Mobile Device Forensics

Smartphone and IoT Device Forensics

Database Forensics

Nelson, Chapter 12

Objectives

Explain the basic concepts of mobile device forensics

Describe procedures for acquiring data from mobile devices

Summarize the challenges of forensic acquisitions of data stored on Internet of Anything devices

Understanding Mobile Device Forensics (1 of 3)

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 (2 of 3)

Items stored on cell phones: (cont'd)

- *Calendars and address books*
- *Social media account information*
- *GPS data*
- *Voice recordings and voicemail*
- *Bank account logins*
- *Access to your home*

A search warrant is needed to examine mobile devices because they can contain so much information

Understanding Mobile Device Forensics (3 of 3)

Investigating cell phones and mobile devices is a 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 (1 of 7)

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)***

Fourth-generation (4G) was introduced in 2009

Several digital networks are used in the mobile phone industry

Fifth-generation (5G) cellular networks

- *Finalized in 2020*
- *Higher bandwidths, lower latencies*
- *Better interconnectivity*

Mobile Phone Basics (2 of 7)

Most **Code Division Multiple Access (CDMA)** networks conform to IS-95

These systems are referred to as CDMAOne

When they went to 3G services, they became CDMA2000

Global System for Mobile Communications (GSM) uses the **Time Division Multiple Access (TDMA)** technique

Multiple phones take turns sharing a channel

Mobile Phone Basics (3 of 7)

The 3G standard was developed by the **International Telecommunications Union (ITU)** under the United Nations

- *It is compatible with CDMA, GSM, and TDMA*
- *The **Enhanced Data GSM Environment (EDGE)** standard was developed specifically for 3G*

Mobile Phone Basics (4 of 7)

4G networks can use the following technologies:

Orthogonal Frequency Division Multiplexing (OFDM)

Mobile WiMAX

Ultra Mobile Broadband (UMB)

Multiple Input Multiple Output (MIMO)

Long Term Evolution (LTE)

Mobile Phone Basics (5 of 7)

5G networks can use the following technologies:

Orthogonal Frequency Division Multiplexing (OFDM)

