

# *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

# Data on iPhones

- Screenshots of every map viewed
- iPhone photos have GPS location data embedded
- Apps store browsing history
- iPhone stores everything you type, like a keylogger
  - Link Ch 13a
- iPhone also stores screenshots after each action, in order to create an aesthetically pleasing shrinking effect (link Ch 13b)

# Banking on iPhones

## iPhone Banking App Automatically Deposits Checks Via Photos

Your iPhone's camera—not just for Twitpic anymore?

By [Corinne Iozzio](#) Posted 08.10.2009 at 1:30 pm [0 Comments](#)



- Link Ch 13c

# 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.

# 4G Networks

- Orthogonal Frequency Division Multiplexing (OFDM)
  - Uses power more efficiently, and is more immune to interference
- Mobile WiMAX
  - Used by Sprint, will support speeds up to 12 Mbps
- Ultra Mobile Broadband (UTMS)
  - Also known as CDMA2000 EV-DO
  - Will support speeds up to 100 Mbps

# 4G Networks

- Multiple Input Multiple Output (MIMO)
  - Will support speeds up to 312 Mbps
- Long Term Evolution (LTE)
  - Will support up to 144 Mbps

# Mobile Phone Basics (continued)

- Main components used for communication:
  - Base transceiver station (BTS)
    - Cell phone tower and associated equipment
  - Base station controller (BSC)
    - Hardware & software that controls the BTS
  - Mobile switching center (MSC)
    - Routes calls
    - Has a database of subscribers with account and location data

# 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 stripped-down versions of PC operating systems

# 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
    - Sometimes even more, up to 1 GB 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

# Understanding Acquisition Procedures for Cell Phones and Mobile Devices

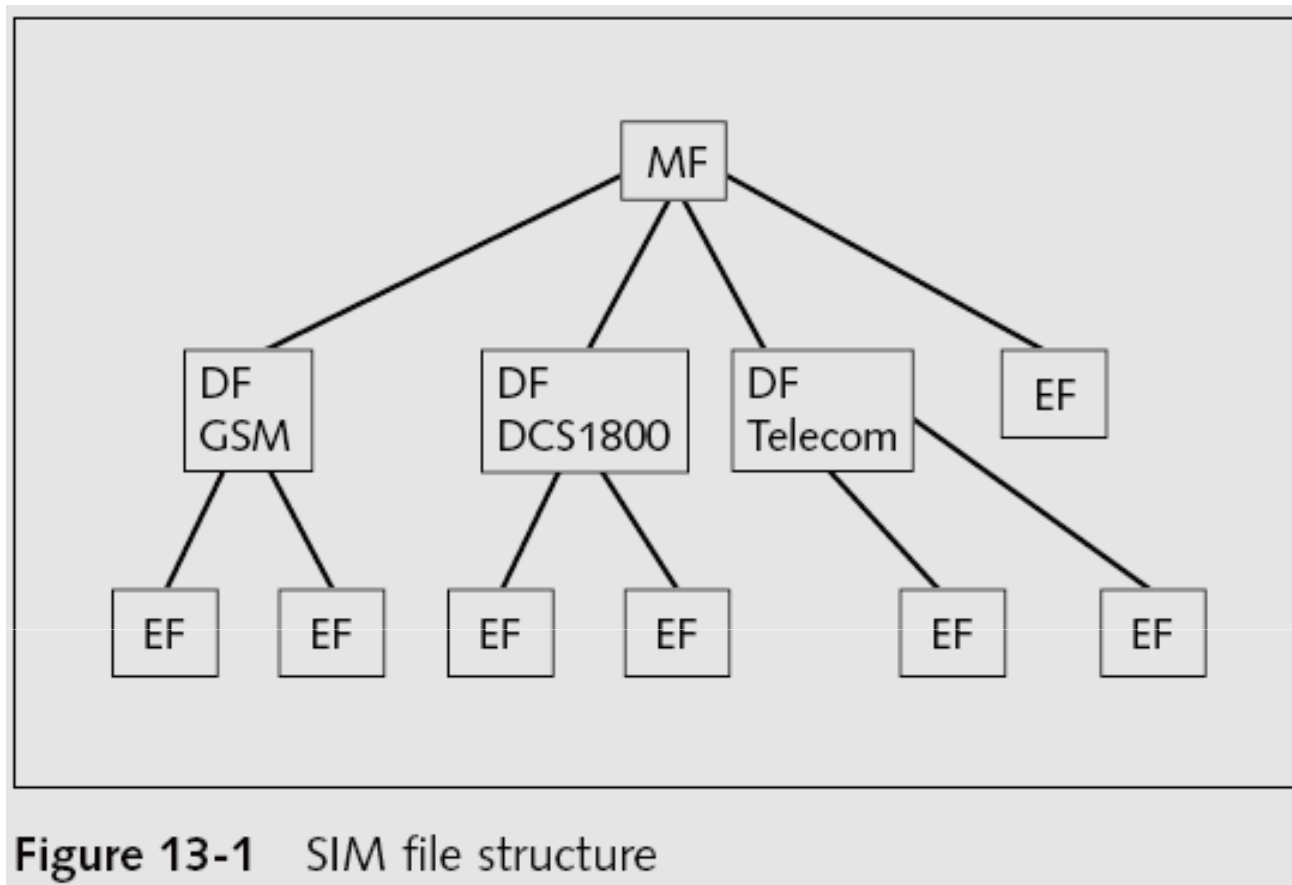
- The main concerns with mobile devices are loss of power and synchronization with PCs
- All mobile devices have volatile memory
  - Making sure they don't lose power before you can retrieve RAM data is critical
- Mobile device attached to a PC via a cable or cradle/docking station should be disconnected 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



