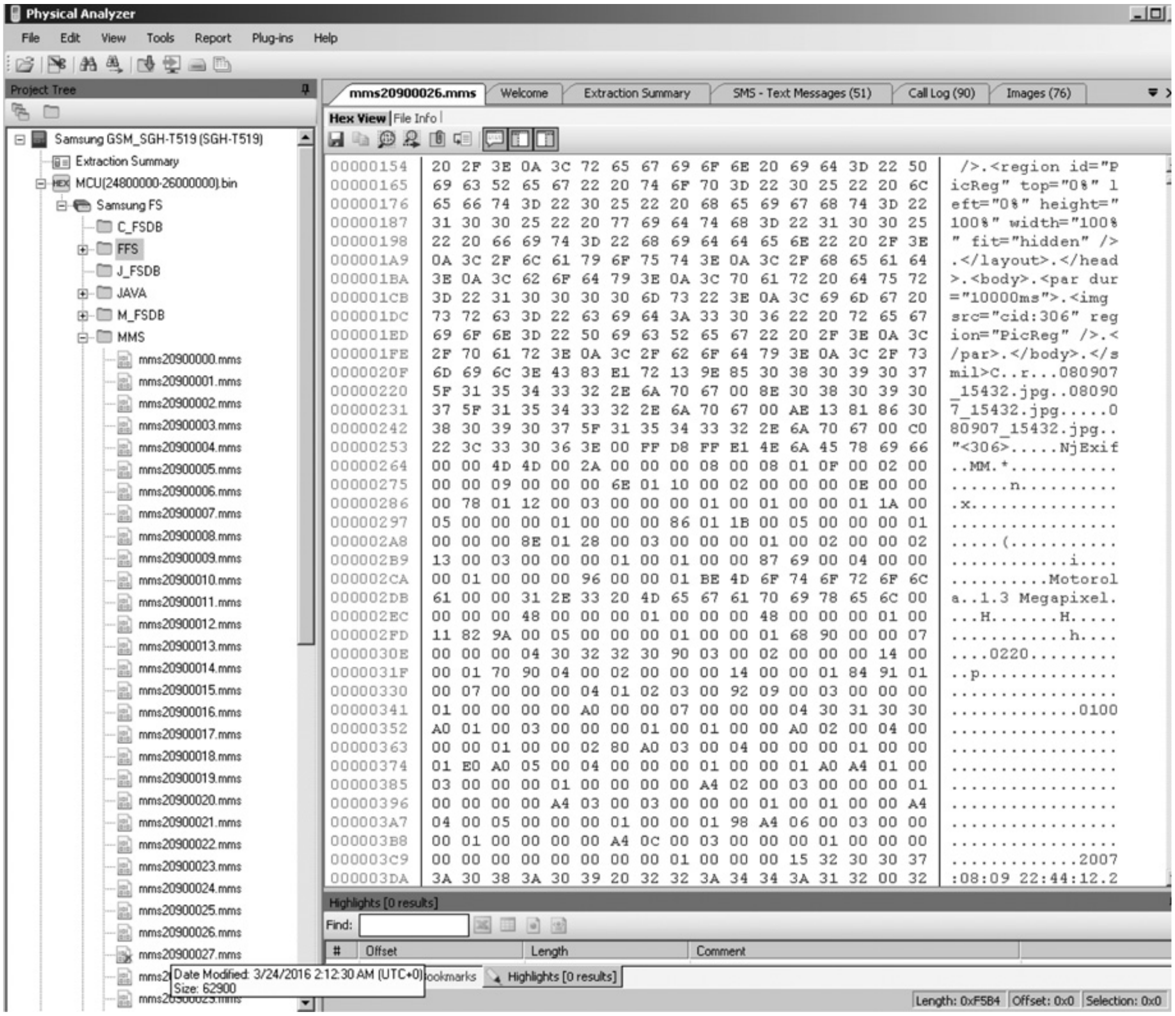
	Name	File Created	Last Written	Logical Size	Initialized Size	Startir Exter
□ 14	Photo-0015.jpg	07/02/05 04:11:48PM	07/02/05 04:11:48PM	20,784	20,784	2C-C11607
□ 15	Photo-0016.jpg	08/06/05 11:22:32AM	08/06/05 11:22:32AM	12,286	12,286	2C-C11615
□ 16	Photo-0017.jpg	08/06/05 01:53:32PM	08/06/05 01:53:32PM	16,008	16,008	2C-C11621
□ 17	Photo-0018.jpg	08/25/05 08:45:30PM	08/25/05 08:45:30PM	12,356	12,356	2C-C11628
□ 18	Photo-0019.jpg	08/27/05 09:18:30AM	08/27/05 09:18:30AM	13,988	13,988	2C-C11637
□ 19	Photo-0020.jpg	08/30/05 11:41:30AM	08/30/05 11:41:30AM	20,528	20,528	2C-C11654
□ 20	Photo-0021.jpg	08/31/05 01:16:30PM	08/31/05 01:16:30PM	16,242	16,242	2C-C11662
□ 21	Photo-0022.jpg	08/31/05 01:16:30PM	08/31/05 01:16:30PM	16,246	16,246	2C-C11668
□ 22	Photo-0023.jpg	08/31/05 01:16:30PM	08/31/05 01:16:30PM	12,696	12,696	2C-C11676
□ 23	Photo-0024.jpg	08/31/05 01:17:30PM	08/31/05 01:17:30PM	15,144	15,144	2C-C11682
□ 24	Photo-0025.jpg	08/31/05 01:17:30PM	08/31/05 01:17:30PM	11,880	11,880	2C-C11688
□ 25	Photo-0026.jpg	08/31/05 01:17:30PM	08/31/05 01:17:30PM	15,876	15,876	2C-C11692
□ 26	Photo-0027.jpg	08/31/05 01:17:30PM	08/31/05 01:17:30PM	15,676	15,676	2C-C11698
□ 27	Photo-0028.jpg	08/31/05 01:19:30PM	08/31/05 01:19:30PM	16,740	16,740	2C-C9844
□ 28	Photo-0029.jpg	08/31/05 01:19:30PM	08/31/05 01:19:30PM	16,090	16,090	2C-C11647
□ 29	Photo-0030.jpg	08/31/05 02:22:30PM	08/31/05 02:22:30PM	6,812	6,812	2C-C11675
□ 30	Photo-0031.jpg	09/02/05 07:39:30PM	09/02/05 07:39:30PM	10,426	10,426	2C-C11708
□ 31	Photo-0032.jpg	09/03/05 09:35:30AM	09/03/05 09:35:30AM	14,272	14,272	2C-C11712

```
00002E 20 20 20 20 20 20 20 20 20 20 10 18 CA 4A 70 41 32 41 32 00 00 4A 70 41 32 25 00 00 ▮           ··ÊJpA2A2··JpA2%··
002900 00 00 2E 2E 20 20 20 20 20 20 20 20 20 10 18 7F 4A 70 41 32 41 32 00 00 4A 70 41 32 ···..         ··|JpA2A2··JpA2
005824 00 00 00 00 00 E5 67 00 00 00 FF FF FF FF FF FF 0F 00 C4 FF FF FF FF FF FF FF FF FF $·····åg···ÿÿÿÿÿÿ··Äÿÿÿÿÿÿÿÿÿ
0087FF FF FF 00 00 FF FF FF FF E5 50 00 68 00 6F 00 74 00 6F 00 0F 00 C4 2D 00 30 00 30 00 ÿÿÿ··ÿÿÿÿåP·h·o·t·o···Ä-·0·0·
011630 00 31 00 2E 00 00 00 6A 00 70 00 E5 48 4F 54 4F 2D 7E 31 4A 50 47 40 10 1E CF 96 8D 0·1·.···j·p·åHOTO-~1JPG@··Ï–|
014532 8D 32 00 00 CF 96 8D 32 94 26 CA 0D 00 00 E5 67 00 00 00 FF FF FF FF FF FF 0F 00 64 2|2··Ï–|2″&Ê··åg···ÿÿÿÿÿÿ··d
0174FF FF FF FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF E5 50 00 68 00 6F 00 74 00 6F 00 ÿÿÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿåP·h·o·t·o·
02030F 00 64 2D 00 30 00 30 00 30 00 32 00 2E 00 00 00 6A 00 70 00 E5 48 4F 54 4F 2D 7E 32 ··d-·0·0·0·2·.···j·p·åHOTO-~2
02324A 50 47 00 10 09 C4 66 92 32 92 32 00 00 C4 66 92 32 2B 26 56 0F 00 00 E5 67 00 00 00 JPG··Äf′2′2··Äf′2+&V···åg···
0261FF FF FF FF FF FF 0F 00 04 FF FF FF FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF E5 50 ÿÿÿÿÿÿ···ÿÿÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿåP
029000 68 00 6F 00 74 00 6F 00 0F 00 04 2D 00 30 00 30 00 30 00 33 00 2E 00 00 00 6A 00 70 ·h·o·t·o····-·0·0·0·3·.···j·p
031900 E5 48 4F 54 4F 2D 7E 33 4A 50 47 00 10 08 24 8A 95 32 95 32 00 00 24 8A 95 32 F6 26 ·åHOTO-~3JPG···$Š•2•2··$Š•2ö&
```

