June 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

FORENSIC TECHNIQUES FOR CELL PHONES

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The data that is captured on mobile phones can be a source of valuable information to organizations that are investigating crimes, policy violations, and other security incidents. The science of recovering digital evidence from mobile phones, using forensically sound conditions and accepted methods, is called mobile phone forensics. In general, forensic science is the application of scientific principles for legal, investigative, and public policy purposes. Digital forensic science refers to the preservation, acquisition, examination, analysis, and reporting of electronic data collected and stored on computer and network systems and on many digital devices.

The digital forensic community faces special challenges when investigating crimes and incidents involving mobile phones. While cell phones are widely used for both personal and professional applications, the technology of cell phones is continually changing as new designs and improved techniques are introduced. As a result of the rapid pace of change, the established guides that provide advice on the application of computer forensics usually do not cover cell phones, especially those with advanced capabilities.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued a new guide to help organizations develop appropriate policies and procedures for dealing with the information on cell phones, and for preparing their forensic specialists to adopt new techniques when cell phones are involved. Developed with the support of the Department of Homeland Security, the guide provides basic information about the characteristics of cell phones and explains the issues to be considered when organizations are conducting incident response and other types of investigations.

Guidelines on Cell Phone Forensics

Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology was issued in May 2007 as NIST Special Publication (SP) 800-101. Written by Wayne Jansen and Rick Ayers of NIST, SP 800-101 provides an in-depth examination of mobile phones, the technology involved, and the management of forensic procedures. It covers phones with advanced features beyond simple voice communication and text messaging, and details their technical and operating characteristics. The guide discusses procedures and techniques involved in cell phone forensic activities, as well as available forensic software tools that support those activities.

The extensive reference list in NIST SP 800-101 provides a rich selection of in-print and online resources for cell phone products and services, as well as discussions of the application of forensic techniques. The appendices to the guide include an acronym list, a glossary of terms used in the guide, and a detailed view of the steps involved in the acquisition of a cell phone with Universal Mobile Telecommunications System capabilities. Another section of the appendices provides information about the contents of records collected by cellular network carriers involving event and call data.

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since June 2006:

- *Domain Name System (DNS) Services: NIST Recommendations for Secure Deployment, June 2006*
- *Protecting Sensitive Information Processed and Stored in Information Technology (IT) Systems, August 2006*
- *Forensic Techniques: Helping Organizations Improve Their Responses to Information Security Incidents, September 2006*
- *Log Management: Using Computer and Network Records to Improve Information Security, October 2006*
- *Guide to Securing Computers Using Windows XP Home Edition, November 2006*
- *Maintaining Effective Information Technology (IT) Security Through Test, Training, and Exercise Programs, December 2006*
- *Security Controls for Information Systems: Revised Guidelines Issued by NIST, January 2007*
- *Intrusion Detection and Prevention Systems, February 2007*
- *Improving the Security of Electronic Mail: Updated Guidelines Issued by NIST, March 2007*
- *Securing Wireless Networks, April 2007*
- *Securing Radio Frequency Identification (RFID) Systems, May 2007*

While not providing specific legal advice to organizations, the guide covers the information and principles that will enable organizations to establish the policies and procedures needed for an effective forensics program developed in conjunction with their legal advisors, agency officials, and managers.

NIST SP 800-101 is available from NIST's website at: http://csrc.nist.gov/publications/nistpubs/index.html.

Who We Are
The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

Cell Phone Technology

In the United States, digital cellular networks have been developed based on different and incompatible sets of standards. Two types of digital cellular networks dominate: Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) networks. Other commonly implemented cellular networks include Time Division Multiple Access (TDMA) and Integrated Digital Enhanced Network (iDEN). iDEN networks use a proprietary protocol designed by Motorola, while the others follow standardized open protocols. Also available is a digital version of the original analog standard for cellular telephone phone service called Digital Advanced Mobile Phone Service (D-AMPS).

Mobile phones work with certain subsets of these network types, with the service provider supplying the phone and the details of the service agreement. For example, a service provider or network operator for a GSM network that has some older TDMA network segments in operation might supply a phone that has GSM voice and data capabilities, and TDMA capabilities. Such a phone would not be compatible with CDMA networks.