5G NR air interface

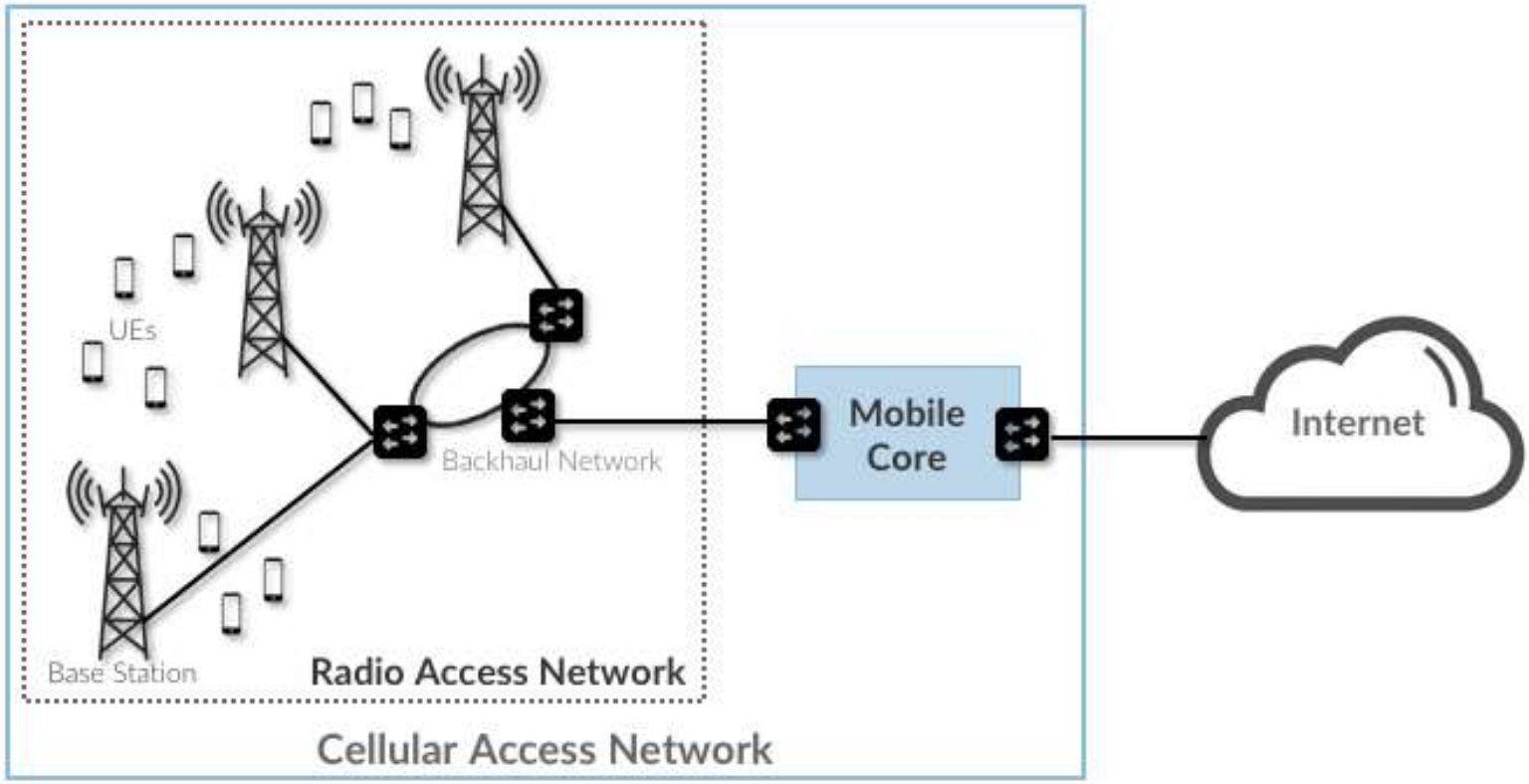
Wider bandwidth technoloigies such as

sub-6 GHz

mmWave

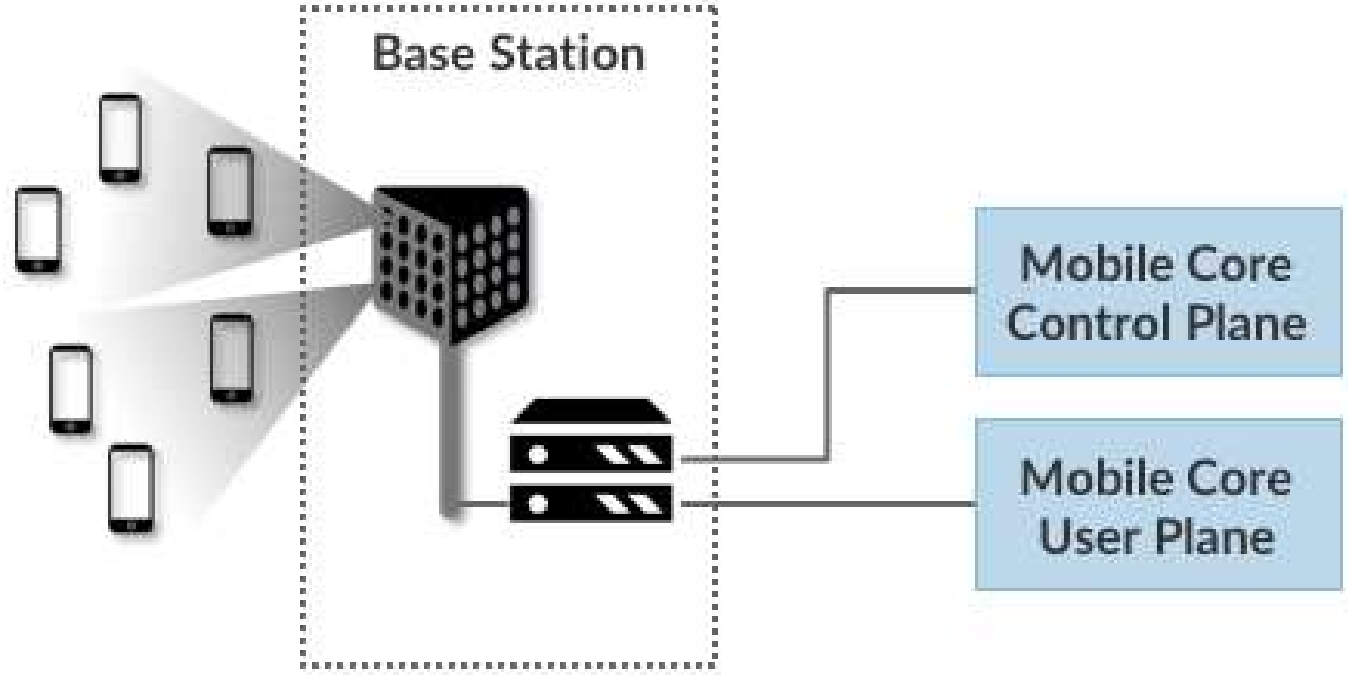
Mobile Phone Basics (6 of 7)

Overview of 5G Network:



Mobile Phone Basics (7 of 7)

Coceptual view of mobile core:



Inside Mobile Devices (1 of 5)

Mobile devices can range from simple phones to **smartphones**, tablets, and smartwatches

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 smartphones use the same OSs as PCs

Inside Mobile Devices (2 of 5)

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 (3 of 5)