FIGURE 20.21

Deleted photographs recovered from the reconstructed FAT file system in a physical memory dump of a Samsung mobile device.

In addition, items such as MMS messages that have been deleted may be recoverable as shown in Figure 20.22 using Cellebrite Physical. The deleted file containing an MMS message is marked with an "X" in the bottom left of the screen, and the contents of these files can be viewed as shown on the right of the screen. As seen in the previous section, these MMS files start with an SMIL header that includes the name of the attached file, followed by the actual content of the attachment.



```
00000154  20 2F 3E 0A 3C 72 65 67 69 6F 6E 20 69 64 3D 22 50   />.<region id="P
00000165  69 63 52 65 67 22 20 74 6F 70 3D 22 30 25 22 20 6C  icReg" top="0%" l
00000176  65 66 74 3D 22 30 25 22 20 68 65 69 67 68 74 3D 22  eft="0%" height="
00000187  31 30 30 25 22 20 77 69 64 74 68 3D 22 31 30 30 25  100%" width="100%
00000198  22 20 66 69 74 3D 22 68 69 64 64 65 6E 22 20 2F 3E  " fit="hidden" />
000001A9  0A 3C 2F 6C 61 79 6F 75 74 3E 0A 3C 2F 68 65 61 64  .</layout>.</head
000001BA  3E 0A 3C 62 6F 64 79 3E 0A 3C 70 61 72 20 64 75 72  >.<body>.<par dur
000001CB  3D 22 31 30 30 30 30 6D 73 22 3E 0A 3C 69 6D 67 20  ="10000ms">.<img
000001DC  73 72 63 3D 22 63 69 64 3A 33 30 36 22 20 72 65 67  src="cid:306" reg
000001ED  69 6F 6E 3D 22 50 69 63 52 65 67 22 20 2F 3E 0A 3C  ion="PicReg" />.<
000001FE  2F 70 61 72 3E 0A 3C 2F 62 6F 64 79 3E 0A 3C 2F 73  /par>.</body>.</s
0000020F  6D 69 6C 3E 43 83 E1 72 13 9E 85 30 38 30 39 30 37  mil>C..r...080907
00000220  5F 31 35 34 33 32 2E 6A 70 67 00 8E 30 38 30 39 30  _15432.jpg..08090
00000231  37 5F 31 35 34 33 32 2E 6A 70 67 00 AE 13 81 86 30  7_15432.jpg.....0
00000242  38 30 39 30 37 5F 31 35 34 33 32 2E 6A 70 67 00 C0  80907_15432.jpg..
00000253  22 3C 33 30 36 3E 00 FF D8 FF E1 4E 6A 45 78 69 66  "<306>.....NjExif
00000264  00 00 4D 4D 00 2A 00 00 00 08 00 08 01 0F 00 02 00  ..MM.*...........
00000275  00 00 09 00 00 00 6E 01 10 00 02 00 00 00 0E 00 00  ......n..........
00000286  00 78 01 12 00 03 00 00 00 01 00 01 00 00 01 1A 00  .x...............
00000297  05 00 00 00 01 00 00 00 86 01 1B 00 05 00 00 00 01  .................
000002A8  00 00 00 8E 01 28 00 03 00 00 00 01 00 02 00 00 02  .....(...........
000002B9  13 00 03 00 00 00 01 00 01 00 00 87 69 00 04 00 00  ............i....
000002CA  00 01 00 00 00 96 00 00 01 BE 4D 6F 74 6F 72 6F 6C  ..........Motorol
000002DB  61 00 00 31 2E 33 20 4D 65 67 61 70 69 78 65 6C 00  a..1.3 Megapixel.
000002EC  00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 00  ...H.......H.....
000002FD  11 82 9A 00 05 00 00 00 01 00 00 01 68 90 00 00 07  ............h....
0000030E  00 00 00 04 30 32 32 30 90 03 00 02 00 00 00 14 00  ....0220.........
0000031F  00 01 70 90 04 00 02 00 00 00 14 00 00 01 84 91 01  ..p..............
00000330  00 07 00 00 00 04 01 02 03 00 92 09 00 03 00 00 00  .................
00000341  01 00 00 00 00 A0 00 00 07 00 00 00 04 30 31 30 30  .............0100
00000352  A0 01 00 03 00 00 00 01 00 01 00 00 A0 02 00 04 00  .................
00000363  00 00 01 00 00 02 80 A0 03 00 04 00 00 00 01 00 00  .................
00000374  01 E0 A0 05 00 04 00 00 00 01 00 00 01 A0 A4 01 00  .................
00000385  03 00 00 00 01 00 00 00 00 A4 02 00 03 00 00 00 01  .................
00000396  00 00 00 00 A4 03 00 03 00 00 00 01 00 01 00 00 A4  .................
000003A7  04 00 05 00 00 00 01 00 00 01 98 A4 06 00 03 00 00  .................
000003B8  00 01 00 00 00 00 A4 0C 00 03 00 00 00 01 00 00 00  .................
000003C9  00 00 00 00 00 00 00 00 01 00 00 00 15 32 30 30 37  .............2007
000003DA  3A 30 38 3A 30 39 20 32 32 3A 34 34 3A 31 32 00 32  :08:09 22:44:12.2
```