Mobile phones can also be acquired without service from a manufacturer, vendor, or other source, and the service can be arranged separately with a service provider or network operator, provided that the phone is compatible with the network. When in operation, mobile phones may contact compatible networks operated for or by another service provider, and gain service. To administer the cellular network system, provide subscribed services, and accurately bill or debit subscriber accounts, data about the service contract and associated service activities are captured and maintained by the network system.

Cellular networks provide coverage based on dividing a large geographical service area into smaller areas of coverage called cells. These cells can often utilize unused radio frequencies in the limited radio spectrum, enabling more calls to take place than might be possible otherwise. As a mobile phone user moves from one cell to another, active connections must be monitored and effectively passed along between cells to maintain the connection

The main components of cellular networks are: the Base Transceiver Station (BTS), the radio transceiver equipment that communicates with the mobile phones; the Base Station Controller (BSC), which manages the transceiver equipment and performs channel assignment; and the Mobile Switching Center (MSC), the switching system for the cellular network. The BSC and the BTS units it controls are sometimes collectively referred to as a Base Station.

Cell Phone Characteristics

Cell phones are highly mobile communications devices that perform functions such as organizing digital data and carrying out basic personal computing activities. Designed for mobility, these phones are compact in size, battery powered, and lightweight. Most cell phones have a basic set of comparable features and capabilities. They are composed of a microprocessor, read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, and a liquid crystal display (LCD). The operating system (OS) of the device is held in ROM, which can be erased and reprogrammed electronically when the proper tools are used. The RAM, which may be used to store user data, is supported by batteries. If the batteries fail, the information can be lost.

The newest cell phones are equipped with system-level microprocessors that reduce the number of supporting chips required to operate the phone and include considerable memory capacity. Other capabilities include card slots that support removable memory cards or specialized peripherals, such as wireless capabilities. Wireless communications capabilities may also be built into the phone.

Different devices have different technical and physical characteristics, such as size, weight, processor speed, and memory capacity. Devices may also use different types of expansion capabilities to provide additional functionality. Cell phones may have the capabilities of other devices such as personal digital assistants (PDAs), global positioning systems, and cameras. While there are many different types of cell phones, they can be generally characterized as: basic phones that are primarily simple voice and messaging communication devices; advanced phones that offer additional capabilities and services for multimedia; and smart phones or high-end phones that combine the capabilities of an advanced phone with those of a PDA.

Forensic Tools

The application of forensic software tools to cell phones is a very different process from the forensic process used with personal computers. The latter devices are primarily designed as general-purpose systems, while cell phones are designed more as special-purpose appliances that perform a set of predefined tasks. Since cellular phone manufacturers tend to rely on different proprietary operating systems rather than the more standardized approach found in personal computers, there are different toolkits for use with mobile devices. Also, the toolkits are often

limited to a narrow range of distinct platforms for a manufacturer's product line, an operating system family, or a type of hardware architecture. Since the technology of cell phones is frequently updated, tool manufacturers must update their tools continually to keep their coverage current. As a result, the development of tools for newer models of cell phones frequently lags behind the introduction of new models.

Forensic tools acquire data from a device by both physical acquisition and logical acquisition methods. Physical acquisition involves a bit-by-bit copy of an entire physical store of data, such as a memory chip. Logical acquisition involves a bit-by-bit copy of logical storage objects, such as directories and files that are located in a file system. Physical acquisition has advantages over logical acquisition, since it allows deleted files and any data remnants present to be examined. Extracted device images need to be parsed, decoded, and translated to uncover the data present. The work is tedious and time-consuming to perform manually. Physical device images can be imported into a tool to automate examination and reporting; however, only a few tools tailored for obtaining cell phone images are currently available. Although logical acquisition is more limited than physical acquisition, the system data structures are usually easier for a tool to extract. The logical acquisition of data provides a more natural and understandable organization of the data for use during examination. Both types of acquisition are useful.

