What is Firmware?

Small mission-critical programs installed in the read-only memory, or ROM, of an electronic device. Modifying it is either impossible or required special equipment.

Many electronic devices, from modems to cell phones, contain chips with operating software written on them. Known as firmware, this software controls the device's basic operations.

What does it contain?

The iOS operating system contains all of the iPhone's pre-installed apps.

Android firmware (also referred to as **Android ROM**), however, is very different. It includes the entire Android operating system and it is stored in a writable form of memory called NAND flash memory. It also contains two additional closed source programs that are usually irreplaceable, a **bootloader** and **radio firmware**.

Understanding Android Bootloaders

An Android bootloader is a small piece of proprietary code that is responsible for starting the Android operating system However It also checks if the operating system it is starting is authentic (whether it is signed by OEM key). Because of the authenticity check, you cannot directly install a custom ROM but these days companies allow user to unlock the bootloader.

Usually, a tool called **fastboot**, which is a part of the Android SDK, is used to run the unlock commands

iPhone Firmware History

iOS 2 added support for third-party apps via the App Store.

In 2010, Apple released iOS 4, which featured multitasking and app folders.

2012's iOS 6 added a notification center, integrated Facebook into the system and replaced Google's Maps app with a new version designed by Apple.

Updating iPhone Firmware

All models of iPhone feature firmware that users can update via iTunes on the computer. IPhones already running iOS 5 or newer can also update directly without need of a computer.

Understanding Android Builds

The Android build is the only part of the firmware that is created from open-source code. When you hear Android, enthusiasts say "I flashed a new ROM on my device", you can be sure that they are talking about a new Android build.

An Android build is usually shared in the form of a ZIP file that can be used by **fastboot**.

```
update.zip
|-- android-info.txt
|-- boot.img
|-- recovery.img
|-- system.img
`-- userdata.img
```

android-info.txt is a text file specifying the prerequisites of the build. Here is a sample:

```
require board=herring
require version-bootloader=I9020XXJK1
require version-baseband=I9020XXKD1
```

boot.img is a binary file that contains both a Linux kernel and a ramdisk in the form of a GZIP archive. The kernel is a boot executable zImage that can be used by the bootloader.

userdata.img is a partition image that will be mounted on the empty **data** directory you can see in the ramdisk directory tree.

recovery.img is very similar to **boot.img**. It has a boot executable kernel file the bootloader can use and a ramdisk.

Survey resoruces

- **An Introduction to Android Firmware**
- **What Is iPhone Firmware?**