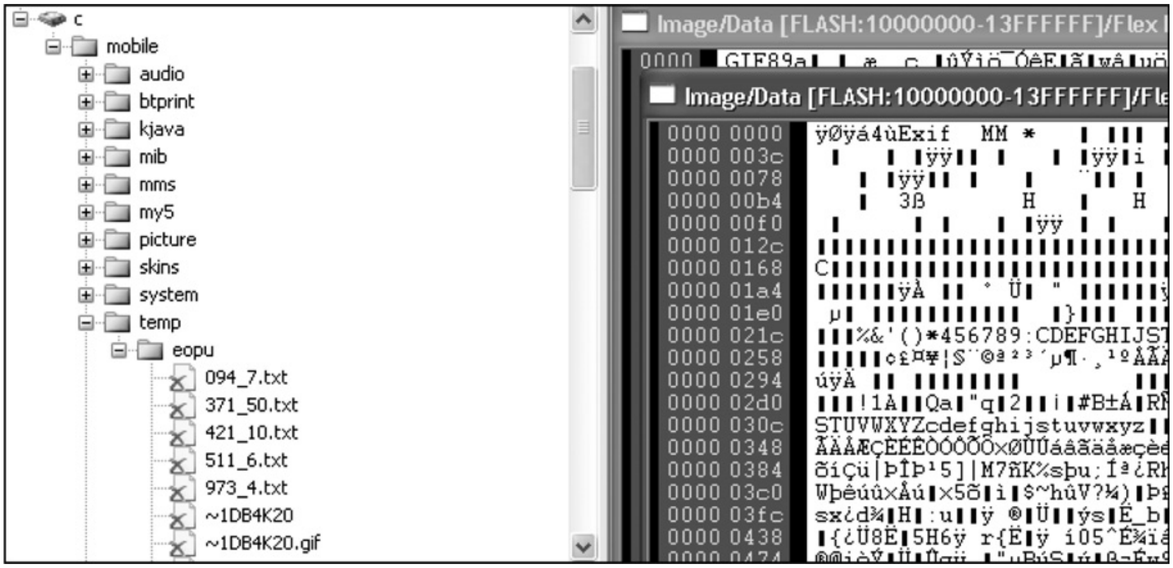
Date Modified: 3/24/2016 2:12:30 AM (UTC+0)
Size: 62900

Length: 0xF5B4 Offset: 0x0 Selection: 0x0

FIGURE 20.22

Deleted MMS message being recovered from a physical memory dump of a Samsung device using Cellebrite Physical.

As another example of how deleted files can be useful in a forensic context, when files are opened on some Motorola mobile devices a temporary artifact is created and subsequently deleted. If such items can be recovered as shown in Figure 20.23, they can contain information that is no longer present elsewhere on the mobile device and they can provide evidence that particular information was viewed on the device.



```
⊟ c
  ⊟ mobile
    ⊞ audio
    ⊞ btprint
    ⊞ kjava
    ⊞ mib
    ⊞ mms
    ⊞ my5
    ⊞ picture
    ⊞ skins
    ⊞ system
    ⊟ temp
      ⊟ eopu
          094_7.txt
          371_50.txt
          421_10.txt
          511_6.txt
          973_4.txt
          ~1DB4K20
          ~1DB4K20.gif
```

Image/Data [FLASH:10000000-13FFFFFF]/Flex

```
0000   GIF89a▮ ▮ æ  c ▮ûÝìö¯ÓêE▮ã▮wâ▮uö
```

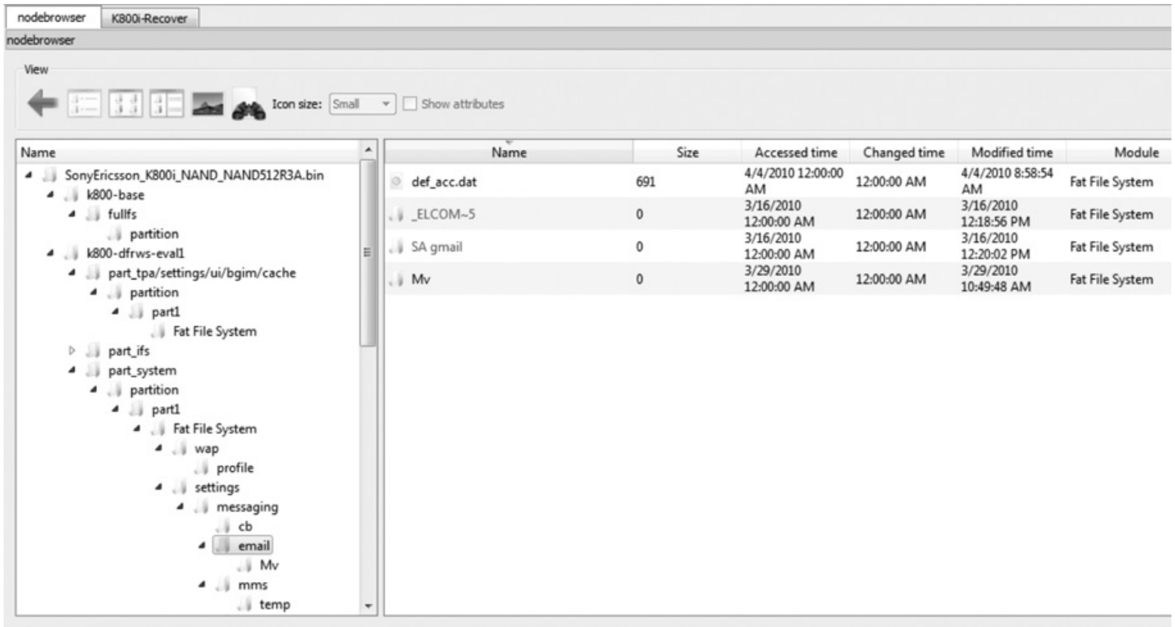
Image/Data [FLASH:10000000-13FFFFFF]/Fle

```
0000 0000   ÿØÿá4ùExif   MM *    ▮ ▮▮▮ ▮
0000 003c    ▮    ▮ ▮ÿÿ▮▮ ▮    ▮ ▮ÿÿ▮i ▮
0000 0078      ▮ ▮ÿÿ▮▮ ▮    ▮    ¨▮▮ ▮
0000 00b4      ▮  3ß        H    ▮    H
0000 00f0    ▮      ▮ ▮    ▮ ▮ÿÿ ▮ ▮   ▮
0000 012c   ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮
0000 0168   C▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮
0000 01a4   ▮▮▮▮▮▮ÿÀ ▮▮  ˚ Ü▮ " ▮▮▮▮▮▮ÿ
0000 01e0    µ▮ ▮▮▮▮▮▮▮▮▮▮▮   ▮}▮▮▮ ▮▮▮
0000 021c   ▮▮▮%&'()*456789:CDEFGHIJST
0000 0258   ▮▮▮▮▮¢£¤¥¦§¨©ª²³´µ¶·¸¹ºÂÃÄ
0000 0294   úÿÄ ▮▮ ▮▮▮▮▮▮▮▮▮          ▮▮▮
0000 02d0   ▮▮▮!1A▮▮Qa▮"q▮2▮▮i▮#B±Á▮RÑ
0000 030c   STUVWXYZcdefghijstuvwxyz▮▮
0000 0348   ÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèé
0000 0384   õíÇü|ÞÎÞ¹5]|M7ñK%sþu;Í ª¿RH
0000 03c0   WþêúûxÅú▮×5õ▮i▮$~hûV?¼)▮Þ
0000 03fc   sx¿d¾▮H▮:u▮▮ÿ ®▮Ü▮▮ýs▮É_b▮
0000 0438   ▮{¿Ü8Ë▮5H6ÿ r{Ë▮ÿ í05^É¾iá
0000 0474   ®@iòÝ▮Ü▮Ûgü ▮"µBúS▮ú▮ß-Éw
```

