Android Forensics

(Part 3)

Contents

- Android File Systems
- Android File Systems: Partitions
- Android File Hierarchy
- Ways to store data
- Summary

Android File Systems

- There is no singularly defined file system for Android.
- Android is developed on Linux kernel and Linux supports many file systems
- Common Android File Systems that are supported by Android Phones can be classified into three (3) main categories
  - Flash Memory File Systems
  - Media-Based File Systems
  - Pseudo File Systems

Android File Systems (Cont'd)

Flash Memory File Systems

- Is a type of non-volatile memory that erases data in units called blocks and rewrites data at the byte level
- Extended File Allocation Table (exFAT)
- Flash Friendly File System (F2FS)
- Journal Flash File System version 2 (JFFS2)
- Yet Another Flash File System version 2 (YAFFS2)
- Robust File System (RFS)

Android File Systems (Cont'd)

Media-Based File Systems

- EXTended file system (EXT2/EXT3/EXT4)
- File Allocation Table (FAT, FAT12, FAT16 & FAT32)
- Virtual File Allocation Table (VFAT)

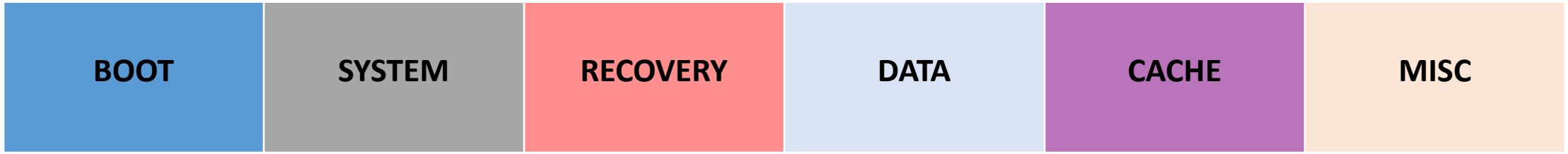
Pseudo File Systems

- virtual entries that the file system itself makes up on processes or functions
- For example, /proc on many operating ssytems is a process information file system which dynamically generates directories for every process
- control group (cgroup)
- rootfs, procfs
- Ysfs
- tmpfs

Android File Systems: Partitions

- Android uses more than one file system and multiple partitions to organize files and folders in the device
- In the file system partitions are represented by directories
- There may be other partitions which differ in each model such as sdcard, sd-ext

Partitions



Android File Systems: Partitions (Cont'd)

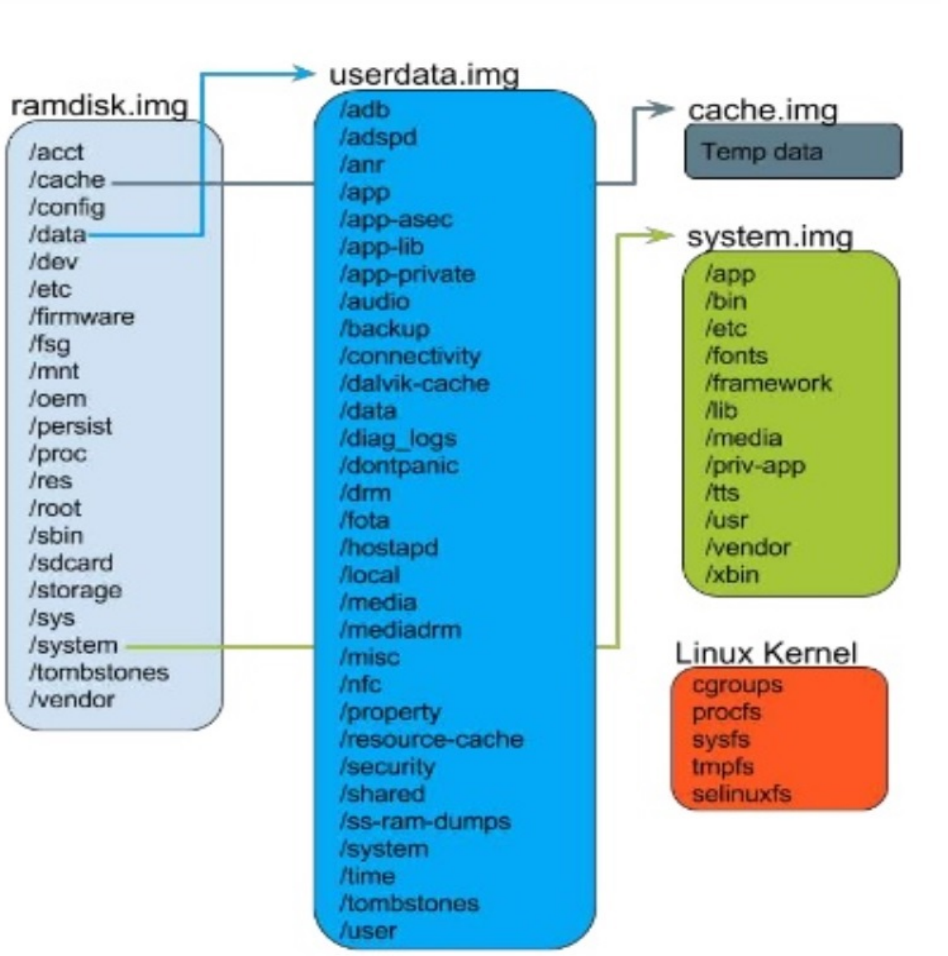
Partition	Explanation
Boot Loader	• Responsible for booting the Android kernel and booting into other boot modes, such as the recovery mode, download mode, and so on
/boot	• This partition has the information and files required for the phone to boot • It contains the kernel and RAM disk
/system	• The Android system image here contains the Android framework, libraries, system binaries, and preinstalled applications • Without this partition, the device cannot boot into normal mode
/Recovery	• Recovery partition allows the device to boot into the recovery console through which activities such as phone updates and other maintenance operations are performed
/data or userdata	• The device's internal storage for application data • It contain all the user data like sms, contacts, settings and all data related to installed applications
/cache	• This partition is used to store frequently accessed data such as recovery logs and update packages downloaded over the cellular network
/misc	• This partition contains other important system setting information, such as a USB configuration, carrier ID, and other hardware settings

