Guide to Computer Forensics and Investigations Fourth Edition

Chapter 13

Cell Phone and Mobile Devices Forensics

Objectives

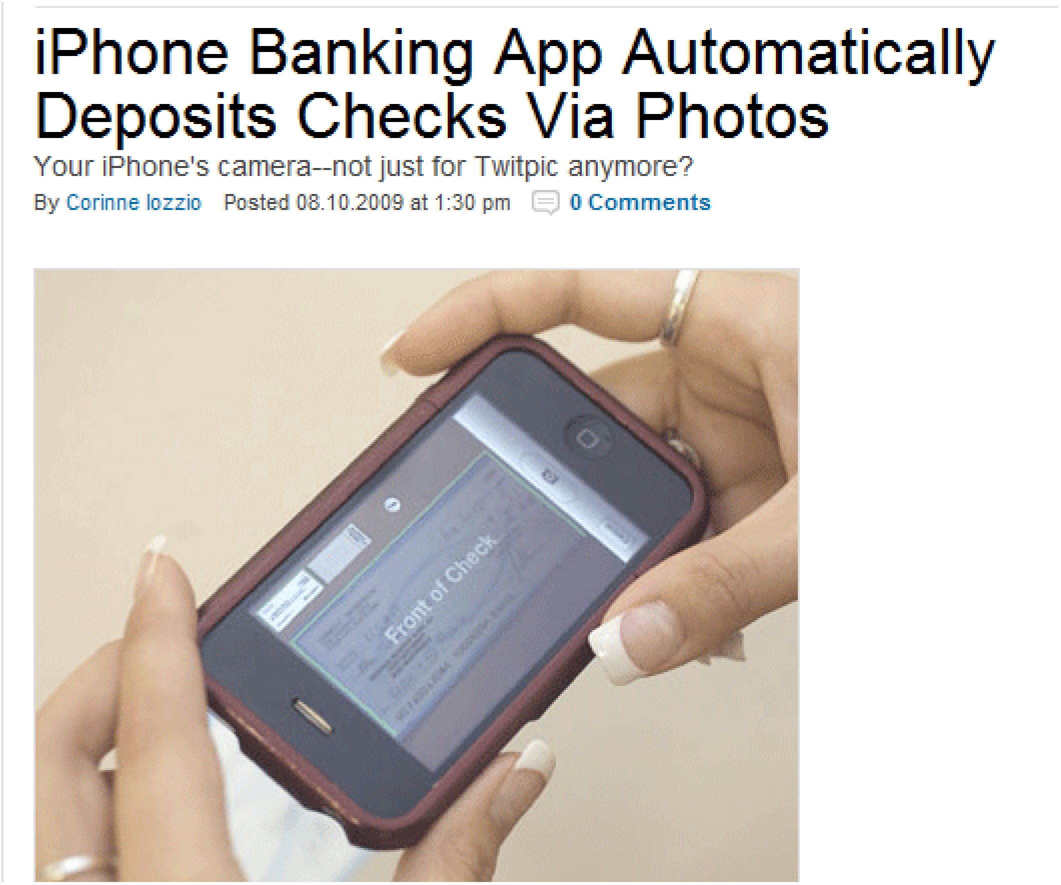
- Explain the basic concepts of mobile device forensics
- Describe procedures for acquiring data from cell phones and mobile devices

Understanding Mobile Device Forensics

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)

