Guide to Computer Forensics and Investigations
Fourth Edition

Chapter 13

Cell Phone and Mobile Devices Forensics

Objectives

- Explain the basic concepts of mobile device forensics

- Describe procedures for acquiring data from cell phones and mobile devices

Understanding Mobile Device Forensics

- People store a wealth of information on cell phones
  - People don't think about securing their cell phones
- Items stored on cell phones:
  - Incoming, outgoing, and missed calls
  - Text and Short Message Service (SMS) messages
  - E-mail
  - Instant-messaging (IM) logs
  - Web pages
  - Pictures

Understanding Mobile Device Forensics (continued)

- Items stored on cell phones: (continued)
  - Personal calendars
  - Address books
  - Music files
  - Voice recordings
- Investigating cell phones and mobile devices is one of the most challenging tasks in digital forensics

Mobile Phone Basics

- Mobile phone technology has advanced rapidly

- Three generations of mobile phones:
  - Analog
  - Digital personal communications service (PCS)
  - **Third-generation (3G)**
    - 3G offers increased bandwidth

- Several digital networks are used in the mobile phone industry

Mobile Phone Basics (continued)

Table 13-1 Digital networks

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during WWII, this technology was patented by Qualcomm after the war. One of the most common digital networks, it uses the full radio frequency spectrum to define channels. Sprint and Verizon, for example, use CDMA networks.
Global System for Mobile Communications (GSM)	The other most common digital network is used by Cingular AT&T and T-Mobile and is the standard in Europe and Asia.
Time Division Multiple Access (TDMA)	This digital network refers to 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 proprietary protocol was developed by Motorola. It combines several services, including data transmission, into one network.
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.

Mobile Phone Basics (continued)

- Main components used for communication:
  - Base transceiver station (BTS)
  - Base station controller (BSC)
  - Mobile switching center (MSC)

Inside Mobile Devices

- Mobile devices can range from simple phones to small computers
  - Also called **smart phones**
- Hardware components
  - Microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces, and an LCD display
- Most basic phones have a proprietary OS
  - Although smart phones use the same OSs as PCs

Inside Mobile Devices (continued)

- Phones store system data in **electronically erasable programmable read-only memory (EEPROM)**
  - Enables service providers to reprogram phones without having to physically access memory chips
- OS is stored in ROM
  - Nonvolatile memory

Inside Mobile Devices (continued)

- **Subscriber identity module (SIM) cards**
  - Found most commonly in GSM devices
  - Microprocessor and from 16 KB to 4 MB EEPROM
  - GSM refers to mobile phones as "mobile stations" and divides a station into two parts:
    - The SIM card and the mobile equipment (ME)
  - SIM cards come in two sizes
  - Portability of information makes SIM cards versatile

Inside Mobile Devices (continued)

- **Subscriber identity module (SIM) cards** (continued)
  - Additional SIM card purposes:
    - Identifies the subscriber to the network
    - Stores personal information
    - Stores address books and messages
    - Stores service-related information

Inside PDAs

- **Personal digital assistants (PDAs)**
  - Can be separate devices from mobile phones
  - Most users carry them instead of a laptop
- PDAs house a microprocessor, flash ROM, RAM, and various hardware components
- The amount of information on a PDA varies depending on the model
- Usually, you can retrieve a user's calendar, address book, Web access, and other items

Inside PDAs (continued)

- Peripheral memory cards are used with PDAs
  - Compact Flash (CF)
  - MultiMedia Card (MMC)
  - Secure Digital (SD)
- Most PDAs synchronize with a computer
  - Built-in slots for that purpose

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- The main concerns with mobile devices are loss of power and synchronization with PCs

- All mobile devices have volatile memory
  - Making sure they don't lose power before you can retrieve RAM data is critical

- Mobile device attached to a PC via a cable or cradle/docking station should be disconnected from the PC immediately

- Depending on the warrant or subpoena, the time of seizure might be relevant

Understanding Acquisition Procedures for Cell Phones and Mobile Devices (continued)

- Messages might be received on the mobile device after seizure

- Isolate the device from incoming signals with one of the following options:
  - Place the device in a paint can
  - Use the Paraben Wireless StrongHold Bag
  - Use eight layers of antistatic bags to block the signal

- The drawback to using these isolating options is that the mobile device is put into roaming mode
  - Which accelerates battery drainage