FIGURE 20.23

Deleted file being recovered from a Motorola device using XACT.

The abstraction layers and wear-leveling associated with Flash memory can make data recovery from mobile devices more difficult, but advances are being made in both commercial and open source forensic tools. For instance, the winning submission for the DFRWS2010 Forensic Challenge provides a technical analysis of data structures found in memory dump from a Sony Ericsson K800i mobile device (www.dfrws.org). The Digital Forensic Framework plug-in that was developed in this submission to recover wear-leveling tables enables a forensic analyst to reconstruct the most recent flash abstraction layer, as well as past states of the device if they still exist in memory. Once the desired state of memory has been reconstructed, the DFF tool can be used to view various states of the file system, including metadata associated with files, folders, and deleted items as shown in Figure 20.24.



```
Name
SonyEricsson_K800i_NAND_NAND512R3A.bin
  k800-base
    fullfs
      partition
  k800-dfrws-eval1
    part_tpa/settings/ui/bgim/cache
      partition
        part1
          Fat File System
    part_ifs
    part_system
      partition
        part1
          Fat File System
            wap
              profile
            settings
              messaging
                cb
                email
                  Mv
                mms
                  temp
```

Name	Size	Accessed time	Changed time	Modified time	Module
def_acc.dat	691	4/4/2010 12:00:00 AM	12:00:00 AM	4/4/2010 8:58:54 AM	Fat File System
_ELCOM~5	0	3/16/2010 12:00:00 AM	12:00:00 AM	3/16/2010 12:18:56 PM	Fat File System
SA gmail	0	3/16/2010 12:00:00 AM	12:00:00 AM	3/16/2010 12:20:02 PM	Fat File System
Mv	0	3/29/2010 12:00:00 AM	12:00:00 AM	3/29/2010 10:49:48 AM	Fat File System

FIGURE 20.24

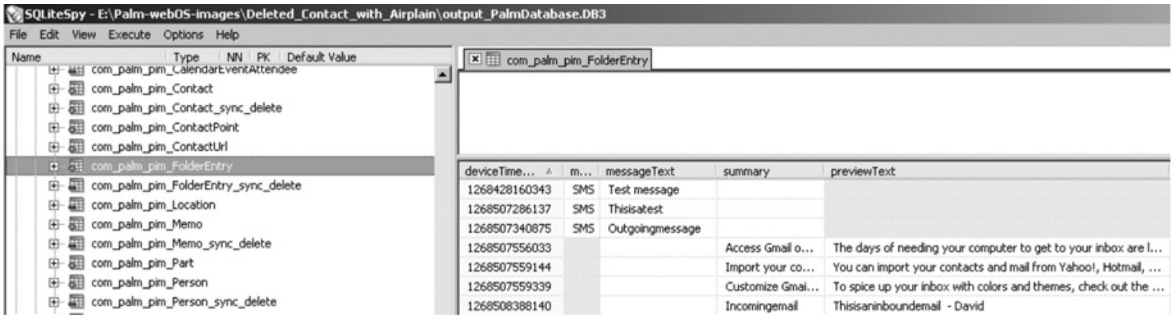
File system, including deleted items, reconstructed from a physical memory dump of a Sony Ericsson mobile device using DFF.

PRACTITIONER'S TIP

Tool Validation

Given the complexity of recovering deleted items from Flash memory of mobile devices, it is generally advisable to validate important results. There are various approaches to validating results, including performing a manual examination and comparing the results of logical and physical acquisitions.

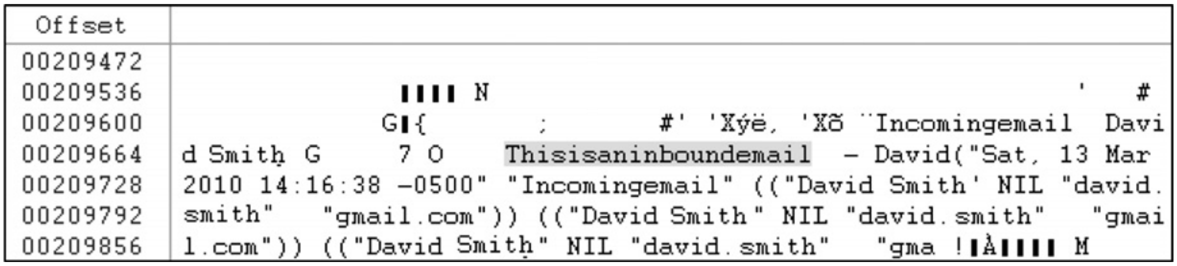
Many smart phones use SQLite databases to store information, including iPhone, Android, and Palm. Figure 20.25 shows the contents of a SQLite database from a Palm device running webOS. Even after items have been deleted from a smart phone, the contents may still exist in the SQLite database file. Although the deleted entry may not be visible using a SQLite browser, it can be recovered by examining the database file in a hexadecimal viewer (Reference Casey E, Cheval A, Lee JY, Oxley D, Song YJ (2011), "Forensic Acquisition and Analysis of Palm webOS on Mobile Devices," Digital Investigation (in press)).


