Android Devices

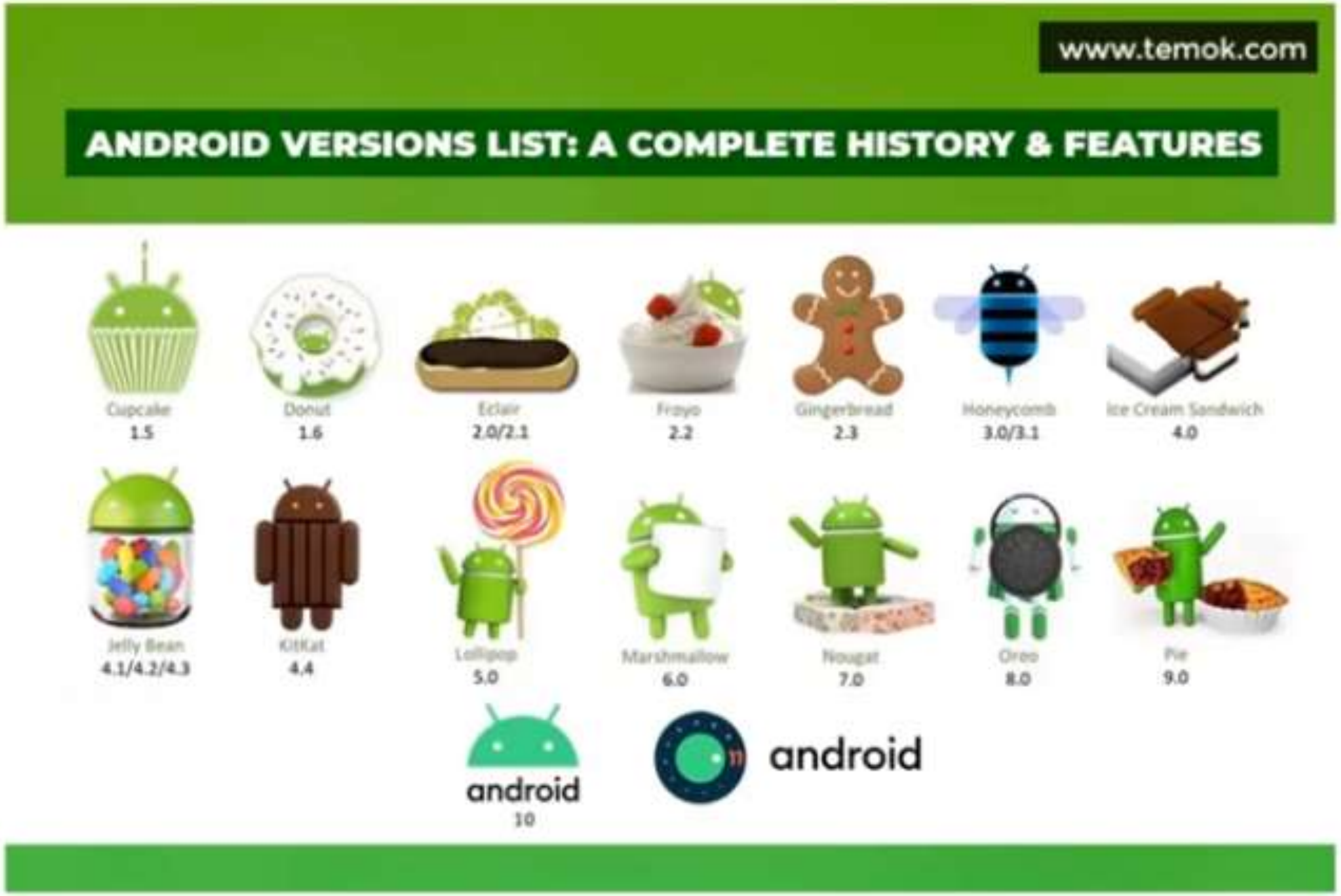
Table of Contents

1. All About Android
2. Android Forensic Environment & Tools
3. Data Acquisition
4. Data Analysis and Recovery
5. App Analysis