- MF: root of the system
- DF: directory files
- EF: elementary data



# 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
- Blackberries may require special hardware

# iPhone Forensics

- MacLockPick II
  - Uses backup files
  - It can't recover deleted files
- MDBackUp Extract
  - Analyzes the iTunes mobile sync backup directory

# iPhone Spy

- Link Ch 13d



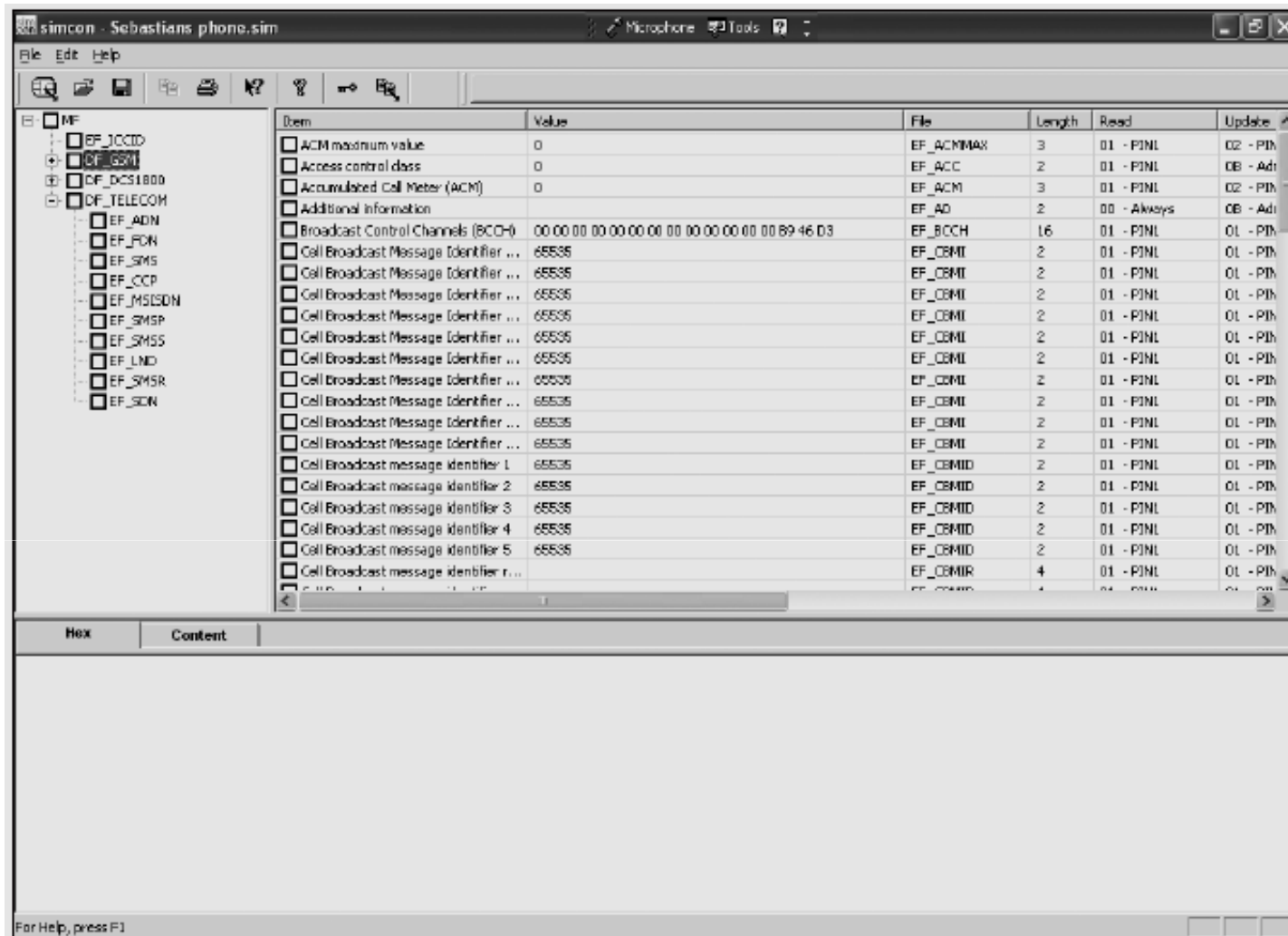
# Mobile Forensics Tools

- Paraben Software Device Seizure Toolbox
