3.6. Cell Phone and Mobile Devices Forensics

Understanding Mobile Device Forensics

- People store a wealth of information on cell phones, and the thought of losing your cell phone and, therefore, the information stored on it can be a frightening prospect.
- Despite this concern, not many people think about securing their cell phones, although they routinely lock and secure laptops or desktops. Depending on your phone's model, the following items might be stored on it:
    - Incoming, outgoing, and missed calls
    - Text and Short Message Service (SMS) messages
    - E-mail
    - Instant messaging (IM) logs
    - Web pages
    - Pictures
    - Personal calendars
    - Address books
    - Music files
    - Voice recordings

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

Mobile Phone Basics

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

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

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

4G networks can use the following technologies:

- **Orthogonal Frequency Division Multiplexing (OFDM)—**The Orthogonal Frequency Division Multiplexing (OFDM) technology uses radio waves broadcast over different frequencies, uses power more efficiently, and is more immune to interference
- **Mobile WiMAX**—This technology uses the IEEE 802.16e standard and Orthogonal Frequency Division Multiple Access (OFDMA) and is expected to support transmission speeds of 12Mbps. Sprint has chosen this technology for its 4G network, although some argue it's not true 4G.
- **Ultra Mobile Broadband (UTMS)—**Also known as CDMA2000 EV-DO, this technology is expected to be used by CDMA network providers to switch to 4G and support transmission speeds of 100 Mbps.

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

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

Fig : Digital Networks

- **Multiple Input Multiple Output (MIMO)—**This technology, developed by Airgo and acquired by Qualcomm, is expected to support transmission speeds of 312 Mbps.
- **Long Term Evolution (LTE)—**This technology, designed for GSM and UMTS

Although digital networks use different technologies, they operate on the same basic principles. Basically, geographical areas are divided into cells resembling honeycombs.

As described in NIST SP 800-101 (mentioned earlier in this section), three main components are used for communication with these cells:

- **Base transceiver station (BTS)—**This component is made up of radio transceiver equipment that defines cells and communicates with mobile phones; it's sometimes referred to as a cell phone tower, although the tower is only one part of the BTS equipment.
- **Base station controller (BSC)—**This combination of hardware and software manages BTSs and assigns channels by connecting to the mobile switching center.

- **Mobile switching center (MSC**)—This component connects calls by routing digital packets for the network and relies on a database to support subscribers. This central database contains account data, location data, and other key information needed during an investigation. If you have to retrieve information from a carrier's central database, you usually need a warrant
- **Inside Mobile Devices**
  - Mobile devices can range from simple phones to small computers, also called smart phones.
  - The hardware consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces (such as keypads,

cameras, and GPS devices), and an LCD display. Many have removable memory cards, and Bluetooth and Wi-Fi are now included in some mobile devices, too.

- Most basic phones have a proprietary OS, although smart phones use the same OSs as PCs (or stripped-down versions of them). These OSs include Linux, Windows Mobile, RIM OS, Palm OS, Symbian OS, and, with the introduction of the Apple iPhone, a version of Mac OS X.
- Typically, phones store system data in electronically erasable programmable read only memory (EEPROM), which enables service providers to reprogram phones without having to access memory chips physically.

SIM Cards Subscriber identity module (SIM) cards are found most commonly in GSM devices and consist of a microprocessor and 16 KB to 4 MB EEPROM. There are also high-capacity, high-density, super, and mega SIM cards that boast as high as 1 GB EEPROM. SIM cards are similar to standard memory cards, except the connectors are aligned differently.

The SIM card is necessary for the ME to work and serves these additional purposes:

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

SIM cards come in two sizes, but the most common is the size of a standard U.S. postage stamp and about 0.75 mm thick. Portability of information is what makes SIM cards so versatile.

By switching a SIM card between compatible phones, users can move their information to another phone automatically without having to notify the service provider.