Personal digital assistants (PDAs) have been essentially replaced by smartphones, tablets 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)

MultiMediaCard (MMC)

Secure Digital (SD)

Inside Mobile Devices (4 of 5)

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 three sizes

Portability of information makes SIM cards versatile

Inside Mobile Devices (5 of 5)

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

eSIM is becoming available

- Software installed on small eUICC chip embedded in mobile device.
- Can't be removed

Phones used to include SD cards for external storage. Trends:

Use of SIMs for external storage no longer supported

Data is migrating from SIM to apps

Understanding Acquisition Procedures for Mobile Devices (1 of 7)

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 data is critical

Mobile device attached to a PC/Mac (wirelessly or via cable) should be disconnected from the PC immediately

Helps prevent synchronization that might occur automatically and overwrite data

Understanding Acquisition Procedures for Mobile Devices (2 of 7)

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 a Faraday bag*
- *Turn the device off*

Understanding Acquisition Procedures for Mobile Devices (3 of 7)

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 Mobile Devices (4 of 7)

Check these areas in the forensics lab :

- *Internal memory*
- *SIM card*
- *Removable or external memory cards*
- *Network provider*
- *Cloud provider*

Checking network and/or cloud provider requires a search warrant or subpoena

- *If not covered by original warrant/subpoena, then additional one is needed*

Understanding Acquisition Procedures for Mobile Devices (5 of 7)

Due to the growing problem of mobile devices being stolen, service providers have provided a remote wiping capability to remove a user's personal information stored on a stolen device (aka *Remote Wipe)*

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

Android: typically EXT4 [same as Linux]

iPhone: APFS [same as Macs]

Understanding Acquisition Procedures for Mobile Devices (6 of 7)

- MF: root
- DF: directory files
- EF: elementary data

- In this figure, Efs under the GSM and DCS1800 DFs contain network data on different frequency bands of operation.
- The Efs under the Telecom DF contain service-related data

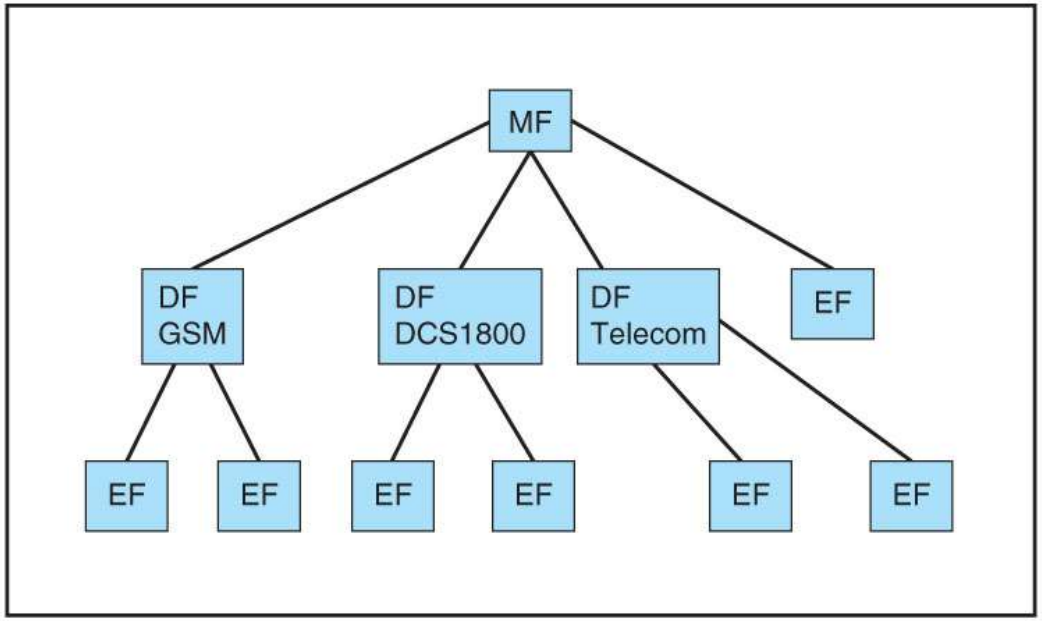


Figure 12-1 SIM file structure

Understanding Acquisition Procedures for Mobile Devices (7 of 7)

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 (1 of 6)

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 (2 of 6)

SIM card readers (non eSIM cards)

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 device's back panel
- Remove the battery
- Remove the SIM card from holder
- Insert the SIM card into the card reader

Mobile Forensics Equipment (3 of 6)

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

eSIM reading is more problematic

Mobile phone forensics tools and methods

AccessData FTK Imager

MacLockPick 3.0

Mobile Forensics Equipment (4 of 6)

NIST guidelines list six types of mobile forensics methods:

- *Manual extraction*
- *Logical extraction*
- *Physical extraction*
- *Hex dumping and Joint Test Action Group (JTAG) extraction*
- *Chip-off*
- *Micro read*