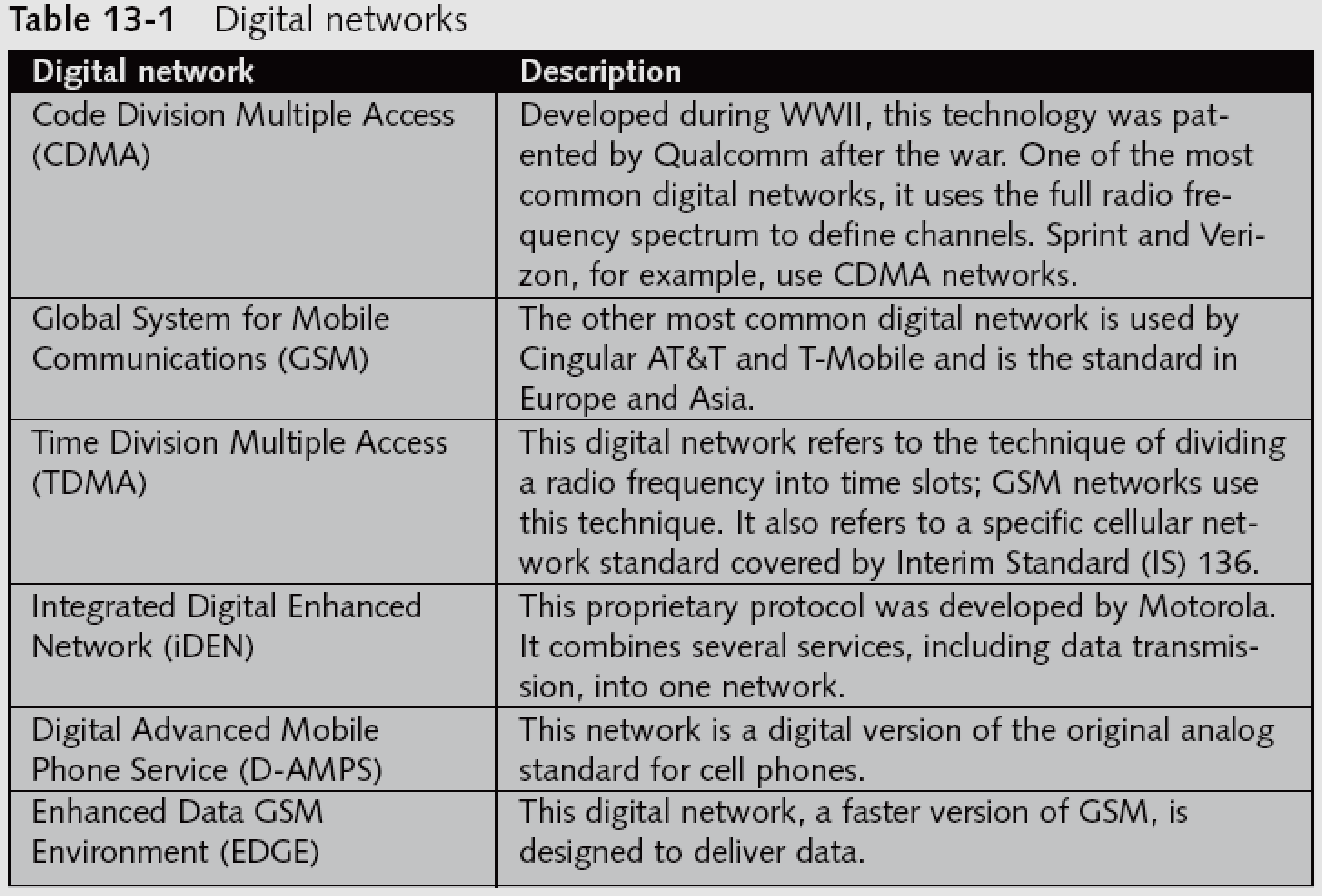


Table 13-1 Digital networks

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

SIM Card

(from Wikipedia)

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 go 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