Understanding Acquisition Procedures for Cell Phones and Mobile Devices (continued)

- Check these areas in the forensics lab :
  - Internal memory
  - SIM card
  - Removable or external memory cards
  - System server
- Checking system servers requires a search warrant or subpoena
- SIM card file system is a hierarchical structure

Understanding Acquisition Procedures for Cell Phones and Mobile Devices (continued)
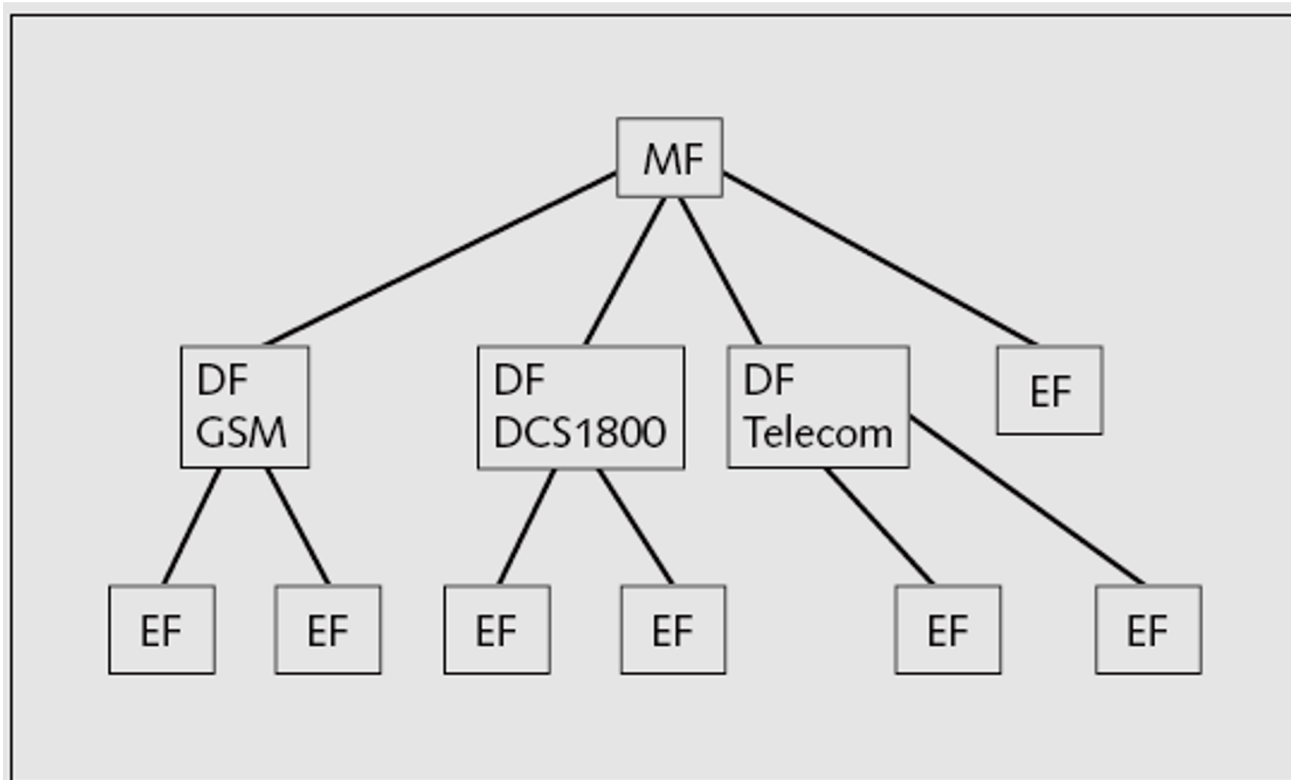
Figure 13-1   SIM file structure

Understanding Acquisition Procedures for Cell Phones and Mobile Devices (continued)

- Information that can be retrieved:
  - Service-related data, such as identifiers for the SIM card and the subscriber
  - Call data, such as numbers dialed
  - Message information
  - Location information
- If power has been lost, PINs or other access codes might be required to view files

Mobile Forensics Equipment

- Mobile forensics is a new science

- Biggest challenge is dealing with constantly changing models of cell phones

- When you're acquiring evidence, generally you're performing two tasks:

  - Acting as though you're a PC synchronizing with the device (to download data)

  - Reading the SIM card

- First step is to identify the mobile device

Mobile Forensics Equipment (continued)