Mobile Forensics Equipment (5 of 6)

Paraben Software offers several tools:

E3:DS – for mobile device investigations

DataPilot – has a collection of cables that can interface with phones from different manufacturers

BitPam - used to view data on many CDMA phones

Cellebrite UFED Forensic System - works with smartphones, PDAs, tablets, and GPS devices

MOBILedit Forensic - contains a built-in write-blocker

Mobile Forensics Equipment (6 of 6)

Software tools differ in the information they display and the level of detail

Some tools are designed for updating files, not retrieving data

In general, tools designed to edit information, although they are user friendly, usually aren't forensically sound

Using Mobile Forensics Tools (1 of 4)

Cellebrite is often used by law enforcement

You can determine the device's make and model, learn what has to be done before connecting a mobile device to the UFED device, and then retrieve the data

Three options for data extraction:

Logical

File system

Physical

You can also simply connect a mobile device to a computer to browse the file system and examine and retrieve files

USB write-blocker may be needed

Using Mobile Forensics Tools (2 of 4)

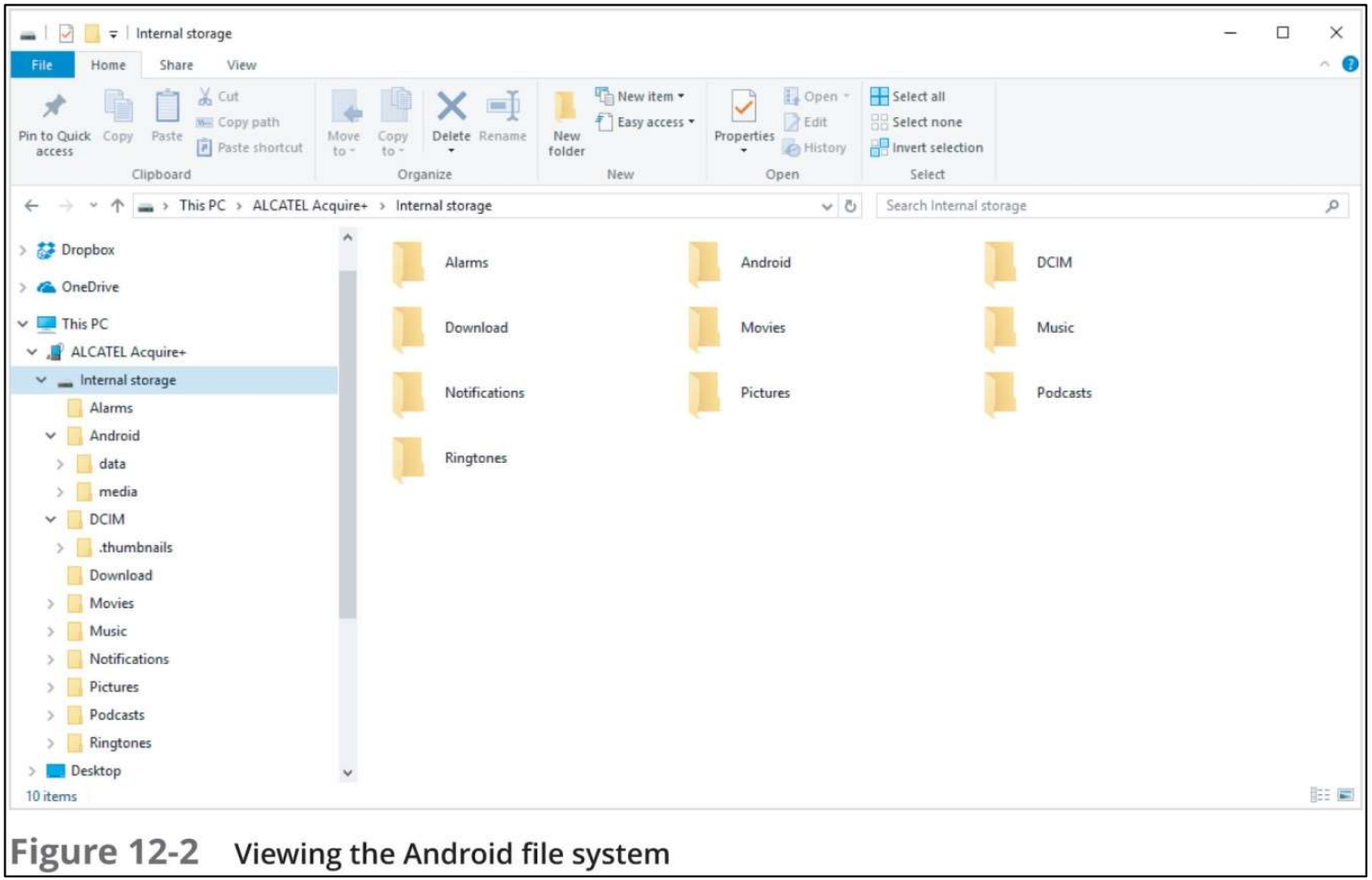


Figure 12-2 Viewing the Android file system

Using Mobile Forensics Tools (3 of 4)