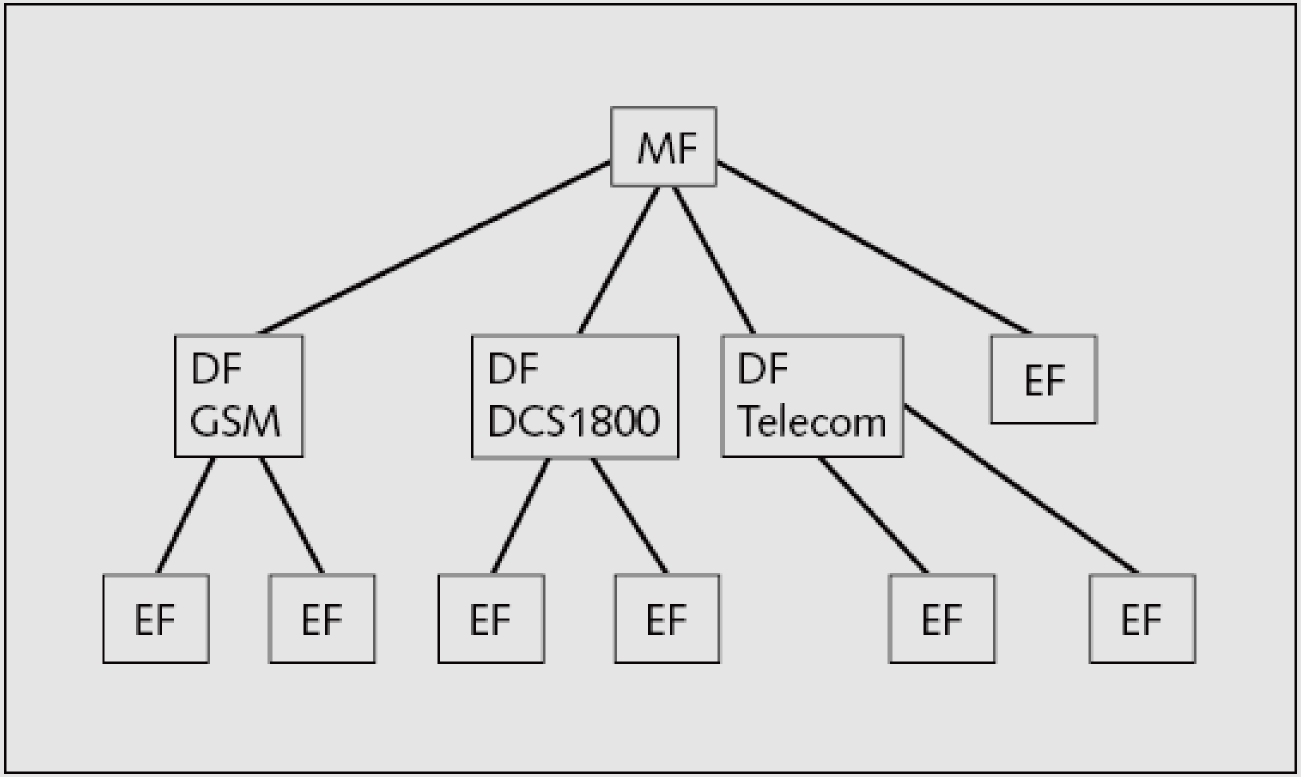


Figure 13-1 SIM file structure

- 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)

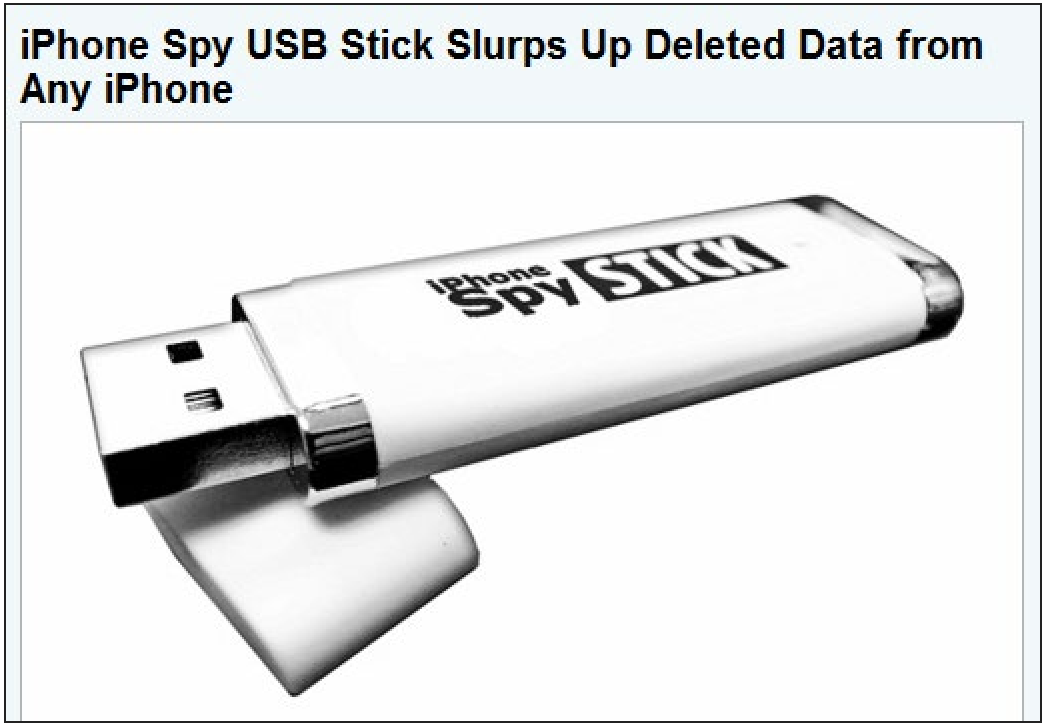
- SIM card readers (continued)
  - A variety of SIM card readers are on the market
    - Some are forensically sound and some are not
  - Documenting messages that haven’t been read yet is critical
    - Use a tool that takes pictures of each screen
- Blackberries may require special hardware