Android Versions

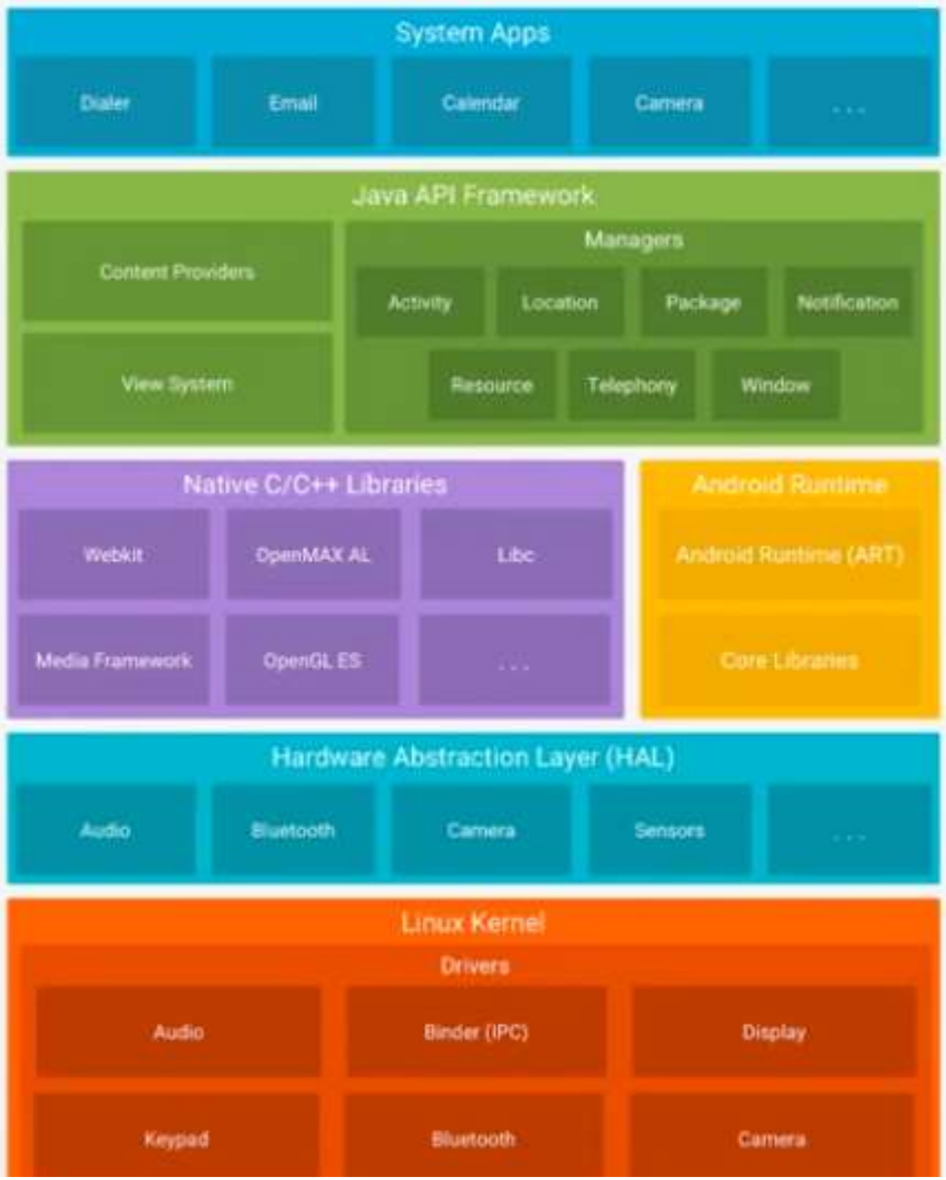
The earliest version (1.0) of Android was released in 2008 with the version name of Apple Pie, followed by 1.1 Banana Bread in 2009.

Each release is labeled with a letter in alphabetical order, making the Android 10.0 and 11 version names of Q and R, respectfully.



Android Architecture

These are the various layers involved in the Android software stack. Read about the layers here



System Apps

Dialer | Email | Calendar | Camera | ...

Java API Framework

Content Providers

View System

Managers

Activity | Location | Package | Notification

Resource | Telephony | Window

Native C/C++ Libraries

Webkit | OpenMAX AL | Libc

Media Framework | OpenGL ES | ...