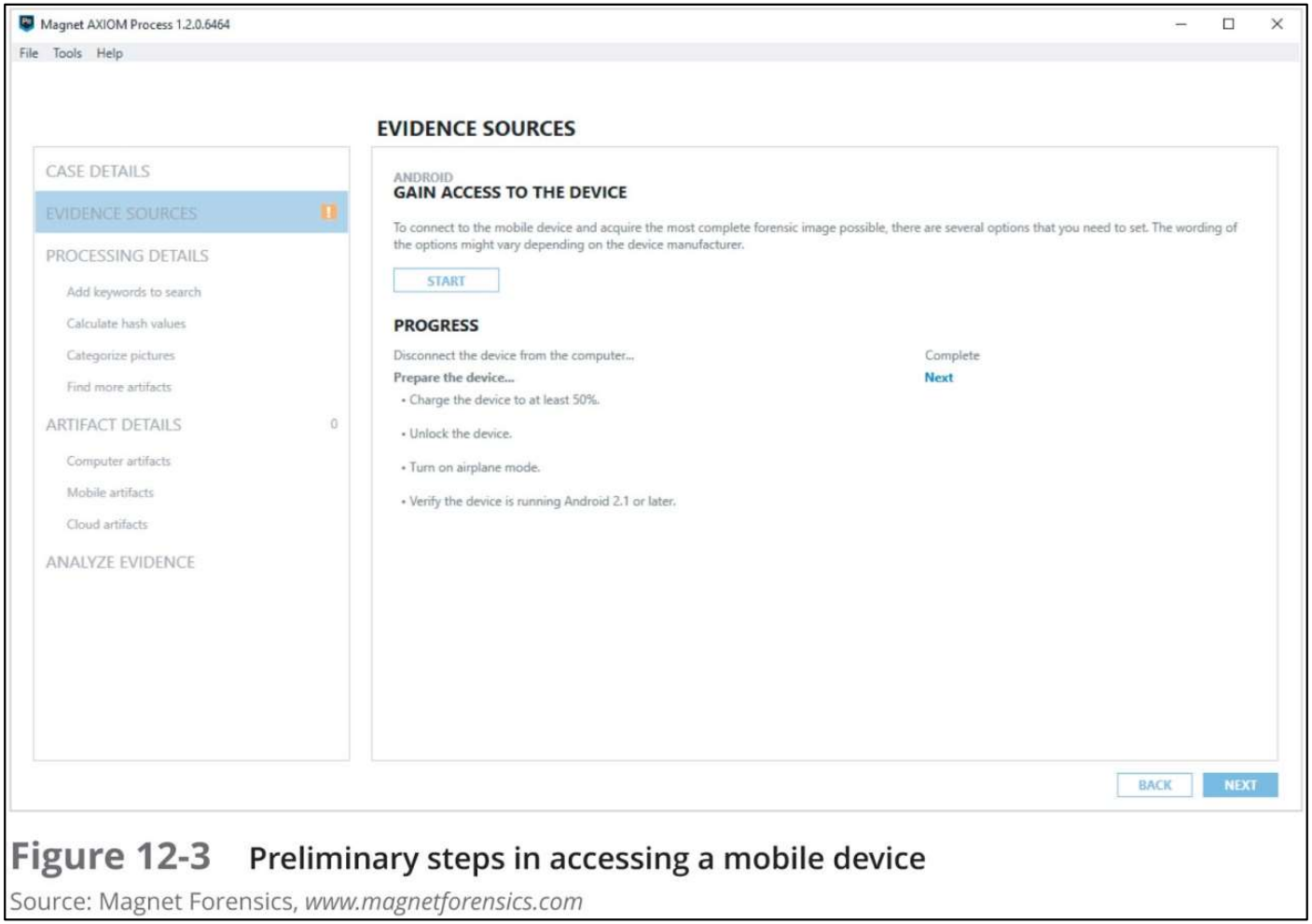


Figure 12-3 Preliminary steps in accessing a mobile device

Source: Magnet Forensics, *www.magnetforensics.com*

Using Mobile Forensics Tools (4 of 4)

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

Understanding Forensics in the Internet of Anything (1 of 3)

In 2010, VMware and BlackBerry were developing

Type 2 hypervisors for mobile devices

Useful for security and protecting personal information but will add another level of complexity to forensics investigations

Separate personal information from business-related data

Bring your own device (BYOD) practices make it even more difficult

Internet of Things (IoT)