SQLiteSpy - E:\Palm-webOS-images\Deleted_Contact_with_Airplain\output_PalmDatabase.DB3
File Edit View Execute Options Help
Name Type NN PK Default Value
com_palm_pim_CalendarEventAttendee
com_palm_pim_Contact
com_palm_pim_Contact_sync_delete
com_palm_pim_ContactPoint
com_palm_pim_ContactUrl
com_palm_pim_FolderEntry
com_palm_pim_FolderEntry_sync_delete
com_palm_pim_Location
com_palm_pim_Memo
com_palm_pim_Memo_sync_delete
com_palm_pim_Part
com_palm_pim_Person
com_palm_pim_Person_sync_delete
com_palm_pim_FolderEntry

deviceTime...	m...	messageText	summary	previewText
1268428160343	SMS	Test message		
1268507286137	SMS	Thisisatest		
1268507340875	SMS	Outgoingmessage		
1268507556033			Access Gmail o...	The days of needing your computer to get to your inbox are l...
1268507559144			Import your co...	You can import your contacts and mail from Yahoo!, Hotmail, ...
1268507559339			Customize Gmai...	To spice up your inbox with colors and themes, check out the ...
1268508388140			Incomingemail	Thisisaninboundemail - David

FIGURE 20.25A

Records in a SQLite database viewed with browser.



```
Offset
00209472
00209536              ▌▌▌▌ N                                   '   #
00209600             G▌{       ;       #' 'Xýë, 'Xõ ¨Incomingemail  Davi
00209664 d Smith G     7 O    Thisisaninboundemail  - David("Sat, 13 Mar
00209728 2010 14:16:38 -0500" "Incomingemail" (("David Smith' NIL "david.
00209792 smith"   "gmail.com")) (("David Smith" NIL "david.smith"   "gmai
00209856 l.com")) (("David Smith" NIL "david.smith"   "gma !▌À▌▌▌▌ M
```

FIGURE 20.25B

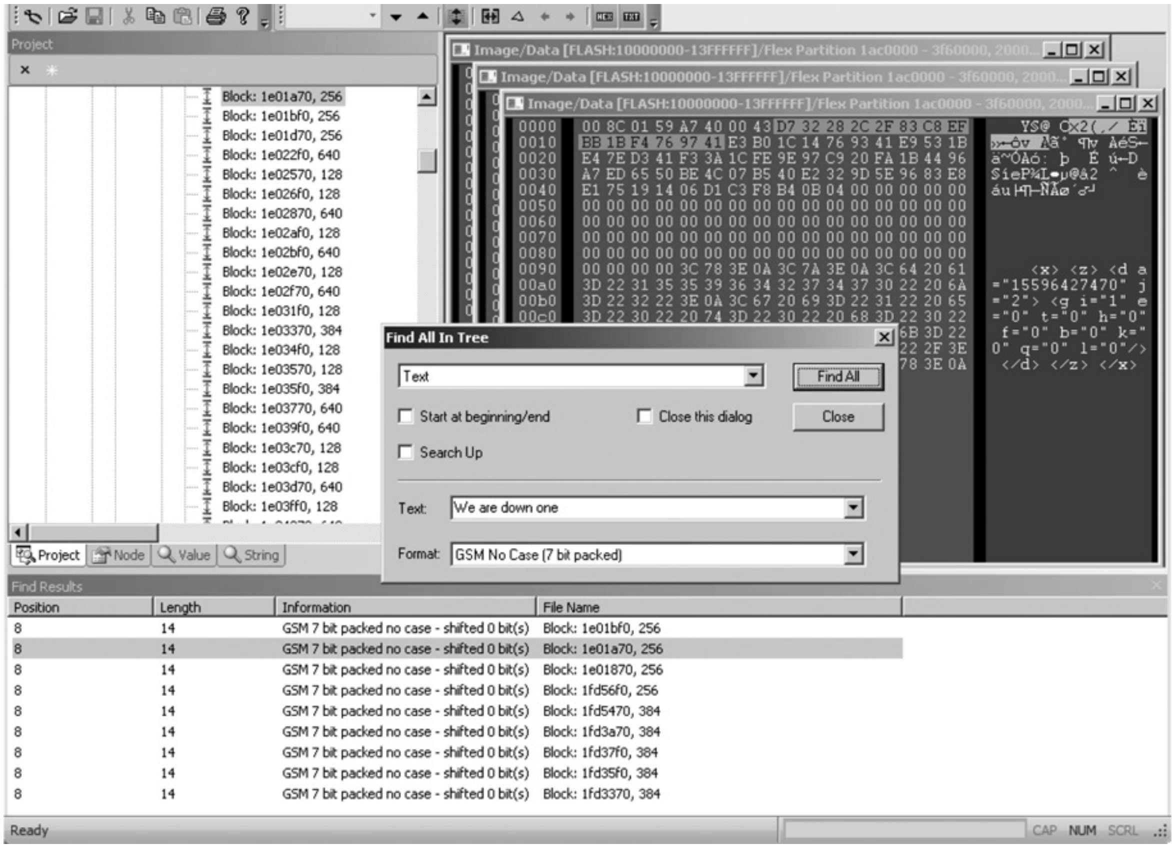
Raw record data in SQLite database viewed using a hex viewer.

Some mobile devices use proprietary file formats to store information, and these may contain deleted data similar to that described in SQLite databases. For instance, Windows Mobile devices store communications in a Microsoft proprietary embedded database named cemail.vol, which can retain deleted items (Casey, Bann, & Doyle, 2009).

20.5.3 Data Formats on Mobile Devices

Mobile devices store data in a variety of formats. In order to interpret data on mobile devices and verify important results at a low level, digital forensic investigators require some understanding of these formats. In addition to understanding binary and hexadecimal numbers, practitioners must be intimately familiar with how these numbers correspond with ASCII and Unicode characters as discussed in Chapter 15.

A peculiarity of mobile devices is that they store SMS messages not in ASCII but using a 7-bit alphabet. For instance, Figure 20.26 shows the results of a keyword search for a specific deleted SMS message in physical memory acquired from a Motorola Z3 device. The SMS message contained the text "We are down one" and multiple copies were found in the memory dump, as shown in the bottom panel of the above screenshot. Observe that the keyword search had to be performed using 7-bit encoding and that the text of the message is not visible in readable form when viewed using a hex viewer (see highlighted data in top right corner of Figure 20.26).



Block: 1e01a70, 256
Block: 1e01bf0, 256
Block: 1e01d70, 256
Block: 1e022f0, 640
Block: 1e02570, 128
Block: 1e026f0, 128
Block: 1e02870, 640
Block: 1e02af0, 128
Block: 1e02bf0, 640
Block: 1e02e70, 128
Block: 1e02f70, 640
Block: 1e031f0, 128
Block: 1e03370, 384
Block: 1e034f0, 128
Block: 1e03570, 128
Block: 1e035f0, 384
Block: 1e03770, 640
Block: 1e039f0, 640
Block: 1e03c70, 128
Block: 1e03cf0, 128
Block: 1e03d70, 640
Block: 1e03ff0, 128