Steps in the Investigation

Investigations and incidents are handled in different ways depending upon the circumstances and severity of the incident, and on the experience of the investigation team. Organizations can advance the effective application of cell phone forensics by carefully planning the steps in the investigative process:

- Defining the procedures and principles that will apply when dealing with digital evidence, and establishing roles and responsibilities for the personnel involved.

- Preserving the evidence related to the investigation through appropriate search, recognition, documentation, and collection procedures, without altering or changing the content of data on devices and media.

- Acquiring information from a digital device and its peripheral equipment and media in a controlled setting, such as a laboratory.

- Examining and analyzing digital evidence through the application of established scientifically based methods, fully describing the content and state of the data.

- Reporting on the investigation by preparing a detailed summary of all of the steps taken and the conclusions reached in the investigation of a case, maintaining a careful record of all actions and observations, describing results of tests and examinations, and explaining the inferences drawn from the evidence.

NIST Recommendations for the Application of Cell Phone Forensics

NIST recommends that organizations implement the following recommendations to facilitate the application of efficient and effective digital forensic activities involving cell phones and cellular devices.

Ensure that organizational policies contain clear statements about forensic considerations involving cell phones.

At a high level, policies should allow authorized personnel to perform investigations of cell phones that have been issued by the organization when there are legitimate reasons for such investigations and they are conducted under the appropriate circumstances. The forensic policy should clearly define the roles and responsibilities of the workforce and of any external organizations performing or assisting with the organization's forensic activities. The policy should also indicate internal teams and external organizations to be contacted under various circumstances.

Create and maintain procedures and guidelines for performing forensic tasks on cell phones.

Guidelines should focus on general methodologies for investigating incidents using forensic techniques. While developing comprehensive procedures tailored to every possible situation is not generally feasible, organizations should consider developing step-by-step procedures for performing all routine activities in the preservation, acquisition, examination and analysis, and reporting of digital evidence found on cell phones and associated media. The guidelines and procedures should facilitate consistent, effective, accurate, and repeatable actions carried out in a forensically sound manner, suitable for legal prosecution or disciplinary actions. The guidelines and procedures should support the admissibility of evidence into legal proceedings, including seizing and handling evidence properly, maintaining the chain of custody, storing evidence appropriately, establishing and maintaining the integrity of forensic tools and equipment, and demonstrating the integrity of any electronic logs, records, and case files. The guidelines and procedures should be reviewed periodically and also whenever there are significant changes in cell phone technology that affect them.

Ensure that organizational policies and procedures support the reasonable and appropriate use of forensic tools for cell phones.

Policies and procedures should clearly explain what actions are to be taken by a forensic unit under various circumstances commonly encountered with cell phones. They should also describe the quality measures to apply in verifying the proper functioning of any forensic tools used in examining cell phones and associated media. Procedures for handling sensitive information that might be recorded by forensic tools should also be addressed. Legal counsel should carefully review all forensic policy and high-level procedures for compliance with international, federal, state, and local laws and regulations, as appropriate.

Ensure that the organization's forensic professionals are prepared to conduct activities in cell phone forensics.

Forensic professionals, especially first responders to incidents, should understand their roles and responsibilities for cell phone forensics and receive training and education on related forensic tools, policies, guidelines, and procedures. Forensic professionals should also consult closely with legal counsel in general preparation for forensics activities, such as determining which actions should and should not be taken under various circumstances. In addition, management should be responsible for supporting forensic capabilities, reviewing and approving forensic policy, and examining and endorsing unusual forensic actions that may be needed in a particular situation.

More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. Publications dealing specifically with digital forensics include:

NIST SP 800-72, *Guidelines on PDA Forensics*, by Wayne Jansen and Rick Ayers, helps organizations develop policies and procedures for personal digital assistants (PDAs) and assists forensic specialists in dealing with situations involving PDAs.

NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, by Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang, provides detailed information on establishing a forensic capability, including the development of policies and procedures and the use of forensic techniques to assist with computer security incident response.

These publications and other security-related publications are available from NIST's website: http://csrc.nist.gov/publications/nistpubs/index.html.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.