- Make sure you have installed the mobile device software on your forensic workstation

- Attach the phone to its power supply and connect the correct cables

- After you've connected the device
  - Start the forensics program and begin downloading the available information

Mobile Forensics Equipment (continued)

- SIM card readers
  - A combination hardware/software device used to access the SIM card
  - You need to be in a forensics lab equipped with appropriate antistatic devices
  - General procedure is as follows:
    - Remove the back panel of the device
    - Remove the battery
    - Under the battery, remove the SIM card from holder
    - Insert the SIM card into the card reader

Mobile Forensics Equipment (continued)

- SIM card readers (continued)
  - A variety of SIM card readers are on the market
    - Some are forensically sound and some are not
  - Documenting messages that haven't been read yet is critical
    - Use a tool that takes pictures of each screen

- Mobile forensics tools
  - Paraben Software Device Seizure Toolbox
  - BitPim

Mobile Forensics Equipment (continued)

- Mobile forensics tools (continued)
  - MOBILedit!
  - SIMCon
- Software tools differ in the items they display and the level of detail
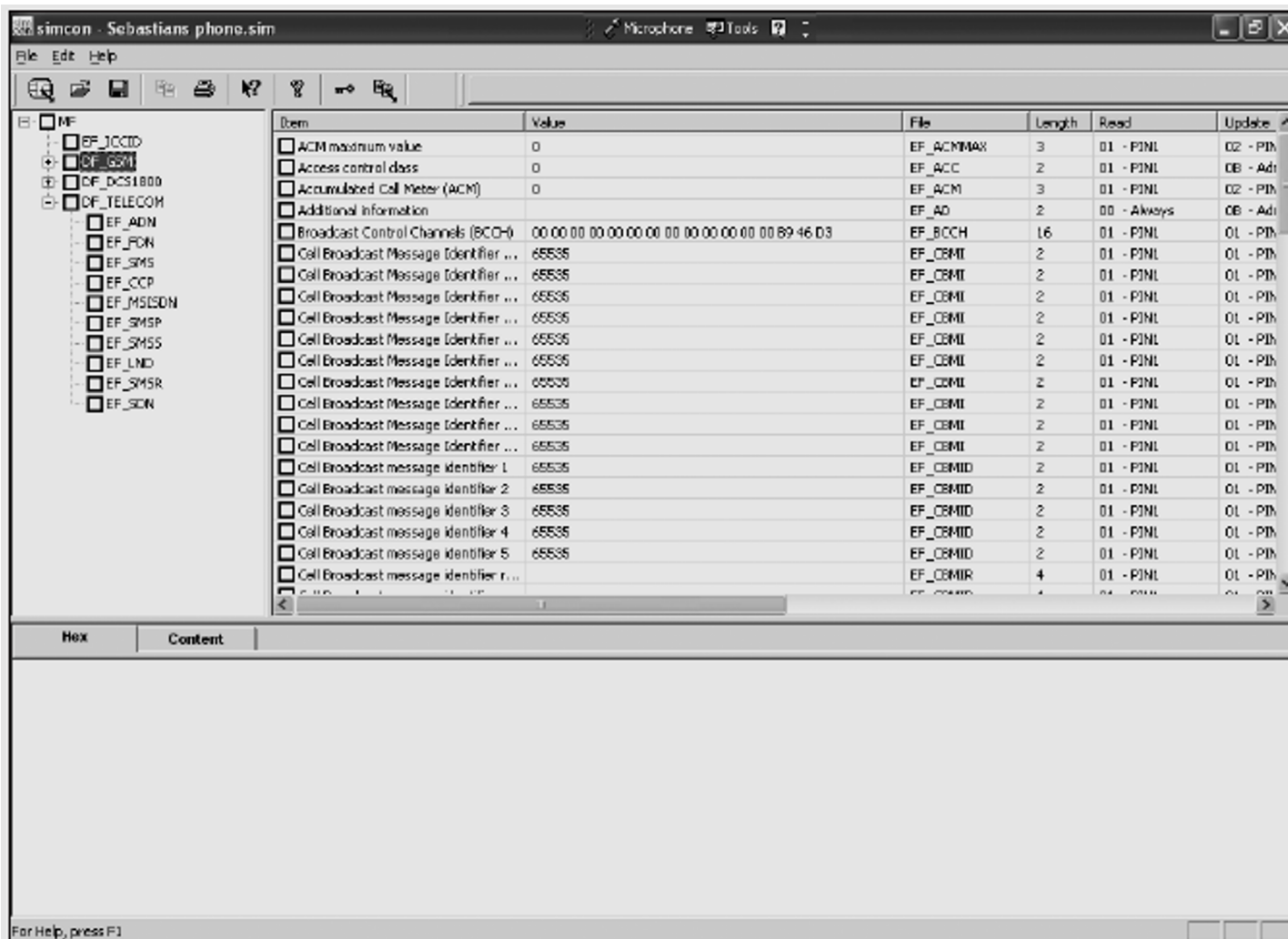
**Figure 13-2** File structure of a SIM card viewed in SIMCon