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



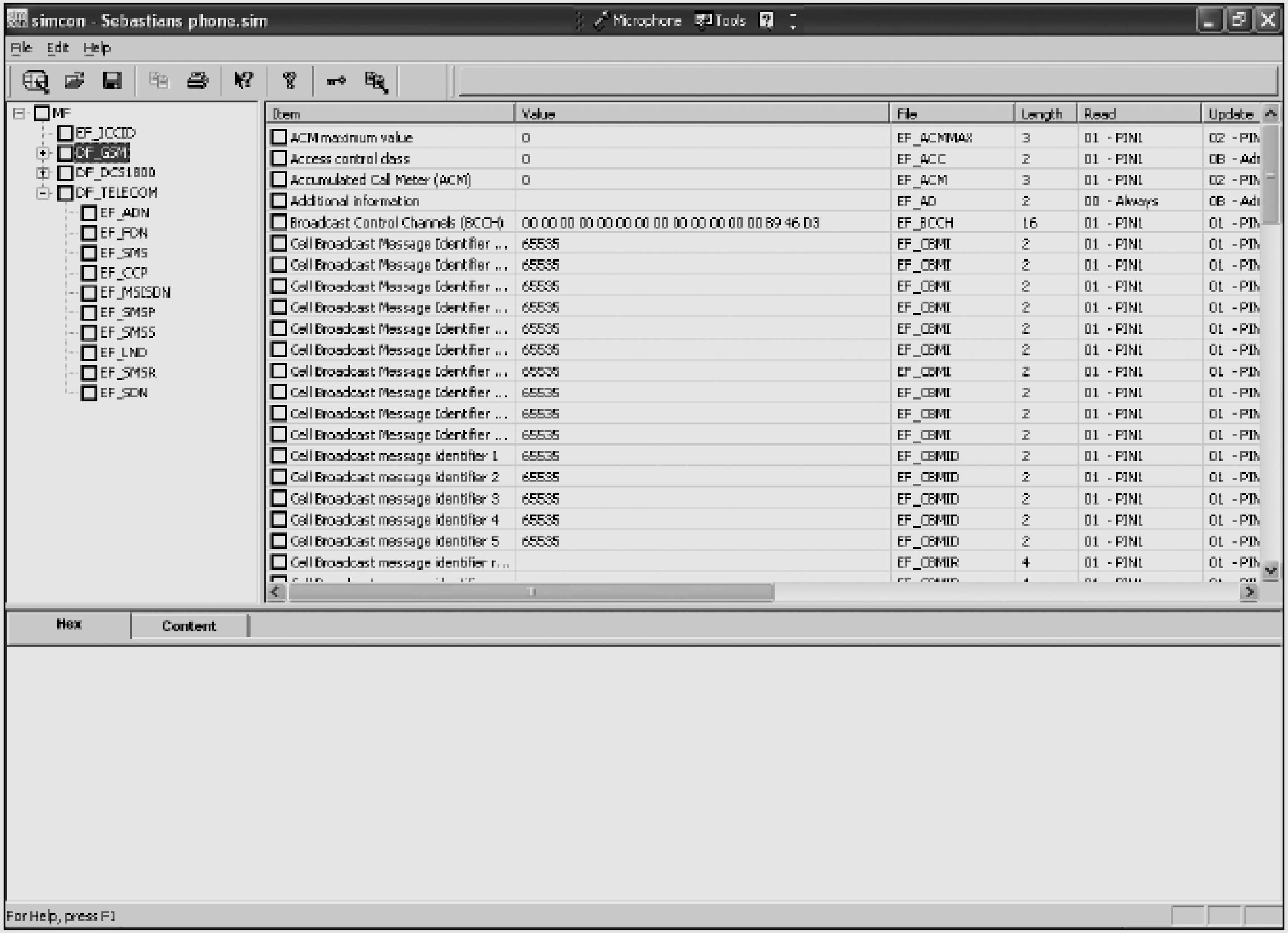
iPhone Spy USB Stick Slurps Up Deleted Data from Any iPhone