Image/Data [FLASH:10000000-13FFFFFF]/Flex Partition 1ac0000 - 3f60000, 2000...

```
0000  00 8C 01 59 A7 40 00 43 D7 32 28 2C 2F 83 C8 EF    YS@ Cx2(,/ Èï
0010  BB 1B F4 76 97 41 E3 B0 1C 14 76 93 41 E9 53 1B  »←ôv Aã° ¶v AéS←
0020  E4 7E D3 41 F3 3A 1C FE 9E 97 C9 20 FA 1B 44 96  ä~ÓAó: þ  É ú←D
0030  A7 ED 65 50 BE 4C 07 B5 40 E2 32 9D 5E 96 83 E8  §íeP¾L•µ@â2 ^  è
0040  E1 75 19 14 06 D1 C3 F8 B4 0B 04 00 00 00 00 00  áu   ÑÃø´
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090  00 00 00 00 3C 78 3E 0A 3C 7A 3E 0A 3C 64 20 61      <x> <z> <d a
00a0  3D 22 31 35 35 39 36 34 32 37 34 37 30 22 20 6A  ="15596427470" j
00b0  3D 22 32 22 3E 0A 3C 67 20 69 3D 22 31 22 20 65  ="2"> <g i="1" e
00c0  3D 22 30 22 20 74 3D 22 30 22 20 68 3D 22 30 22  ="0" t="0" h="0"
                                        6B 3D 22   f="0" b="0" k="
                                        22 2F 3E  0" q="0" l="0"/>
                                        78 3E 0A   </d> </z> </x>
```

Text

☐ Start at beginning/end ☐ Close this dialog

☐ Search Up

Text: We are down one

Format: GSM No Case (7 bit packed)

Find Results

Position	Length	Information	File Name
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1e01bf0, 256
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1e01a70, 256
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1e01870, 256
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1fd56f0, 256
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1fd5470, 384
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1fd3a70, 384
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1fd37f0, 384
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1fd35f0, 384
8	14	GSM 7 bit packed no case - shifted 0 bit(s)	Block: 1fd3370, 384

FIGURE 20.26

Deleted SMS messages recovered from physical memory dump of Motorola Z3 device by keyword searching for a 7-bit encoded string.

Certain data on mobile devices, particularly phone numbers, are stored in nibble reversed format. This means that each byte in the number is stored in reverse order. For instance, the phone number 12036452774 is 2130462577F4 in nibble reversed format (where the F is padding).

To complicate matters, some mobile devices (e.g., Motorola) store some data in big-endian format, with the most significant bit first. This basically means that the entire data structure is stored in the opposite order than on a little-endian system. For instance, a little-endian UNIX date-time stamp C7 BE FE 49, which equates to May 4, 2009, at 10:09:11 AM, would be stored as 49 FE BE C7 on a Motorola device.

In addition to these various data formats, mobile devices use specific data structures to represent call logs and other information. Researchers and tool developers are delving into such data structures to help digital investigators extract more useful data and correctly interpret the information they obtain correctly. For instance, as noted in the previous section, Windows Mobile devices store communications in Microsoft proprietary embedded databases. The structure of these embedded databases has been explored by several digital forensic researchers and tools have been developed to extract information from these database files (Casey, Bann, & Doyle, 2009; Klaver, 2009; Rehault, 2010). For more instruction on forensic examination and analysis of mobile devices, see the cmdLabs Web site (http://www.cmdlabs.com).

20.6 FORENSIC ACQUISITION AND EXAMINATION OF SIM CARDS

When conducting forensic examinations of GSM/UMTS mobile devices, it is also important to inspect the contents of associated SIM cards. In some cases, there might be multiple SIM cards that an individual uses in different countries or for different purposes. Some devices function with dual SIM cards. In addition, the storage capacity and utilization of USIM cards is increasing and may contain substantial amounts of relevant information. Furthermore, when a user deletes items from a SIM card, some devices will leave remnants of deleted data on the card like SMS messages.

The hierarchical storage structure of a SIM card is relatively straightforward, and the content of each file is defined in the GSM Technical Specification (GSM 11.11). There is one master file that contains references to all other files on the SIM card. Each file is addressed using a unique two-byte hexadecimal value, with the first byte indicating whether it is a master file, dedicated file, or elementary file:

3F = Master file (MF)
7F = Dedicated file (DF)
2F = Elementary file under the master file
6F = Elementary file under a dedicated file

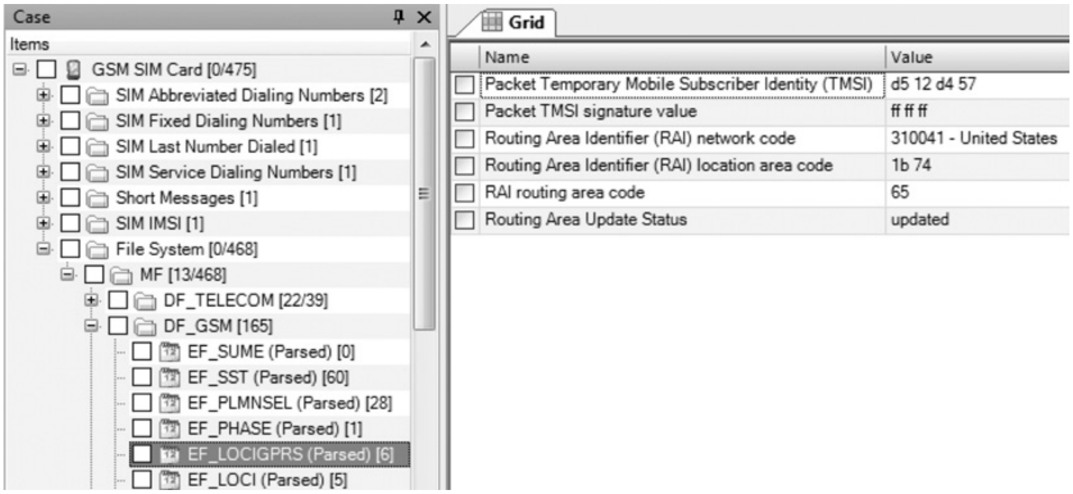
The technical specification designates some files with common names. For instance, the 3F00:7F10 directory is named DFTELECOM, and contains service-related information, including user-created data like SMS messages and last numbers dialed. The 3F00:7F20 directory is named DFGSM, and contains network-related information for GSM 900 MHz band operation (DFDCS1800 contains information for 1800 MHz band operation). Similarly, some Elementary Files have common names. For example, 3F00:2FE2 is named EFICCID (stores the ICC-ID) and 3F00:7F20:6F07 is named EFIMSI (stores the IMSI).

There are many tools for extracting data from SIM cards, including TULP2G (http://tulp2g.sourceforge.net/), developed by the Netherlands Forensic Institute and made freely available. Although, the tool is generally limited to second-generation technologies, it has been updated to extract information from third-generation SIM cards. To use TULP2G to acquire data from a SIM card, first open the SIM Investigation profile, select the Investigation tab, and Run the SIM plug-in to extract data from card.

The types of information that may be available on a SIM card are listed in Table 20.3. This includes the location area identifier (LAI), which is stored in EFLOCI (7F20:6F7E), providing the country, network, and location area identifier. Each time a mobile device moves to a new area, the LAI information is updated on the SIM card. Location information may also be available when the GPRS mobile data service is used. The EFLOCIGPRS (7F20:6F53) contains GPRS Routing Area Information similar to the LAI information as shown in Figure 20.27 using Paraben's Device Seizure software.