Android Runtime

Android Runtime (ART)

Core Libraries

Hardware Abstraction Layer (HAL)

Audio | Bluetooth | Camera | Sensors | ...

Linux Kernel

Drivers

Audio | Binder (IPC) | Display

Keypad | Bluetooth | Camera

Android Security

The current kernel releases are 4.9, 4.41, and 4.19

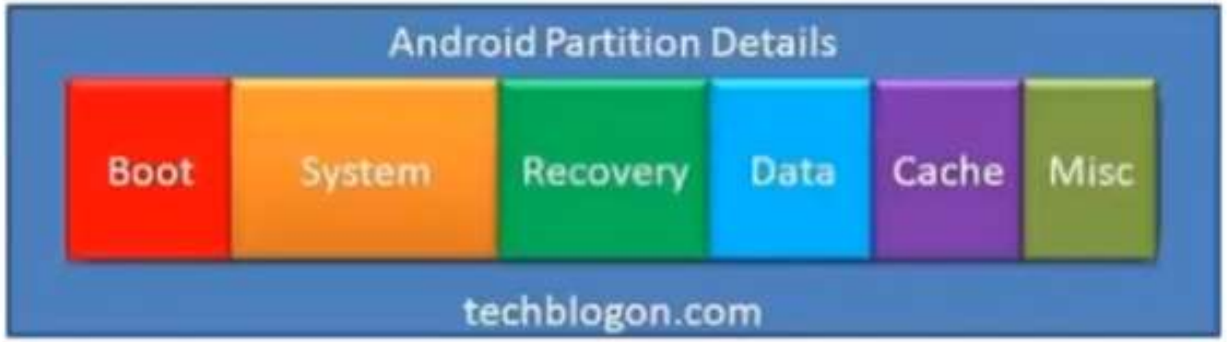
Inherited security features:

- User-based permissions model
- Isolation of running processes
- Secure inter-process communication (IPC)

Android File Hierarchy

Important folders that are common to most Android devices:

- /boot
- /system
- */recovery
- /data
- */cache
- */misc



Android File Systems

Flash Memory:

- exFAT
- F2FS
- YAFFS2
- RFS

Media-Based:

- EXT
- VFAT

Pseudo:

- rootfs
- sysfs
- devpts
- cgroup
- proc
- tmpfs

Android Forensic Environment and Tools

Android Forensic Environment

1. Forensically sterile computer environment
2. Install the necessary software/forensic tools
3. Obtain access to the device
4. Conduct data extractions

Android Tools - SDK

Android Software Development Kit

The Android SDK can help you extract data from the device by utilizing software libraries, APIs, tools, emulators and other material.

Using the Android Studio, you can create an Android Virtual Device (AVD) that can help you understand how applications behave and execute on devices.