  - Contains cables, SIM card readers, and more
- Data Pilot
  - Similar to Paraben
- BitPim
  - Can view data on many phones, but it's not intended for forensics
- MOBILedit!
  - Has a write-blocker



# Mobile Forensics Tools

- SIMCon
  - Reads files on SIM cards
  - Recovers deleted text messages
  - Archives files with MD5 and SHA-1 hashes
- 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

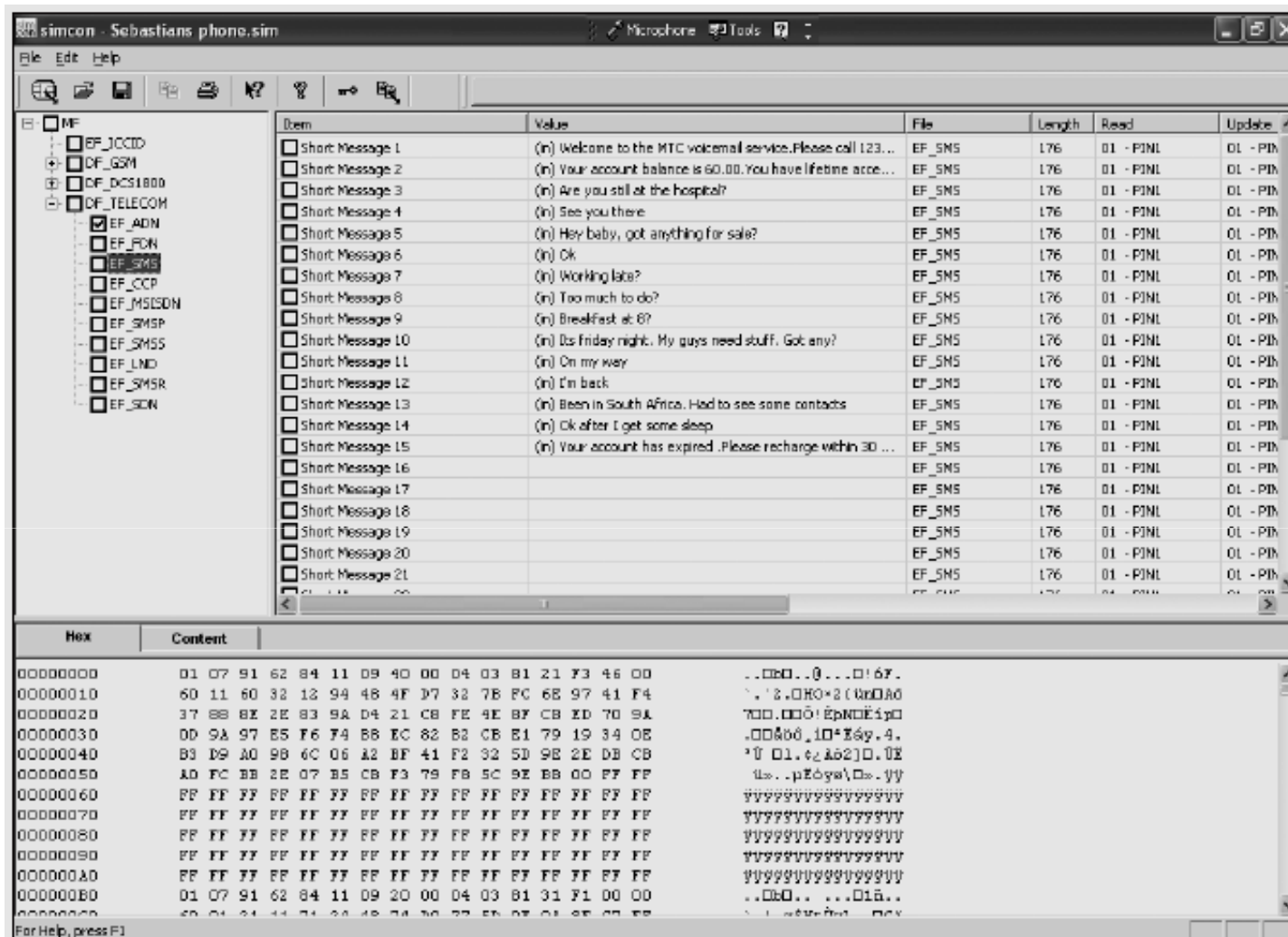
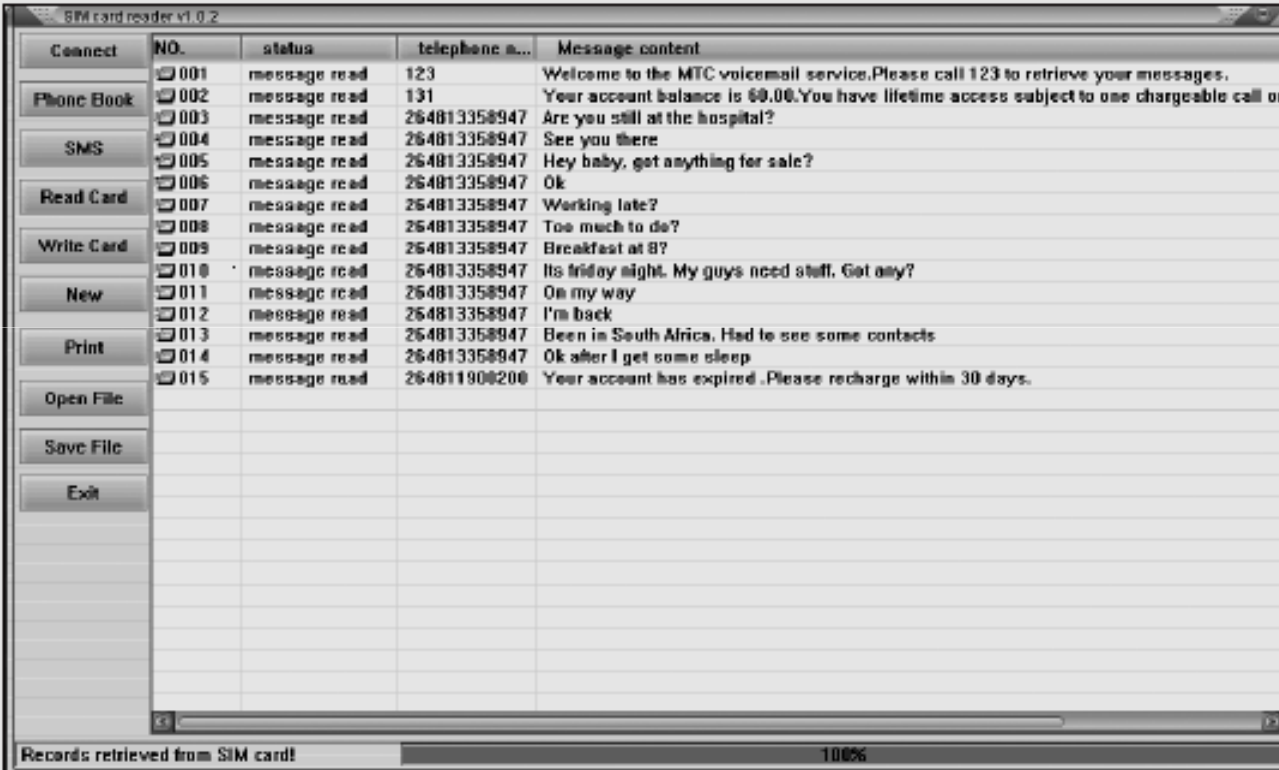


