NFSU

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

विद्यया अमृतं अश्नुते

An Institute of National Importance
(Ministry of Home Affairs, Government of India)

Mobile Phone Security and Forensics

Dr. Digvijaysinh Rathod

Associate Professor & Associate Dean

School of Cyber Security and Digital Forensics

National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in

Android partition layout
and
Android file hierarchy

Android partition layout

- ✓ The partition layout varies between vendors and versions.
- ✓ However, a few partitions are present in all the Android devices.

- ✓ Boot Loader :
  - ✓ This partition stores the **phone's boot loader program**.
  - ✓ This program takes care of initializing the **lowlevel hardware when the phone boots**.
  - ✓ Thus, it is responsible for booting the Android kernel and booting into **other boot modes**, such as the recovery mode, download mode, and so on.

- ✓ Boot
  - ✓ As the name suggests, this partition has the information and files required for the **phone to boot**.
  - ✓ It contains the **kernel and RAM disk**. So, without this partition, the phone cannot start its processes.

- ✓ 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.**
  - ✓ For this purpose, a minimal Android boot image is stored.

- ✓ Userdata
  - ✓ This partition is usually called the **data partition** and is the **device's internal storage for application** data.
  - ✓ A bulk of user data is stored here, and this is where most of **our forensic evidence will reside**.
  - ✓ It stores all app data and standard communications as well.

Android partition layout

- System
  - All the major components other than **kernel and RAM disk** are present here.
  - 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.

- ✓ Cache
  - ✓ This partition is used to store **frequently accessed data** and various other files, such as recovery logs
  - ✓ and update packages downloaded over the cellular network.

- ✓ Radio
  - ✓ Devices with **telephony capabilities have a baseband image stored in** this partition that takes care of various telephony activities.

Identifying partition layout

- ✓ adb shell
- ✓ root@android: cat proc/partition
- ✓ root@android: cat /proc/mounts

or

- ✓ root@android: cat /proc/mounts
- ✓ cat /proc/mtd

Filesystem path alias

- ✓ Using df lists the filesystem path alias and size info as seen below (total size, used, free and block size)
- ✓ root@android: df

mapping between the partition alias and the path of actual partition file

- ✓ You get the mapping between the partition alias and the path of actual partition file (you also get the owner, their user group, etc)
- ✓ root@android:

  ls -al /dev/block/platform/msm_sdcc.1/by-name

Or

- ✓ root@android: cat /proc/emmc
- ✓ cat /proc/dumchar_info
- ✓ root@android: cat /dev/block/plateform/dw_mmc

https://android.stackexchange.com/questions/5232/how-can-i-view-the-android-internal-partition-table

mapping between the partition alias and the path of actual partition file

- ✓ root@android: ls -l $(find /dev/block -name by-name)
- ✓ this will cover all possible paths (which of course varies for other devices)
- ✓ busybox fdisk [the various fdisk options...]
- ✓ busybox fdisk -l /dev/block/sda
- ✓ busybox you can find it in the /proc
- ✓ BusyBox is a software suite that provides several Unix utilities in a single executable file.

Practical

NFSU

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

विद्यया अमृतं अश्नुते

An Institute of National Importance
(Ministry of Home Affairs, Government of India)

Mobile Phone Security and Forensics

Dr. Digvijaysinh Rathod

Associate Professor & Associate Dean

School of Cyber Security and Digital Forensics

National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in