Guide to Computer Forensics and Investigations 24
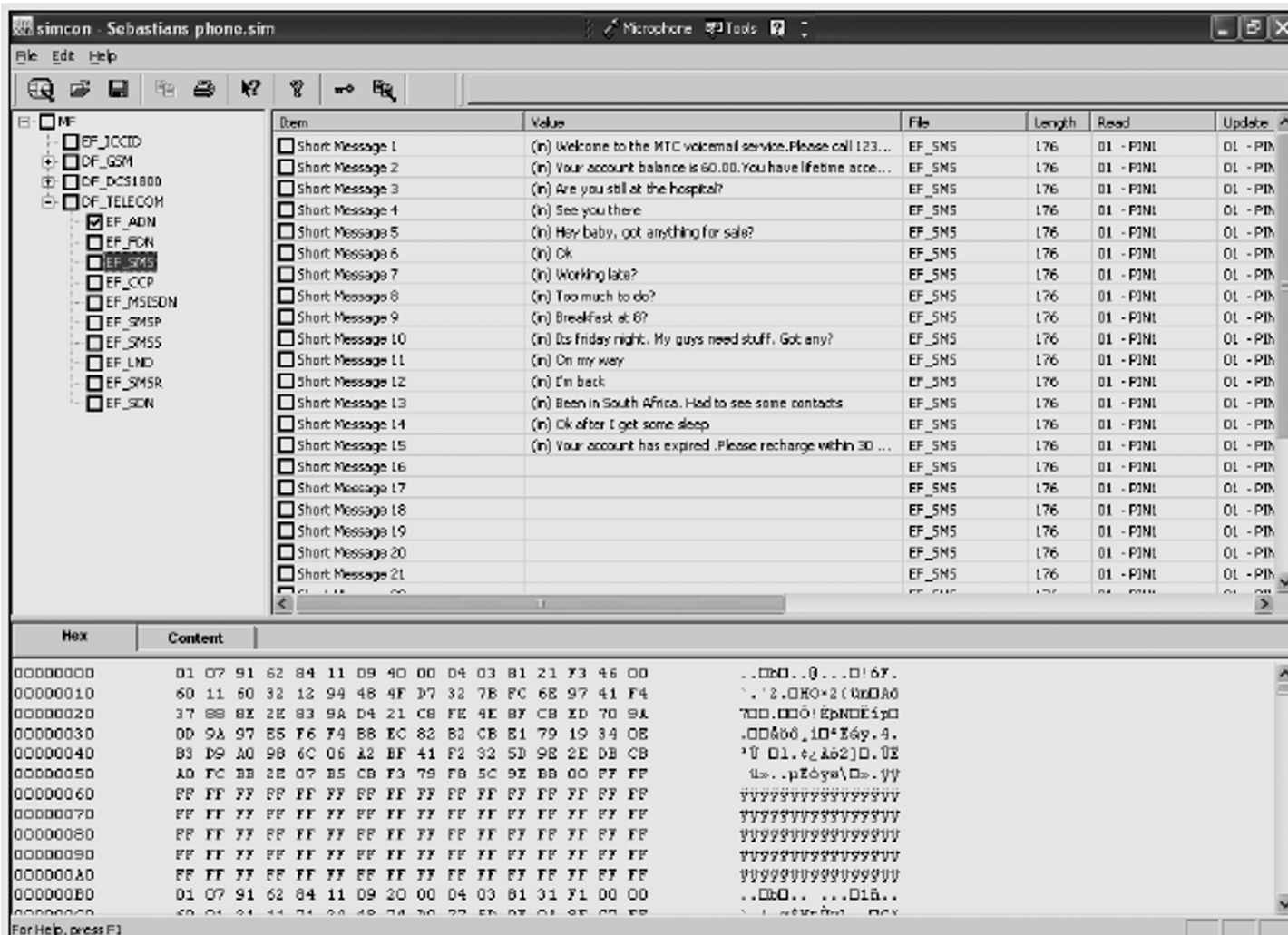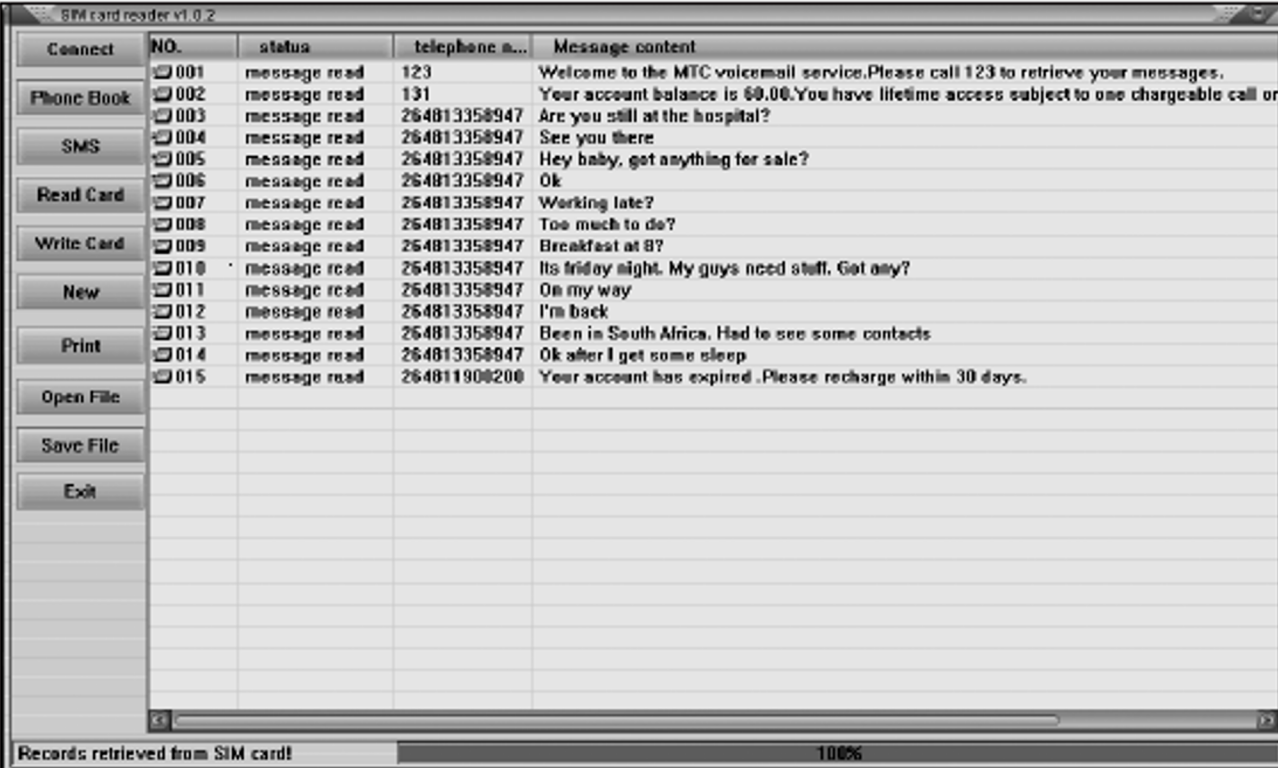
Figure 13-3 SMS messages viewed in SIMCon

Mobile Forensics Equipment (continued)

Figure 13-4 Information available in Sim Card Reader

Summary

- People store a wealth of information on their cell phones

- Three generations of mobile phones: analog, digital personal communications service (PCS), and third-generation (3G)

- Mobile devices range from basic, inexpensive phones used primarily for phone calls to smart phones

Summary (continued)

- Data can be retrieved from several different places in phones

- Personal digital assistants (PDAs) are still in widespread use and often contain a lot of personal information

- As with computers, proper search and seizure procedures must be followed for mobile devices

Summary (continued)

- To isolate a mobile device from incoming messages, you can place it in a specially treated paint can, a wave-blocking wireless evidence bag, or eight layers of antistatic bags
- SIM cards store data in a hierarchical file structure
- Many software tools are available for reading data stored in mobile devices