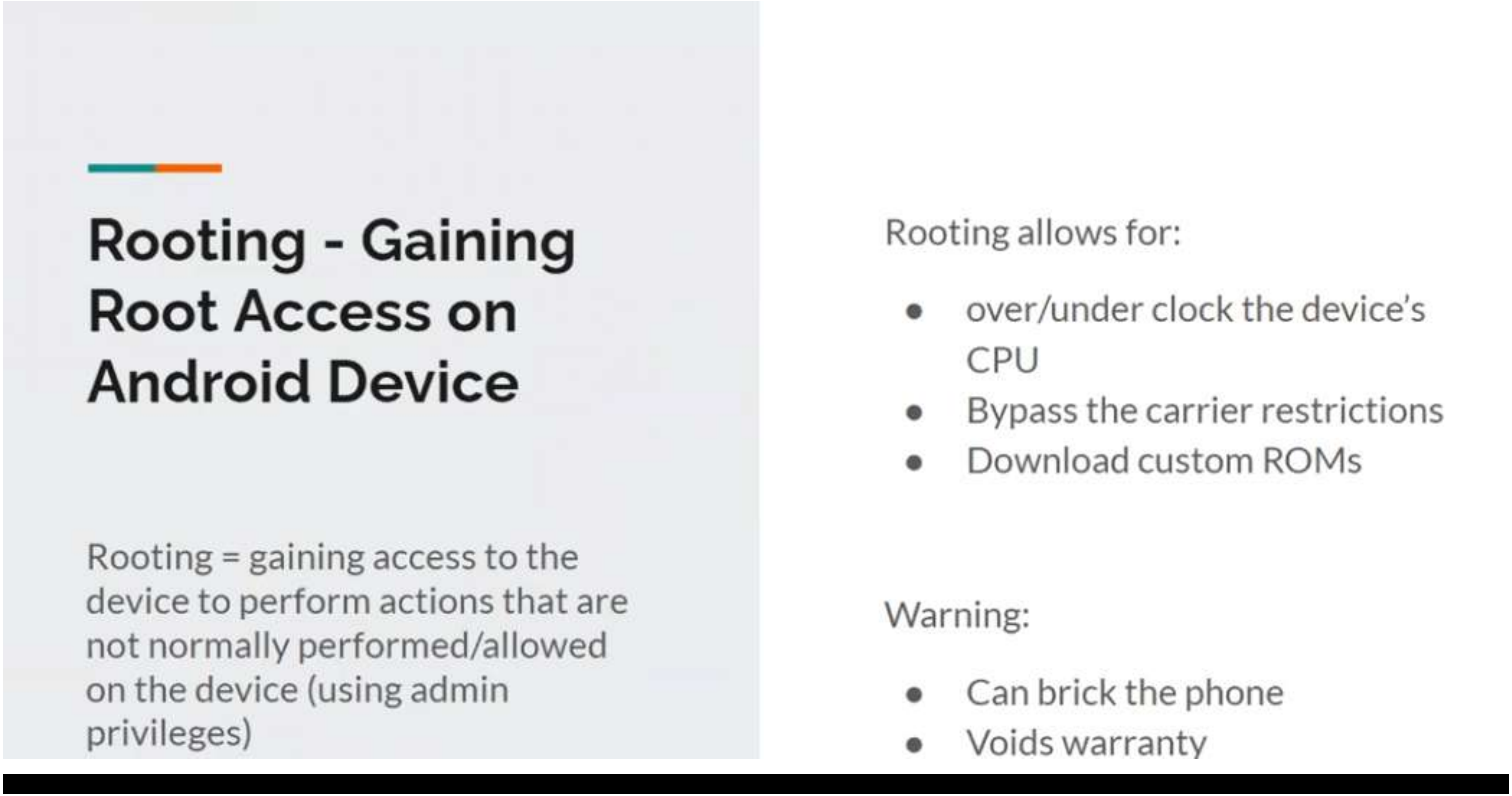
The Android Debug Bridge (ADB) allows you to communicate with the device and control it, and even bypass the screen lock.

Proper Handling of Android Device

- Place device in Airplane mode
- Disable Wi-Fi
- Remove the SIM card
- Enable USB debugging
- Enabling Stay awake setting
- Increase screen timeout

Bypassing Screen Lock Methods

- Using ADB & keys
- Using Automated Tools (Cellebrite)
- Using Android Device Manager
- Using Find My mobile (Samsung only)
- Using Smudge Attack
- Using Forgot Password/Pattern
- Booting into safe mode (3rd party lock)



Rooting - Gaining Root Access on Android Device

Rooting = gaining access to the device to perform actions that are not normally performed/allowed on the device (using admin privileges)

Rooting allows for:

- over/under clock the device's CPU
- Bypass the carrier restrictions
- Download custom ROMs

Warning:

- Can brick the phone
- Voids warranty

Data Acquisition

3 Types of Data Extraction Techniques

Manual Data Extraction:

- Manually handling the device to access and view details and information
- Pictures can be taken and presented as evidence

Logical Data Extraction:

- Extraction of data by interacting with the OS and accessing the filesystem.
- Root access can result in additional data

Physical Data Extraction:

- Bit-by-Bit image of the device is taken

Data Analysis and Recovery

Recovery Techniques

- Deleted data from an external SD card:
  - Mount the card as an external mass storage device and acquire the data using any tool previously discussed
- Deleted data from internal memory:
  - Image the device before and after rooting the device
- Parse SQLite files:
  - Check for unallocated and free blocks
- Use file-carving techniques:
  - Recovers from the unallocated space based on the file structure and content
- Use Google account for data recovery