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

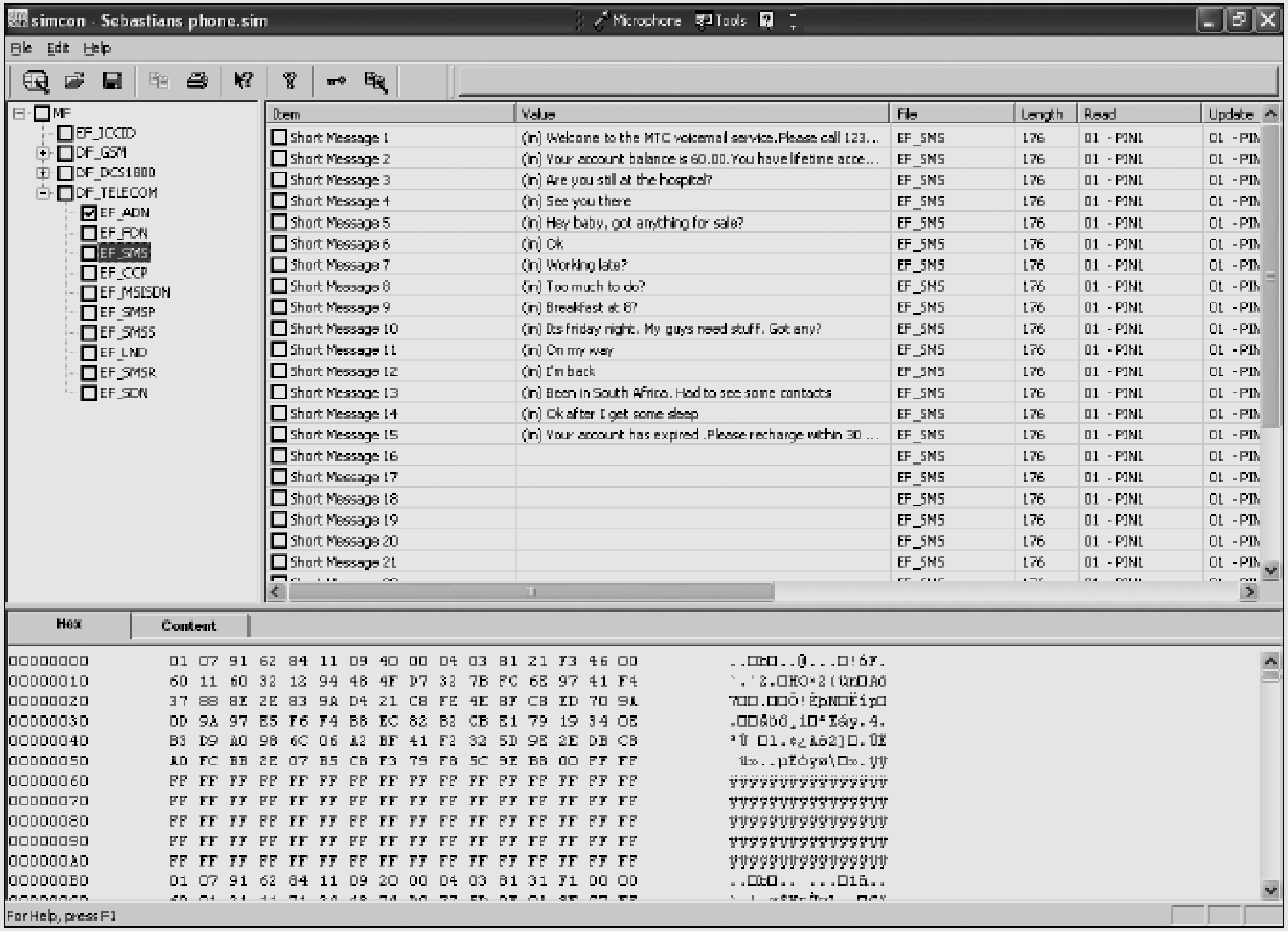
Mobile Forensics Tools

- SIMCon
  - Reads files on SIM cards
  - Recoveres deleted text messages
  - Archives files with MD5 and SHA-1 hashes
- Software tools differ in the items they display and the level of detail



Item	Value	File	Length	Read	Update
□ ACM maximum value	0	EF_ACMMAX	3	01 - PIN1	02 - PIN
□ Access control class	0	EF_ACC	2	01 - PIN1	0B - Adr
□ Accumulated Call Meter (ACM)	0	EF_ACM	3	01 - PIN1	02 - PIN
□ Additional information		EF_AD	2	00 - Always	0B - Adr
□ Broadcast Control Channels (BCCH)	00 00 00 00 00 00 00 00 00 00 00 00 00 89 46 D3	EF_BCCH	16	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast Message Identifier ...	65535	EF_CBMI	2	01 - PIN1	01 - PIN
□ Cell Broadcast message identifier 1	65535	EF_CBMID	2	01 - PIN1	01 - PIN
□ Cell Broadcast message identifier 2	65535	EF_CBMID	2	01 - PIN1	01 - PIN
□ Cell Broadcast message identifier 3	65535	EF_CBMID	2	01 - PIN1	01 - PIN
□ Cell Broadcast message identifier 4	65535	EF_CBMID	2	01 - PIN1	01 - PIN
□ Cell Broadcast message identifier 5	65535	EF_CBMID	2	01 - PIN1	01 - PIN
□ Cell Broadcast message identifier r...		EF_CBMIR	4	01 - PIN1	01 - PIN

