



## Call for Cell Phone Forensics

*The functionality of cellular phones today rivals that of personal digital assistants (PDAs) and even laptop computers. Cellular phones can perform all of these tasks and more: voicemail, music/MP3 player, camera, video camera, voice recorder, Web browser, e-mail appliance, text/instant messenger, address book, calendar, notepad, and games. They also send and receive phone calls.*

Early cellular phone technology (circa 1984) featured very little functionality. Cellular phones were communication devices that supported wireless voice transmissions as two-way full-duplex radios. Within a few years, features such as voicemail and text messaging became available. Now, data come and go using wireless data transfer coupled with Bluetooth®, infrared, and proprietary or USB data cables that connect directly to a computer. Small external media placed inside the phone can hold up to 6 gigabytes of information.

Any technology that can be used for legitimate purposes can be used to accomplish illegal aims as well. State and local law enforcement officials responding to emergencies and criminal complaints almost inevitably discover the presence of a cell phone. These cellular phones should not be overlooked as a potential source of evidence and intelligence in any type of criminal investigation. A quick look at the headlines will reveal criminals using cellular phone technology as a network for coordinating a criminal enterprise, a means to send harassing text messages to a victim, a method of producing photographs viewed by a pedophile, or a way for international or domestic terrorists to detonate devices.

Knowing a cellular phone may contain useful information and being able to extract that all-important data, however, are two different matters. Cellular phones present many hurdles to the investigator, including custom-designed operating systems and varied network providers with an almost infinite number of operating systems, all combining to produce unfamiliar file systems and hardware and using proprietary cables, chargers, and connectors. Law enforcement investigators need to learn about all of the potential sources of evidence that may be found in cellular phones, as well as mastering the

options for reliably seizing the devices and methods available for locating cellular phone forensic information.

Cellular phones present a number of potential sources of evidence:

- **Media devices** such as MicroSecureDisk (MicroSD) cards, present a very straightforward source of evidence for a forensic examiner to process, because standard forensic tools will work to recover this type of data.

### BASIC RESOURCES

The following list of resources, which may not be all inclusive, may be helpful to law enforcement officers looking to learn the basics of cell phone forensics.

### TRAINING

BKForensics ([www.bkforensics.com](http://www.bkforensics.com))

Forensic Telecommunications Services (FTS) ([www.forensictts.co.uk](http://www.forensictts.co.uk))

Mobile Forensics Inc. (MFI) ([www.mobileforensicstraining.com](http://www.mobileforensicstraining.com))

Paraben Corporation ([www.paraben.com](http://www.paraben.com))

### SOFTWARE AND HARDWARE

BitPim ([www.bitpim.sourceforge.net](http://www.bitpim.sourceforge.net))

BKForensics ([www.bkforensics.com](http://www.bkforensics.com))

Compelson Laboratories ([www.mobiledit.com](http://www.mobiledit.com)):  
MOBILedit! Forensic

*Continued on page 2*

- **SIM (Subscriber Identity Module) cards** are present in all GSM (Global System for Mobile communications) phones. All GSM phones contain one or more SIM cards. SIM cards also can be read through a fairly straightforward process since the type of data held on SIM cards and the manner in which it is stored is clearly defined by GSM standards. Similar technology is also emerging for CDMA (Code Division Multiple Access) phones.
- **Memory chips**, located inside the handset, use the same type of memory found in compact flash cards and thumb drives. However, the storage of the data is typically proprietary and standard forensic tools usually will not decipher the data. This makes forensic examinations of cellular phones extremely difficult.
- **Network providers** such as T-Mobile, Cingular, AT&T, Verizon, and others present another source of forensic information.

When seizing a cellular phone, investigators need to realize that when a phone is turned on and connected to a provider's network, the data on the phone constantly changes; thus, potential evidence could be lost. Officers must immediately sever a phone's connectivity to a provider network in order to preserve this vital data. This can be accomplished in several ways; all methods have advantages and disadvantages, and only proper training will determine which method is right for a particular situation.

It is vital that investigators obtain any keyboard lock codes or PIN codes used to access a phone. If a power charger, data cable, original box, or bills can be found, they should be seized immediately. Document all identifying information so that an investigator can identify the phone to the network provider when requesting information on its subscribers in addition to any other information that could be useful in an investigation.

The type of cellular phone, an investigator's training, and an agency's access to hardware and software will dictate the best methods for forensic examination of a particular cell phone. If it is necessary to turn a phone on to examine it, an investigator should be aware that the phone will connect to the provider network and the received missed calls, voicemail notifications, and/or software updates, any or all of which will cause the phone's internal memory to be reorganized. Steps should be taken therefore to isolate the cellular phone during an examination.