The number of devices that connect to the Internet is higher than the amount of people

That number is expected to reach 50 billion in the next few decades

Understanding Forensics in the Internet of Anything (2 of 3)

Evolution from Internet of Thing (IoT) to Internet of Everything (IoE) to Internet of Anything (IoA)

IoE adds features that aren't tangible but are widespread on the Internet

Google search engine and YouTube

IoA includes cars, homes, pets, livestock, and applications for making all these things work together

Eventually will include 5G smart devices

5G devices categories:

enhanced Mobile Broadband (eMBB)

Ultra-reliable and Low-latency Communications (uRLLC)

massive Machine Type Communications (mMTC)

Understanding Forensics in the Internet of Anything (3 of 3)

5G devices introduce new challenges for digital forensics:

People-to-device communications (P2D)

Device-to-device (D2D) communications

Device-to-cloud (D2C) communications

Wearable computers will pose many new challenges for investigators

Vehicle system forensics

Addresses the many parts that have sensors in cars

Most IoT devices run a version of Linux

Summary (1 of 3)

People store a wealth of information on smartphones, including calls, text messages, picture and music files, address books, and more

Mobile devices have gone through four generations: analog, digital personal communications service (PCS), third-generation (3G), and fourth-generation (4G)

5G standards are being negotiated and developed by the IMT 2020 working group of the International Telecommunications Union

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

Summary (2 of 3)

Data can be retrieved from several different places in phones

Use of personal digital assistants (PDAs) has declined due to the popularity of smartphones

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

To isolate a mobile device from incoming messages, you can put it in airplane mode, turn the device off, or place it in a special treated paint can or evidence bag

SIM cards store data in a hierarchical file structure

Mobile device forensics is becoming more important as these devices grow in popularity

Summary (3 of 3)

Many software tools are available for reading data stored in mobile devices

The Internet of Things (IoT) has resulted in yet another challenge for digital forensics investigators

Collecting information from wearable computers will pose many new challenges for investigators

Database Forensics

Focus: Android

(Largely applicable to iOS as well)

Android Data Recovery
Data from Apps

Until this point, we have been recovering deleted files

The process is very analogous to computer forensics

But, in Android systems

- *Almost all of the user activity is done through apps*
- *Most of the apps use SQLite databases to store information*
- *It follows, therefore, that we need to examine the SQLite databases created by the Android apps*

Android Data Recovery
SQLite Databases

Can data be recovered from SQLite databases?

The answer is yes

Deleted records are not deleted, but put into a freeblock list

Records might eventually get overwritten, but no guarantee unless a "vacuum" command is issued

- Rebuilds database
- Reclaims deleted records and space

Android Data Recovery
SQLite Deleted Data Recovery

To understand how SQLite deleted records can be discovered, we need to understand the basic structure of the SQLite database

We will review this at a high level

Android Data Recovery
SQLite Database Structure

SQLite database structure:

SQLite databases are made up of pages

The size is fixed at powers of 2 ranging from 2^{10} to 2^{16}

The first page is called the root page

Different types of pages

Lock-byte

Freelist

B-Tree

Payload overflow

Pointer map

Android Data Recovery
SQLite Database Page Types

Lock-byte Page

Used by OS Interface (VFS) in implementing database locking

Not relevant to file recovery

Freelist Page

Unused pages

Created when information is deleted from database

Reused when additional pages are required

Android Data Recovery
SQLite Database Page Types

B-Tree Page

Used to store key and data storage for active database pages

Organized as a B-Tree

Self-balancing tree data structure

Enables efficient access, insertion and deletion

Types of B-Tree pages

Table Interior	(describes table schema)
Table leaf	(contains table data/payload)
Index Interior	(schema for indices)
Index leaf	(indices)