Figure 13-2 File structure of a SIM card viewed in SIMCon

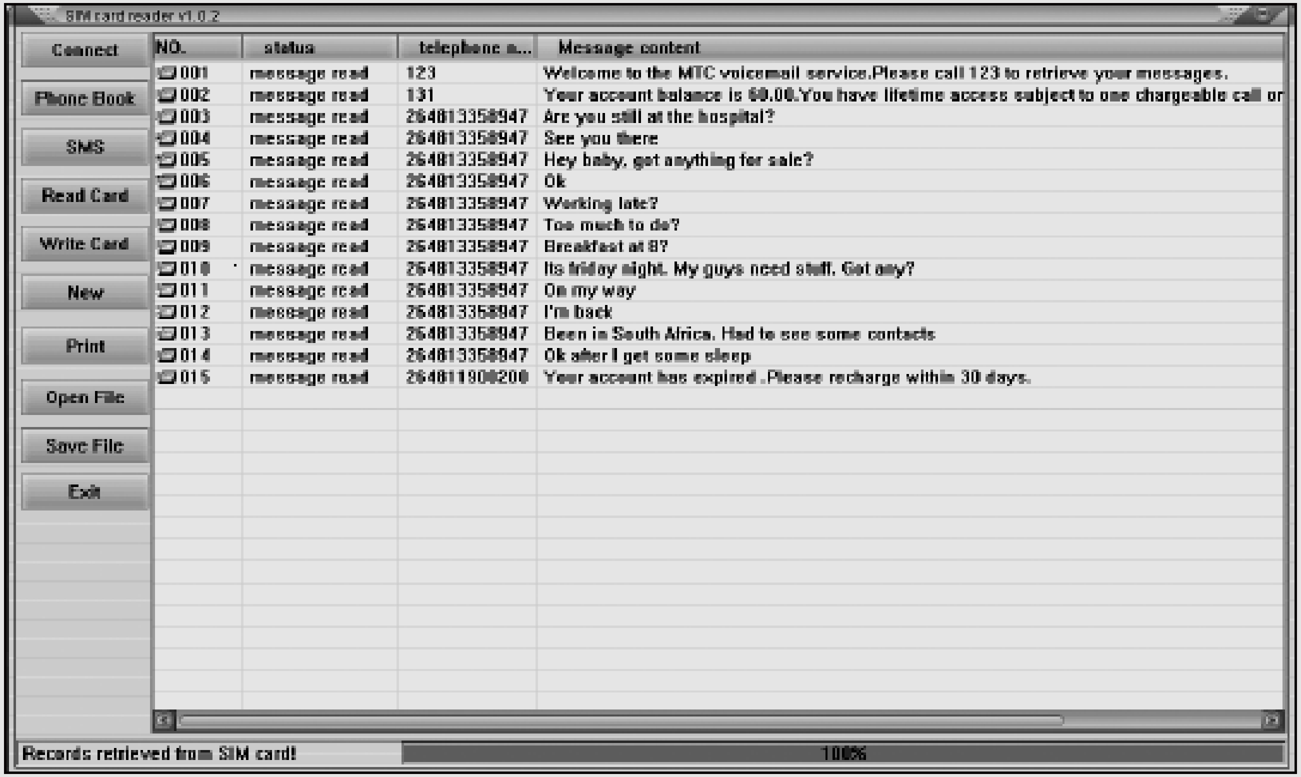


Item	Value	File	Length	Read	Update
□ Short Message 1	(in) Welcome to the MTC voicemail service.Please call 123...	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 2	(in) Your account balance is 60.00.You have lifetime acce...	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 3	(in) Are you still at the hospital?	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 4	(in) See you there	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 5	(in) Hey baby, got anything for sale?	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 6	(in) Ok	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 7	(in) Working late?	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 8	(in) Too much to do?	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 9	(in) Breakfast at 8?	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 10	(in) Its friday night. My guys need stuff. Got any?	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 11	(in) On my way	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 12	(in) I'm back	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 13	(in) Been in South Africa. Had to see some contacts	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 14	(in) Ok after I get some sleep	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 15	(in) Your account has expired .Please recharge within 30 ...	EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 16		EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 17		EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 18		EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 19		EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 20		EF_SMS	176	01 - PIN1	01 - PIN
□ Short Message 21		EF_SMS	176	01 - PIN1	01 - PIN

```
00000000      01 07 91 62 84 11 09 40 00 04 03 81 21 F3 46 00      ..□b□..@...□!óF.
00000010      60 11 60 32 12 94 48 4F D7 32 7B FC 6E 97 41 F4      `.`2.□HO×2{ün□Aô
00000020      37 88 8E 2E 83 9A D4 21 C8 FE 4E BF CB ED 70 9A      7□□.□□Ô!ÈþN¿Ëíp□
00000030      0D 9A 97 E5 F6 F4 B8 EC 82 B2 CB E1 79 19 34 0E      .□□åöô¸ì□²Ëáy.4.
00000040      B3 D9 A0 98 6C 06 A2 BF 41 F2 32 5D 9E 2E DB CB      ³Ù □l.¢¿Aò2]□.ÛË
00000050      A0 FC BB 2E 07 B5 CB F3 79 F8 5C 9E BB 00 FF FF       ü»..µËóyø\□».ÿÿ
00000060      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF      ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000070      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF      ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000080      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF      ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00000090      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF      ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000A0      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF      ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000000B0      01 07 91 62 84 11 09 20 00 04 03 81 31 F1 00 00      ..□b□.. ...□1ñ..
```

Figure 13-3 SMS messages viewed in SIMCon

Mobile Forensics Equipment (continued)



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 60.00.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.

Records retrieved from SIM card!

100%

Figure 13-4 Information available in Sim Card Reader