Guide to Computer Forensics and Investigations Fifth Edition

Chapter 12
Mobile Device 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 phones
- Items stored on cell phones:
  - Incoming, outgoing, and missed calls
  - Multimedia Message Service (MMS; text messages) and Short Message Service (SMS) messages
  - E-mail accounts
  - Instant-messaging (IM) logs
  - Web pages
  - Pictures, video, and music files

Understanding Mobile Device Forensics

- Items stored on cell phones: (cont'd)
  - Calendars and address books
  - Social media account information
  - GPS data
  - Voice recordings and voicemail
- A search warrant is needed to examine mobile devices because they can contain so much information

Understanding Mobile Device Forensics

- Investigating cell phones and mobile devices is one of the more challenging tasks in digital forensics
  - No single standard exists for how and where phones store messages
  - New phones come out about every six months and they are rarely compatible with previous models

Mobile Phone Basics

- Mobile phone technology has advanced rapidly
- By the end of 2008, mobile phones had gone through three generations:
  - Analog
  - Digital personal communications service (PCS)
- **Third-generation (3G)** introduced new capabilities, such as being able to download while you were walking or in a moving vehicle.
- **Fourth-generation (4G)** was introduced in 2009
- Several digital networks are used in the mobile phone industry

Mobile Phone Basics

Table 12-1 Digital networks

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during World War II, 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. In the United States, Sprint, U.S. Cellular, 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 in the United States 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 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.

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

- 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
  - Available even if the phone loses power

Inside Mobile Devices

- **Personal digital assistants (PDAs)** have been mostly replaced by iPods, iPads, and other mobile devices
- Their use has shifted to more specific markets
  - Such as medical or industrial PDAs
- Peripheral memory cards used with PDAs:
  - *Compact Flash (CF):* CF cards were used for extra storage
  - *MultiMediaCard (MMC):* MMC cards were 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; they're now used on smartphones.

Inside Mobile Devices

- **Subscriber identity module (SIM) cards**
  - Found most commonly in GSM devices
  - Consist of a microprocessor and internal memory
  - 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 flexible

Inside Mobile Devices

- **Subscriber identity module (SIM) cards** (cont'd)
  - The SIM card is necessary for the ME to work and serves these additional purposes:
    - Identifies the subscriber to the network
    - Stores service-related information
    - Can be used to back up the device

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- The main concerns with mobile devices are loss of power, synchronization with cloud services, and remote wiping
- 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 USB cable should be disconnected from the PC immediately
  - Helps prevent synchronization that might occur automatically and overwrite data

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- Depending on the warrant or subpoena, the time of seizure might be relevant
- 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 airplane mode
  - Place the device in a paint can
  - Use the Paraben Wireless StrongHold Bag
  - Turn the device off

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- The drawback of using these isolating options is that the mobile device is put into roaming mode
  - Accelerates battery drainage
- SANS DFIR Forensics recommends:
  - If device is on and unlocked - isolate it from the network, disable the screen lock, remove passcode
  - If device is on and locked - what you can do varies depending on the type of device
  - If device is off - attempt a physical static acquisition and turn the device on

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- Check these areas in the forensics lab :
  - Internal memory
  - SIM card
  - Removable or external memory cards
  - Network provider
- Checking network provider requires a search warrant or subpoena
  - A new complication has surfaced because backups might be stored in a cloud provided by the carrier or third party

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- Due to the growing problem of mobile devices being stolen, service providers have started using remote wiping to remove a user's personal information stored on a stolen device
- Memory storage on a mobile device is usually a combination of volatile and nonvolatile memory
- The file system for a SIM card is a hierarchical structure

Understanding Acquisition Procedures for Cell Phones and Mobile Devices

- Information that can be retrieved falls into four categories:
  - 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 an evolving science
- Biggest challenge is dealing with constantly changing phone models
- Procedures for working with mobile forensics software:
  - Identify the mobile device
  - Make sure you have installed the mobile device forensics software
  - Attach the phone to power and connect cables
  - Start the forensics software and download information

Mobile Forensics Equipment

- 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
    - Remove the SIM card from holder
    - Insert the SIM card into the card reader

Mobile Forensics Equipment

- SIM card readers (cont'd)
  - A variety of SIM card readers are available
    - 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
  - AccessData FTK Imager
  - MacLockPick 3.0

Mobile Forensics Equipment

- NIST guidelines list six types of mobile forensics methods:
  - **Manual extraction**
  - **Logical extraction**
  - **Hex dumping and Joint Test Action Group (JTAG) extraction**:
    - involves using a modified boot loader to access the RAM for analysis.
    - The JTAG extraction method gets information from the processor, flash memory, or other physical components.
  - **Chip-off**: requires physically removing flash memory chip and gathering information at the binary level.
  - **Micro read:** looks at logic gates with an electron microscope and can be used even when data has been overwritten on magnetic media.