Android Data Recovery
SQLite Database Page Types

Payload Overflow Page

When payload is too large for a B-Tree page

Data overflows onto pages of this type

Pointer Map Pages

Makes operation of **vacuum** *operation more efficient.*

Android Data Recovery
SQLite Logical Structure

B-Tree Page Hierarchy

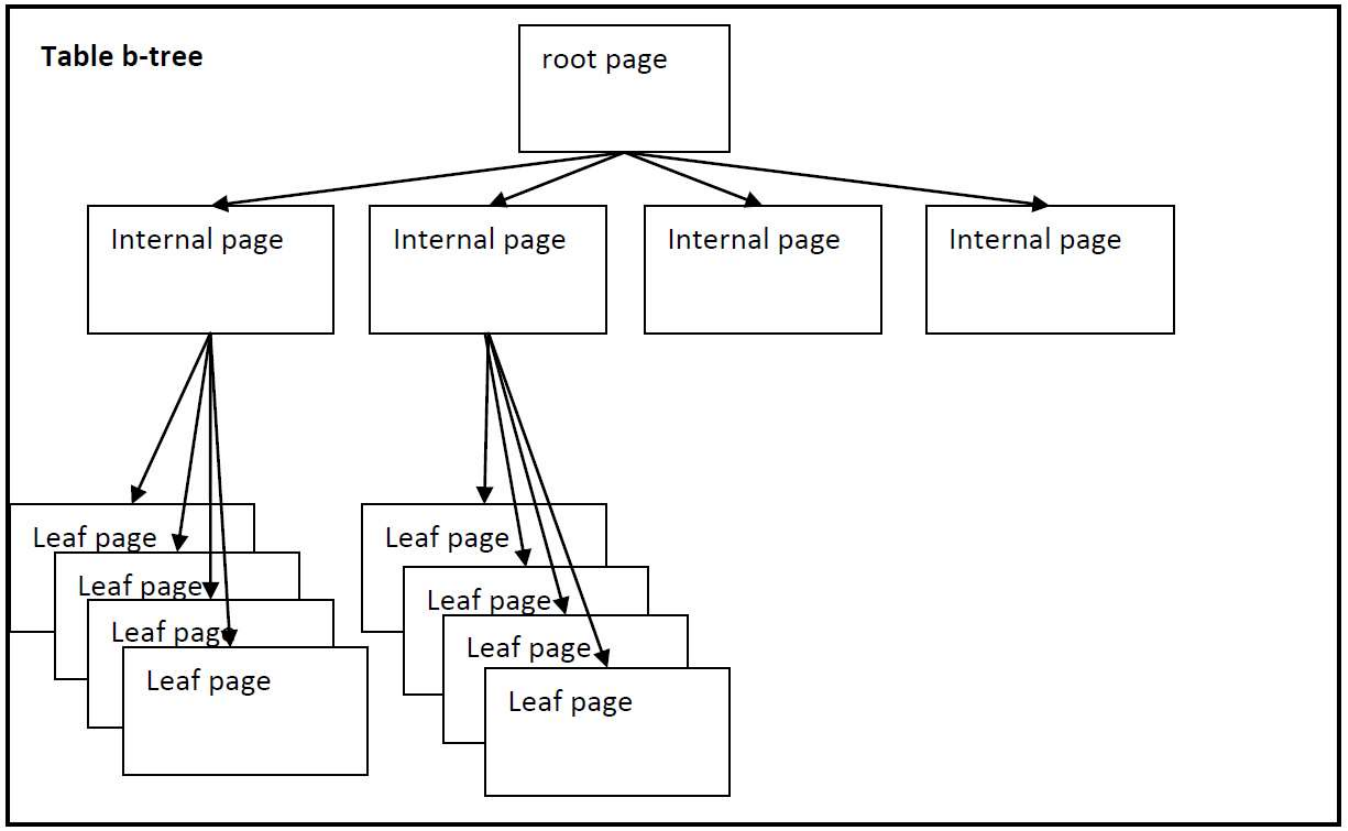


Figure 1. B-tree page hierarchy

Android Data Recovery
SQLite Database Header

- The first 100 bytes of the database file contains the database header
- In root page
- Note the “SQLite format 3” magic string
- Database page size
- Note that it contains pointer to freelist pages

Database Header Format

Offset	Size	Description
0	16	The header string: "SQLite format 3\000"
16	2	The database page size in bytes. Must be a power of two between 512 and 32768 inclusive, or the value 1 representing a page size of 65536.
18	1	File format write version. 1 for legacy; 2 for WAL.
19	1	File format read version. 1 for legacy; 2 for WAL.
20	1	Bytes of unused "reserved" space at the end of each page. Usually 0.
21	1	Maximum embedded payload fraction. Must be 64.
22	1	Minimum embedded payload fraction. Must be 32.
23	1	Leaf payload fraction. Must be 32.
24	4	File change counter.
28	4	Size of the database file in pages. The "in-header database size".
32	4	Page number of the first freelist trunk page.
36	4	Total number of freelist pages.
40	4	The schema cookie.
44	4	The schema format number. Supported schema formats are 1, 2, 3, and 4.
48	4	Default page cache size.
52	4	The page number of the largest root b-tree page when in auto-vacuum or incremental-vacuum modes, or zero otherwise.
56	4	The database text encoding. A value of 1 means UTF-8. A value of 2 means UTF-16le. A value of 3 means UTF-16be.
60	4	The "user version" as read and set by the user_version pragma.
64	4	True (non-zero) for incremental-vacuum mode. False (zero) otherwise.
68	4	The "Application ID" set by PRAGMA application_id.
72	20	Reserved for expansion. Must be zero.
92	4	The version-valid-for number.
96	4	SQLITE_VERSION_NUMBER