Android File Systems: Partitions (Cont'd)

Partition	Explanation
/sdcard	• This partition is for the SD card, not for the internal memory. It is used to store any type of data such as media, documents, ROM etc. • The SD card can be internal or external SD card depending on the device
/sd-ext	• This partition is commonly used by custom ROMs and not a standard Android partition. • It is an additional partition on SD card that act as data partition in some custom ROMs that have the features like app2sd to get additional storage for installing their apps.

Android file hierarchy

- A basic understanding of how Android organizes its data in files and folders helps a forensic analyst narrow down his research to specific locations
- If you are familiar with Unix-like systems, you will understand the file hierarchy in Android very well
- Based on the device manufacturer and the underlying Linux version, the structure of this hierarchy may have a few insignificant changes



Android file hierarchy (Cont'd)

Directories Overviews

- **Acct**
  - This is the mount point for the acct cgroup (control group) that provides for user accounting
- **Cache**
  - This is the directory (/cache) where Android stores frequently accessed data and app components
  - Wiping the cache doesn't affect your personal data, but simply deletes the existing data there
  - There is also another directory in this folder called lost+found. This directory holds recovered files (if any) in the event of filesystem corruption, such as incorrectly removing the SD card without unmounting it and so on
  - The cache may contain forensically relevant artifacts, such as images, browsing history, and other app data

Android file hierarchy (Cont'd)

Directories Overviews

- **d**
  - This is a symbolic link to /sys/kernel/debug
  - This folder is used to mount the debugfs file system and to debug kernel
- **Data**
  - This is the partition that contains the data of each application
  - Most of the data belonging to a user, such as the contacts, SMS, dialed numbers, and so on, is stored in this folder
  - This folder has significant importance from a forensic point of view as it holds valuable data

Android file hierarchy (Cont'd)

Important sub-directories under /data or userdata

Partitions	Descriptions
/dalvik-cache	This folder contains several logs that might be useful during the examination, depending on the underlying requirements
/data/data	The /data/data partition contains the private data of all the applications
/dev	This directory contains special device files for all the devices Defines the devices available to the applications
/init	When booting the Android kernel, the init program is executed
/mnt	This directory serves as a mount point for all the file systems, internal and external SD cards
/proc	It contains files that have useful information about the processes
/root	This is the home directory for the root account This folder can be accessed only if the device is rooted

Android file hierarchy (Cont'd)

Important sub-directories under data/userdata folder

Partitions	Descriptions
/misc	miscellaneous settings. Information about hardware settings, USB settings, and so on can be accessed from this folder
/sdcard	This is the partition that contains the data present on the SD card of the device There are some default folders, such as android_secure, Android, DCIM, media, and so on, present in most of the mobiles
Digital Camera Images (DCIM)	Within DCIM, you will find photos you have taken, videos, and thumbnails (cache) files. Photos are stored in /DCIM/Camera
/system	Directory contains libraries, system binaries, and other system-related files The pre-installed applications that come along with the phone are also present in this partition

Ways to store data

- Android devices store a lot of sensitive data through the use of apps
- Various sources of Data on Android
  - Apps that come along with Android
  - Apps installed by the manufacturer
  - Apps installed by a wireless carrier
  - Apps installed by the user
- Ways to store data locally in an Android app
  - Shared preferences
  - Internal storage
  - External storage
  - SQLite database
  - Network

Ways to store data (Cont'd)

Shared preferences

- Store data in key values pairs of data types in the .xml format
- Save user preferences data of the current application (e.g user account name and passwords, settings)
- These files are typically stored in the application's ***/data/data/<package_name>/shared_prefs***

Internal Storage

- These files are located typically in the application's /data/data subdirectory
- Data stored here is private and cannot be accessed by other applications (unless they have root access)
- Internal data for each of the app is stored in respective folders
- Usually, **shared pref**, **lib**, **Cache**, **database** folders are created for most of the applications

Folder description

- **shared_prefs** - XML file of shared preferences contains data in a key-value pair
- **lib** - Custom library files required by app
- **files** - Developer-saved files
- **cache** - Files cached by app
- **databases** - SQLite and journal files

Ways to store data (Cont'd)

External storage

- Files can also be stored by the apps in external storage.
- External storage can be a removable media, such as an SD card or non-removable storage that comes with the phone
- SD cards are usually formatted with the FAT32 filesystem, however it can be stored as other filesystems, such as EXT3 and EXT4, are also being used increasingly.
- Data stored in SD Card are public and can be accessed by other applications, provided the requesting apps have the necessary permissions

SQLite database

- SQLite is a popular database format present in many mobile systems
- The SQLite files used by the apps are generally stored at ***/data/data/<ApplicationPackageName>/databases***

Network

- You can use the network to store and retrieve data on your own web-based services
- To do network operations, the classes in the java.net.* and android.net.* packages can be used

Summary

- With this knowledge of Android internals, we are able to understand the followings:
  - What data is stored on the Android device
  - Where are the data stored on Android device
  - How it is stored on the Android Device
- Android devices store a lot of sensitive data through the use of apps
- A basic understanding of how Android organizes its data, in files and folders helps a forensic analyst narrow down his research to specific locations during analysis