Mobile Forensics Equipment

- Paraben Software offers several tools:
  - **Device Seizure** - used to acquire data from a variety of phone models
  - **Device Seizure Toolbox** - contains assorted cables, a SIM card reader, and other equipment
- BitPam - used to view data on many CDMA phones
- Cellebrite UFED Forensic System - works on smartphones, PDAs, tablets, and GPS devices
- MOBILedit Forensic - contains a built-in write-blocker

Mobile Forensics Equipment

- SIMcon used to recover files on a GSM/3G SIM or USIM card and includes the following features:
  - Reads files on SIM cards
  - Analyzes file content
  - 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 spreadsheets
  - Supports international character sets

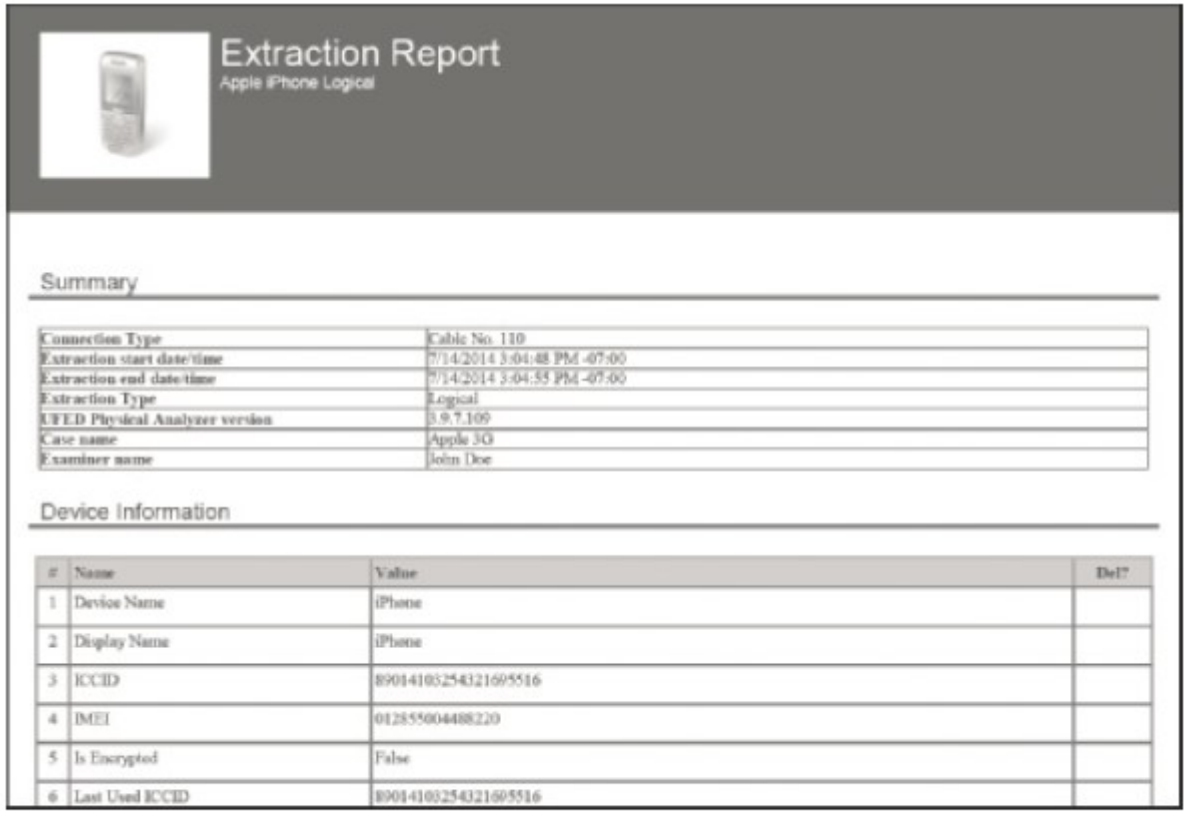
Mobile Forensics Equipment

- Roughly half of Facebook users access their accounts via mobile devices
- Following standard procedures, doing a logical acquisition followed by a physical acquisition, can yield solid evidence

Mobile Forensics Tools in Action

- **Cellebrite is often used by law enforcement**
  - You can determine the device's make and model, hook up the correct cable, turn the device on, and retrieve the data
  - There are more than half a million aps for mobile devices and Cellebrite can analyze data from only a few hundred

Mobile Forensics Tools in Action



Extraction Report

Apple iPhone Logical

Summary

Connection Type	Cable No. 110
Extraction start date/time	7/14/2014 3:04:48 PM -07:00
Extraction end date/time	7/14/2014 3:04:55 PM -07:00
Extraction Type	Logical
UFED Physical Analyzer version	3.9.7.109
Case name	Apple 3G
Examiner name	John Doe