Android Data Recovery
SQLite Logical Structure

B-Tree Page Layout

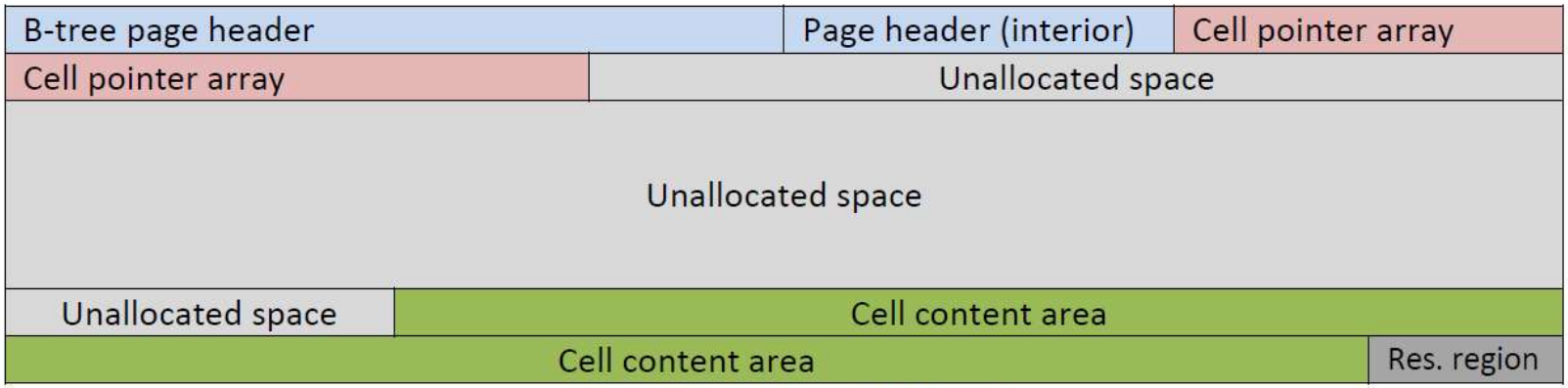


Figure 2. Sqlite b-tree page layout

B-Tree Page Header	
Byte 0	B-tree type (e.g., 0xD is leaf table)
Bytes 1-2	Byte offset into free freeblock
Bytes 3-4	Number of cells on page
Bytes 5-6	Offset into first byte of cell content area
Byte 7	Number of fragmented free bytes in cell area content
Bytes 8-11	Right most pointer (interior pages only)

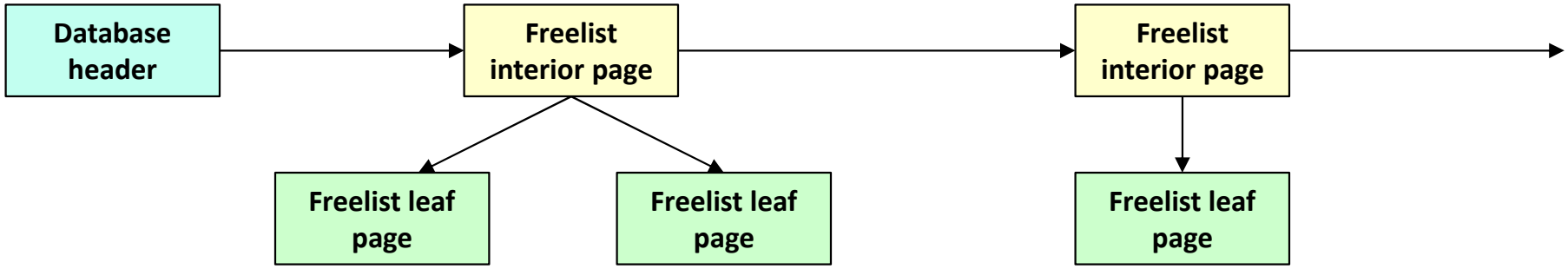
Points to first block of freeblock list in Cell Content area

Android Data Recovery
SQLite Free List

When information is deleted from the database that frees up an entire page, it is stored on a freelist

Stored as a linked list of freelist pages

Beginning of list is at database header



Android Data Recovery
SQLite Record Recovery

So, where is the deleted data?

Freelist page list

Granularity: database page

To find list: Start from Database header

Freeblock list

Granularity: < database page; minimum 4 bytes

To find list: Start from B-tree page header

Unallocated space

Granularity: < database page;

To find list: deduce from B-tree page header information

Android Data Recovery
SQLite Deleted Data Methodology

The basic methodology for recovering data in SQLite databases involves:

Find SQLite database ("SQLite Format 3" magic string)

- Locate beginning of Freelist
- Traverse freelist records, looking for valid records

File carving to find leaf nodes (0xD signals start of header)

- Use B-tree page headers to find freeblock list
- Find unallocated area
- More file carving based on tags, heuristics,etc. to rebuild records