Inside PDAs

Personal digital assistants (PDAs) can still be found as separate devices from mobile phones. Most users carry them instead of a laptop to keep track of appointments, deadlines, address books, and so forth. Palm Pilot and Microsoft Pocket PC were popular models when PDAs came on the market in the 1990s, and standalone PDAs are still made by companies such as Palm, Sharp, and HP.

A number of peripheral memory cards are used with PDAs:

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

Understanding Acquisition Procedures for Cell Phones and Mobile Devices All mobile devices have volatile memory, so making sure they don't lose power before you can retrieve RAM data is critical. At the investigation scene, determine whether the device is on or off. If it's off, leave it off, but find the recharger and attach it as soon as possible. If the device is on, check the LCD display for the battery's current charge level. Because mobile devices are often designed to synchronize with applications on a user's PC, any mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately.

The alternative is to isolate the device from incoming signals with one of the following options:

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

When you're back in the forensics lab, you need to assess what can be retrieved.

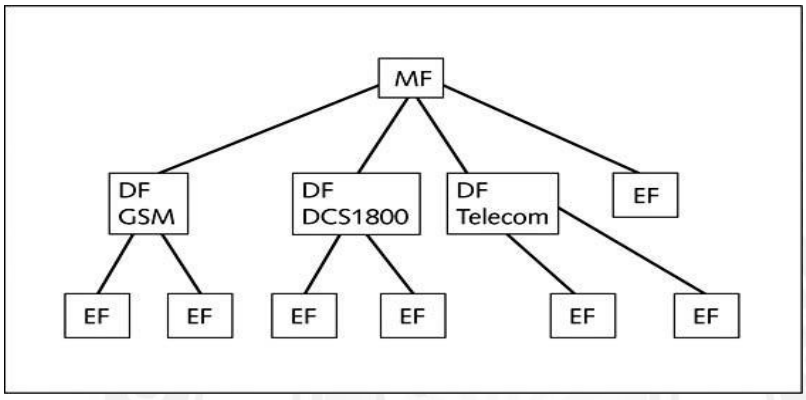
Knowing where information is stored is critical. You should check these four areas:

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

✓ Memory storage on a mobile device is usually implemented as a combination of volatile and nonvolatile memory.

✓ Volatile memory requires power to maintain its contents, but nonvolatile memory does not.

- ✓ Although the specific locations of data vary from one phone model to the next, volatile memory usually contains data that changes frequently, such as missed calls, text messages, and sometimes even user files.
- ✓ Nonvolatile memory, on the other hand, contains OS files and stored user data, such as a personal information manager (PIM) and backed-up files.



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

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

Mobile Forensics Equipment

- ✓ Mobile forensics is such a new science that many of the items you're accustomed to retrieving from computers, such as deleted files, aren't available on mobile devices.
- ✓ The biggest challenge is dealing with constantly changing models of cell phones.
- ✓ The first step is identifying the mobile device. Most users don't alter their devices, but some file off serial numbers, change the display to show misleading data, and so on.
- ✓ When attempting to identify a phone, you can make use of several online sources, such as www.cellphoneshop.com, www.phonescoop.com, and www.mobileforensicscentral.com.
- ✓ The next step is to attach the phone to its power supply and connect the correct cables.

- ✓ Often you have to rig cables to connect to devices because cables for the model you're investigating are not available. U.S. companies usually don't supply cables for phones not commonly used in the United States, but the reverse is true for companies based in Europe.
- ✓ Some vendors have toolkits with an array of cables you can use (discussed later in —Mobile Forensics Tools).
- ✓ After you've connected the device, start the forensics program and begin downloading the available information.

SIM Card Readers

- ✓ **SIM Card Readers** With GSM phones and many newer models of mobile devices, the next step is accessing the SIM card, which you can do by using a combination hardware/ software device called a SIM card reader.
- ✓ The general procedure is as follows:
    1. Remove the back panel of the device.
    2. Remove the battery.
    3. Under the battery, remove the SIM card from its holder.
    4. Insert the SIM card into the card reader, which you insert into your forensic workstation's USB port.

iPhone Forensics

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

Mobile Forensics Tools

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

SIMCon's features include the following:

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