Device Information

#	Name	Value	Del?
1	Device Name	iPhone	
2	Display Name	iPhone	
3	ICCID	8901410325432169551 6	
4	IMEI	012855004488220	
5	Is Encrypted	False	
6	Last Used ICCID	8901410325432169551 6	

Figure 12-2 A Cellebrite report

Source: Cellebrite Mobile Synchronization LTD

Mobile Forensics Tools in Action

	9	Name: clients.plist Path: /Library/Caches/locationd/clients.plist MD5: f8dd4daca97c53c07880b25cd06f5df9 SHA256: 4f341dfec01f3bdf44ee8910e313ea510 65ab526c2deb02b405ffb43b6ab4a2ad	Size (Bytes): 1803 Created: 4/10/2014 3:44:42 PM(UTC+0) Modified: 7/14/2014 9:58:22 PM(UTC+0) Accessed: 7/14/2014 9:58:22 PM(UTC+0)		
	10	Name: ClientTruth.plist Path: /Library/ConfigurationProfiles/ClientTruth.plist MD5: 2def6f04edba79ad13580e17d5f70ee5f SHA256: 97704a8960b4faeceef54397a08ffb5d0 a456247e362735921 5aa2a27df22656e	Size (Bytes): 181 Created: 4/10/2014 3:44:29 PM(UTC+0) Modified: 4/10/2014 3:44:29 PM(UTC+0) Accessed: 4/10/2014 3:44:29 PM(UTC+0)		
	11	Name: com.apple.Accessibility.plist Path: /Library/Preferences/com.apple.Accessibility.plist MD5: 9218fbd80b4ff9d26e6e3c8ab10ad871 SHA256: c1a0df76325b2706fe26167b38439b1e9a a255d57d46e0215cf5767e6195b12b6	Size (Bytes): 288 Created: 7/14/2014 10:03:24 PM(UTC+0) Modified: 7/14/2014 10:03:24 PM(UTC+0) Accessed: 7/14/2014 10:03:24 PM(UTC+0)		
	12	Name: com.apple.accounts.exists.plist Path: /System/Configuration/com.apple.accounts.exists.plist MD5: 16422e4b7e14e9dde66ef53e727ede0f SHA256: a6c9ccd9eedcacdbd6546765a15eb855 0be51beee24e8f8f8ed3e6c27c96c3ed	Size (Bytes): 111 Created: 7/14/2014 9:23:04 PM(UTC+0) Modified: 7/14/2014 9:23:04 PM(UTC+0) Accessed: 7/14/2014 9:23:04 PM(UTC+0)		
	13	Name: com.apple.accountsettings.plist Path: /Library/Preferences/com.apple.accountsettings.plist MD5: b433aabe90564102ad12e4ae589fb524 SHA256: ee1a3d4c3c381c0ee92319dd48e33c4c 0ebce4e48edfc7334fee0848b1fe94a1	Size (Bytes): 4079 Created: 7/14/2014 10:03:46 PM(UTC+0) Modified: 7/14/2014 10:03:46 PM(UTC+0) Accessed: 7/14/2014 10:03:46 PM(UTC+0)		
	14	Name: com.apple.aggregated.plist Path: /Library/Preferences/com.apple.aggregated.plist MD5: 91a20145343d8872b4d4ce4a70053c6a SHA256: 19ccf13eaed4d725a127fbd4eae6f1c9 5bfc6f47d06dd49ad3fe708cf9dc4aff	Size (Bytes): 78 Created: 7/14/2014 7:13:13 PM(UTC+0) Modified: 7/14/2014 7:13:13 PM(UTC+0) Accessed: 7/14/2014 7:13:13 PM(UTC+0)		
	15	Name: com.apple.AppSupport.plist Path: /Library/Preferences/com.apple.AppSupport.plist MD5: 2444b5d902ad0e78d0c34edad8ee1237 SHA256: d15a6c98d9dd1d6b3a3552b005a90c8a 57fb4ae32f8b7e51fa50c8e9356e4290	Size (Bytes): 98 Created: 7/14/2014 7:17:42 PM(UTC+0) Modified: 7/14/2014 7:17:42 PM(UTC+0) Accessed: 7/14/2014 7:17:42 PM(UTC+0)		
	16	Name: com.apple.apsd.plist Path: /Library/Preferences/com.apple.apsd.plist MD5: 218d6fef6891ae9b5224964520c30e1aa SHA256: 23edb2be51f32441fba37b170e3e62e0b 4793645a71ed37d141f97d39484d6f73	Size (Bytes): 152 Created: 7/14/2014 10:03:49 PM(UTC+0) Modified: 7/14/2014 10:03:49 PM(UTC+0) Accessed: 7/14/2014 10:03:49 PM(UTC+0)		
	17	Name: com.apple.awdd.persistent.plist Path: /Library/Preferences/com.apple.awdd.persistent.plist MD5: d130d96fbc5a49e22a74a01acb7df25b SHA256: 61114c7b4f401acdbca40a52ed846dbd 5c805b9a1e8a19fbdbe4614de4dd59e38	Size (Bytes): 177 Created: 7/14/2014 10:03:48 PM(UTC+0) Modified: 7/14/2014 10:03:48 PM(UTC+0) Accessed: 7/14/2014 10:03:48 PM(UTC+0)		
	18	Name: com.apple.awdd.persistent.plist.GelkAKj Path: /Library/Preferences/com.apple.awdd.persistent.plist.GelkAKj MD5: d991734a3dfe852ee1b05289e30674f	Size (Bytes): 177 Created: 7/14/2014 7:17:44 PM(UTC+0) Modified: 7/14/2014 7:17:44 PM(UTC+0) Accessed: 7/14/2014 7:17:44 PM(UTC+0)		