Table 20.3 Selection of Information that can be Stored on SIM Cards

Description	Location
SMS	7F10:6F3C
MSISDN	7F10:6F40
Last Dialed Numbers (LDN)	7F10:6F44
Abbreviated Dial Numbers (ADN)	7F10:6F3A
IMSI	7F20:6F07
LOCI	7F20:6F7E
LOCIGPRS	7F20:6F53



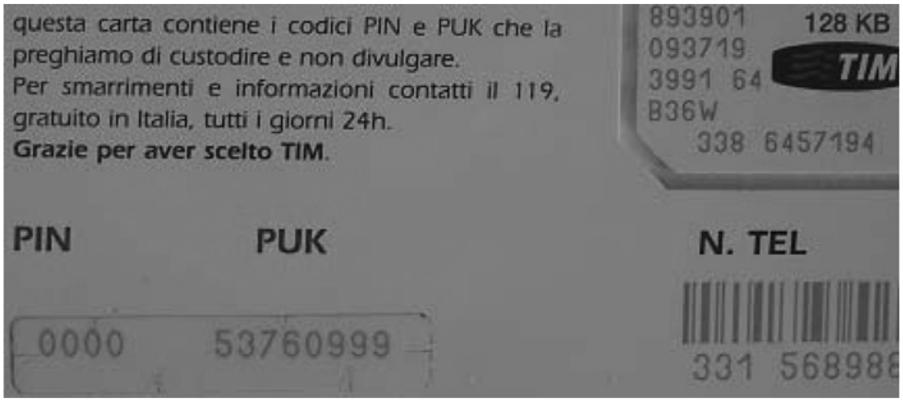
- □ GSM SIM Card [0/475]
  - □ SIM Abbreviated Dialing Numbers [2]
  - □ SIM Fixed Dialing Numbers [1]
  - □ SIM Last Number Dialed [1]
  - □ SIM Service Dialing Numbers [1]
  - □ Short Messages [1]
  - □ SIM IMSI [1]
  - □ File System [0/468]
    - □ MF [13/468]
      - □ DF_TELECOM [22/39]
      - □ DF_GSM [165]
        - □ EF_SUME (Parsed) [0]
        - □ EF_SST (Parsed) [60]
        - □ EF_PLMNSEL (Parsed) [28]
        - □ EF_PHASE (Parsed) [1]
        - □ EF_LOCIGPRS (Parsed) [6]
        - □ EF_LOCI (Parsed) [5]

	Name	Value
□	Packet Temporary Mobile Subscriber Identity (TMSI)	d5 12 d4 57
□	Packet TMSI signature value	ff ff ff
□	Routing Area Identifier (RAI) network code	310041 - United States
□	Routing Area Identifier (RAI) location area code	1b 74
□	RAI routing area code	65
□	Routing Area Update Status	updated

FIGURE 20.27
Information extracted from a SIM card using Paraben Device Seizure.

20.6.1 SIM Security

As with mobile devices, security codes can be a barrier to acquiring data from SIM cards. Therefore, it is important to understand how such security protection can be overcome. Users can set a personal identification number (PIN) to restrict access to their SIM card. Brute force attacks against the PIN are generally ineffective unless the manufacturer default was never reset by the user, because three failed PIN attempts will result in the SIM being locked. Fortunately, some phones have a PIN unblocking key (PUK) in their documentation as shown in Figure 20.28, and many network service providers (NSP) can provide the PUK to get around the PIN or to access a locked SIM card.



questa carta contiene i codici PIN e PUK che la
preghiamo di custodire e non divulgare.
Per smarrimenti e informazioni contatti il 119,
gratuito in Italia, tutti i giorni 24h.
Grazie per aver scelto TIM.

893901
093719
3991 64
B36W
338 6457194

128 KB
TIM

PIN PUK N. TEL

0000 53760999 331 56898

FIGURE 20.28
Original documentation associated with SIM card contains PUK.

With the proper legal authorization and NSP contact, forensic investigators may be able to obtain a PUK in a matter of minutes. However, not all NSPs retain the PUK for the SIM cards they sell, and in some situations it may not be feasible to involve the NSP.

20.7 INVESTIGATIVE RECONSTRUCTION USING MOBILE DEVICES

Given the variety of information that mobile devices contain about peoples' communications, movements, and online activities, these sources of digital evidence can be instrumental in helping digital investigators reconstruct events surrounding a crime. The primary methods covered in Chapter 6 for performing investigative reconstruction are presented here in the context of mobile devices.

20.7.1 Temporal Analysis

One of the most common forms of temporal analysis is creating a timeline of events to gain a greater understanding of what occurred around the time of a crime and to help investigators identify patterns and gaps, potentially leading to other sources of evidence. Given the variety and potentially large quantity of temporal information on mobile devices, it is a good practice to maintain a timeline as events are uncovered to ensure that nothing is overlooked and that important events become apparent promptly. There are other approaches to analyzing temporal data, such as plotting them in a histogram to find repeated events or periods of highest activity.

When multiple sources of information are being correlated, temporal analysis may tie events together based on coincidental timing of their occurrence. For instance, location-based evidence may place the suspect at the scene of a crime at the exact time the offense occurred. As such, combining details from the various forms of analysis can lead to detailed reconstruction of who did what, when, and where.

20.7.2 Relational Analysis

A full relational analysis can include the geographic location of mobile devices and the associated users, as well as any communication/transaction that occurred between them. In a major crime investigation involving a large group of people and devices, creating a detailed relational analysis—where each party was located and how they interacted—can reveal a crucial relationship.

GPS-enabled mobile devices and SatNav systems may store waypoints and other GPS coordinates in a file format that can be imported into mapping tools as shown in Figure 20.29. Google Earth has a feature to import location information, and a standalone tool for plotting various GPS coordinate files on a map is PoiEdit (www.poiedit.com).

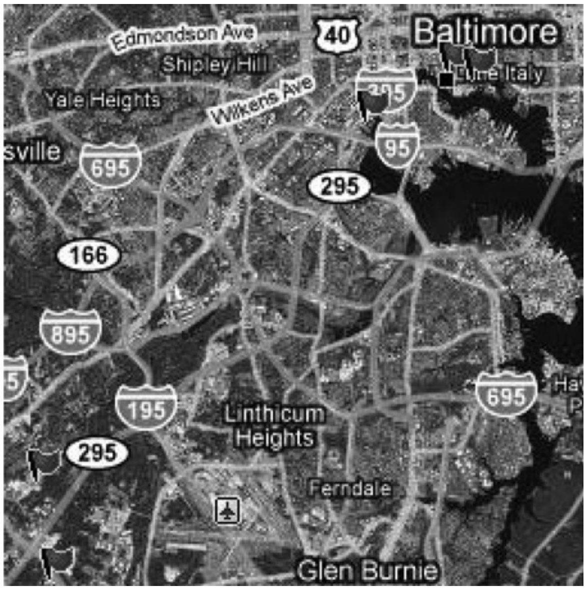


FIGURE 20.29
Waypoints extracted from a Garmin SatNav device plotted on a map using flags as markers.