Figure 13-3 SMS messages viewed in SIMCon

# Mobile Forensics Equipment (continued)



The screenshot shows a software window titled "SIM card reader v1.0.2". On the left is a sidebar with buttons: Connect, Phone Book, SMS, Read Card, Write Card, New, Print, Open File, Save File, and Exit. The main area displays a table with four columns: NO., status, telephone n..., and Message content. The table contains 15 rows of message data. At the bottom, a status bar indicates "Records retrieved from SIM card!" and "100%".

NO.	status	telephone n...	Message content
001	message read	123	Welcome to the MTC voicemail service. Please call 123 to retrieve your messages.
002	message read	131	Your account balance is \$0.00. You have lifetime access subject to one chargeable call or
003	message read	264813358947	Are you still at the hospital?
004	message read	264813358947	See you there
005	message read	264813358947	Hey baby, got anything for sale?
006	message read	264813358947	Ok
007	message read	264813358947	Working late?
008	message read	264813358947	Too much to do?
009	message read	264813358947	Breakfast at 8?
010	message read	264813358947	Its Friday night. My guys need stuff. Got any?
011	message read	264813358947	On my way
012	message read	264813358947	I'm back
013	message read	264813358947	Been in South Africa. Had to see some contacts
014	message read	264813358947	Ok after I get some sleep
015	message read	264811900200	Your account has expired. Please recharge within 30 days.

Figure 13-4 Information available in Sim Card Reader