## Cellular Phone Forensics

In some cases, investigators will glean data from the cellular phone by turning on the phone and perusing various screens and settings, recording information displayed via video, photograph, or handwritten notes. It is

### Basic Resources (continued)

Fernico ([www.fernico.com](http://www.fernico.com)):  
Zippy Reporting Tool

Guidance Software, Inc.  
([www.guidancesoftware.com](http://www.guidancesoftware.com)):  
Neutrino device acquisition tool and Neutrino WaveShield™ signal-blocking bag

iCardForensics  
([www.icardforensics.com](http://www.icardforensics.com)): .XRY

Logicube ([www.logicubeforensics.com](http://www.logicubeforensics.com)): CellDEK

Oxygen Software  
([www.oxygensoftware.com](http://www.oxygensoftware.com)):  
Oxygen Forensic Suite

Paraben ([www.paraben.com](http://www.paraben.com)):  
Device Seizure, Device Seizure Toolbox, SIM Card Seizure

Susteen, Inc. ([www.datapilot.com](http://www.datapilot.com)):  
DataPilot, SecureView for Forensics

### REPORTS

*Cell Phone Forensics: An Overview & Analysis Update*, NIST, <http://csrc.nist.gov/publications/nistir/nistir-7387.pdf>

*Guidelines on Cell Phone Forensics*, National Institute of Standards and Technology (NIST), <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>

### GLOSSARY OF COMMON TERM

**CDMA:** Code division multiple access. A type of digital cellular network.

**GSM:** Global system for mobile communications (originally from Groupe Spécial Mobile). A type of digital - cellular network.

**IMEI:** International mobile equipment identity number. A 15-digit number that indicates a manufacturer, model type, and country of approval for GSM devices.

**PIN:** Personal identification number. A code used to complete a call.

**PUC:** Personal unblocking code used in GSM mobile phones and some smartcards. Most mobile telephones offer the feature of personal identification number protection. After switching on the phone, the user is (optionally) requested for security reasons to enter a 4- to 8-digit PIN enabling the phone's non-emergency calling functions. If the wrong PIN is typed in more than three times, either the SIM card, the device, or

*Continued on page 3*

important that investigators, through training and experience, know all their options when confronted with a seized cellular phone.

Devices such as “project-a-phone” can facilitate this process. However, this is probably the least favorable way to examine a cellular phone and should be done only as a last resort. Using methods like this one make it very easy to miss data and impossible to retrieve deleted information.

Investigators can also retrieve cellular phone data by using a data connection from a computer to a cellular phone along with software that understands the phone’s data storage. Many different tools can be used to accomplish this purpose, some phone specific, others able to examine a wider range of phone makes and models. Investigators using this method, however, will not see deleted data or data that may reside in memory but cannot be accessed by this particular tool (much like the problems that may arise when investigators perform forensic analysis of logical files from a hard drive).

The most favorable method for examining cellular phones is not always an option for all cellular phone types. Ideally, an investigator can read data directly from the memory chips on the phone’s circuit board and store this data in a file. The contents of this file can then be examined with a hex editor or interpreted with software such as Cell Phone Analyzer (CPA), allowing extraction of both active and deleted data. Another advantage is that this method can be used with the cellular phone powered off, so there is no change to the data in the phone’s memory.

A thorough examiner will use one (or all) of the methods described above when examining cellular phones for valuable evidence. Some cellular phones, however, simply defy any examination beyond direct viewing.

Investigators who find this information overwhelming should know there is help available. State, local, and Federal agencies continually endeavor to build their resources and create strategies that work for handling cell phone technology. Listservs and bulletin board forums for cellular phone forensics may provide answers to questions. There are also software packages and training courses that specifically target law enforcement. Investigators need to reach out and find these resources quickly, before their next investigation that hinges on data from a cellular phone.

***For more information, visit BK Forensics at [www.bkforensics.com](http://www.bkforensics.com), or phone 888-781-7178.***

#### ***Basic Resources (continued)***

both become locked. They can be reverted to their original unlocked state, however, by entering a PUC, but if the wrong PUC is entered 10 times in a row, the device will become permanently blocked and unrecoverable, requiring a new SIM card. Cellular phone users are therefore advised by most providers to keep their PUC written down in a safe place separate from the device.

**PUK:** PIN unblocking key or personal unblocking key, another term for PUC.

**SIM:** Subscriber identity module, a removable “smart card” for mobile phones. SIM cards securely store the service-subscriber key used to identify a mobile phone. A SIM card allows users to change phones by simply removing the SIM card from one mobile phone and inserting it into another mobile phone. The use of a SIM card is mandatory in the GSM world.

**UMTS:** Universal mobile telecommunications system is one of the third-generation (3G) mobile phone technologies. Currently, the most common form uses W-CDMA as the underlying air interface, is standardized by the 3GPP, and is the European answer to the ITU IMT-2000 requirements for 3G cellular radio systems. To differentiate UMTS from competing network technologies, UMTS is sometimes marketed as 3GSM, emphasizing the combination of the 3G nature of the technology and the GSM standard that it was designed to succeed.

---

Source: Adapted from Wikipedia (<http://wikipedia.org>).

The National Law Enforcement and  
Corrections Technology Center System  
**Your Technology Partner**

[www.justnet.org](http://www.justnet.org)  
800-248-2742



This article was reprinted from the Winter 2008 edition of *TechBeat*, the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center System, a program of the National Institute of Justice under Cooperative Agreement #2005-MU-CX-K077, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Lockheed Martin. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).