Figure 12-3 Plists found on an iPhone 3G
Source: Cellebrite Mobile Synchronization LTD

Mobile Forensics Tools in Action

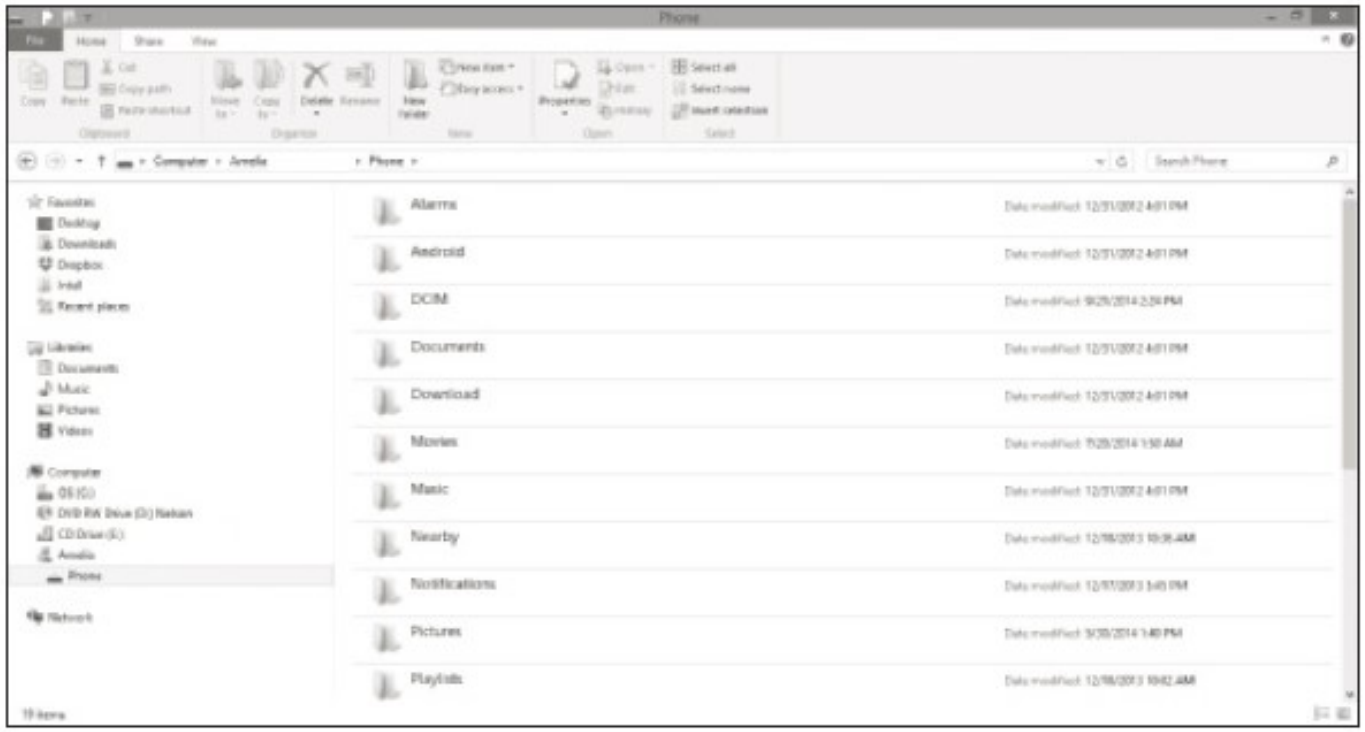


Figure 12-4 Viewing the Android file system
Courtesy of Microsoft Corporation

Mobile Forensics Tools in Action

- Many mobile forensics tools are available
  - Most aren't free
- Methods and techniques for acquiring evidence will change as market continues to expand and mature
- Subscribe to user groups and professional organizations to stay abreast of what's happening in the industry