Another form of relational analysis is determining how one item of evidence relates to another. This form of analysis is often called *evaluation of source*, and may reveal the location origin of an item of evidence, the mobile device used to create the evidentiary item, or that the evidentiary item was once part of a particular mobile device. For example, relational questions in a child exploitation case might include: Was a particular mobile device used to take evidential digital photographs? Where were the photos taken? Was the suspect's SIM card ever placed in the mobile device?

20.7.3 Functional Analysis

Forensic examiners perform a functional analysis to determine how a particular function or program on a mobile device works and how the device was configured at the time of the crime. This type of analysis can be performed using emulation software or a physical test device (Murphy, 2009).

The aim of this type of analysis is to gain a better understanding of a crime or a piece of digital evidence. Malware forensics is another example of functional analysis that may be necessary when a mobile device has been misused.

20.8 FUTURE TRENDS

Digital Forensics is a reactive field, and as such future trends in mobile phone analysis are largely dependent on trends in the mobile phone industry. Phones are becoming much more capable, and while there remains a market for phones with only basic functionality, phones with greater functionality are the expanding market. The term smart phone is ceasing to be relevant as it becomes the standard. For forensic investigators and analysts, this is positive for two reasons: phones will have greater capability and hence will contain more potential evidence, and the industry is stabilizing to a smaller number of core operating system platforms.

The proliferation of high-end smart phones in both the consumer and commercial sectors will ultimately have an impact on forensic investigation. The increased capacity of phones will require greater analysis on a per-device basis but can provide greater insight. Mobile phones are a data store largely abstracted away from individual users and are less likely to be altered or tampered with.

The number of mobile phone and device operating systems is consolidating to a discrete group, largely independent of the hardware. This will aid data extraction and analysis in reduced learning curves for different devices as well as a greater understanding of what can be extracted for each platform. The need to reverse-engineer the idiosyncrasies found in custom operating systems or individual implementations will decrease over time.

The future of mobile phone and device forensic analysis will, to a greater degree, involve the reverse-engineering of third party applications. Such applications are platform-dependent, written either with native SDKs or through third-party tool sets, and have differing access to the underlying operating system. Understanding the capability and intent of third-party applications may be vital to forensic analysts in certain circumstances, as they may be malicious in nature, indirectly facilitate crime, provide communication mechanisms outside of standard on-phone systems, or store data of forensic value (either locally or on externally hosted servers). Third-party applications are also likely gateways to cloud services, which are increasingly catering to mobile devices. The forensic implications of cloud computing are beyond the scope of this work, but you must be aware of both their existence and the idea that evidence exists beyond the device itself.

Low-end phones with basic functionality will continue to exist in significant numbers. From a digital forensic perspective, these phones are cheap and disposable, and it is difficult to attribute ownership. Such analysis needs greater scalability in analysis, for situations where an individual may control multiple phones, multiple groups control a single phone, and for large-scale social network analysis.

Current links between workstations and notebook computers and phones almost exclusively view the phone as a satellite device. Improved connectivity between phones and other data sources may alter this and provide greater links between connected systems.

By far the most obvious trend is that mobile devices will continue to be important in forensic analysis and have a large role in both civil and criminal investigations.

20.8 SUMMARY

There are a growing number of mobile devices for personal organization and communication, many with access to the Internet. These devices can be a source of digital evidence in any crime, containing personal information about an individual, including photographs, passwords, and other useful data, or showing where individuals were at a specific time and with whom they were communicating. The information they contain can also be an instrumentality of a crime when they are used to steal intellectual property or create and disseminate child pornography. These devices can be an instrumentality of a crime when used to eavesdrop on wireless network traffic. In recent years, it has become routine for investigators to collect mobile devices as evidence. Embedded systems are a challenging source of evidence because the data on them is volatile and different tools are needed to process different devices. Currently tools and training in this area are limited but, given the rapid increase in their use, this is likely to become one of the largest growth areas in the field of digital evidence examination.

REFERENCES

Borland, S. (2008, February 2008). "Happy slap" girl facing jail after conviction. *The Telegraph*. Available from http://www.telegraph.co.uk/news/uknews/1578776/Happy-slap-girl-facing-jail-after-conviction.html.

Breeuwsma, M. (2006). Forensic imaging of embedded systems using JTAG. *Digital Investigation*.

Breeuwsma, M., de Jongh, M., Klaver, C., van der Knjiff, R., & Roeloffs, M. (2007). Forensic data recovery from flash memory. *Small Scale Digital Device Forensics Journal*, 1(1). Available from www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf.

Casey, E. (2009). Delving into mobile device file systems. Available from http://blog.cmdlabs.com/category/http://blog.cmdlabs.com/2009/12/10/delving-into-mobile-device-file-systems/.

Casey, E., Bann, M., & Doyle, J. (2009). Introduction to windows mobile forensics. *Digital Investigation*, 6(3–4).

Conrad, C. (2010, October 3). Cell phones cause hang-up for police to track drug deals. *Mail Tribune*. Available from http://www.mailtribune.com/apps/pbcs.dll/article?AID=/20101003/NEWS/10030336/-1/MARKET.

Jones, A. (2008, January 21–23). Keynote speech. In: First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia, Adelaide, Australia.

Klaver, C. (2009). Windows mobile advanced forensics. *Digital Investigation*, 6(3–4).

Koschade, S. (2006). A social network analysis of Jemaah Islamiyah: The applications to counter-terrorism and intelligence. *Studies in Conflict and Terrorism*.

Krueger, C. (2011, February 11). Man found guilty of lesser charge in murder recorded on cell phone.

St. Petersburg Times.

Mislan, R., Casey, E., & Kessler, G. (2010). The growing need for on-scene triage of mobile devices. *Journal of Digital Investigation*, 6.

Moore, H. D. (2007, September 25). A root shell in my pocket (and maybe yours). Available from http://blog.metasploit.com/2007/09/root-shell-in-my-pocket-and-maybe-yours.html.

Murphy, C. (2009). The fraternal clone method for CDMA cell phones. *Small Scale Digital Device Forensics Journal*, 3(1). Available from http://www.ssddfj.org/papers/SSDDFJ_V3_1_Murphy.pdf.

Rehault, F. (2010). Windows mobile advanced forensics: An alternative to existing tools. *Journal of Digital Investigation*, 7(1–2).

Wilson, C. (2006). Improvised Explosive Devices (IEDs) in Iraq: Effects and countermeasures. In: Congressional Research Service Report for Congress. Available from http://www.history.navy.mil/library/online/ied.htm.

Williams, R. (2010, December 02). Baby video torture killer an "Evil Monster." *Sky News*. Available from http://news.sky.com/skynews/Home/UK-News/Charlie-Hunt-Murderer-Of-Baby-Filmed-While-He-Was-Tortured-Darren-Newton-Branded-Evil-Monster/Article/201012115845372?f=rss.