ANDROID ACQUISITION METHODS FROM ROOT TO RECOVERY

WHAT YOU NEED TO KNOW IN THE LAB AND ON THE STAND

MAGNET FORENSICS®

ANDROID ACQUISITION METHODS FROM ROOT TO RECOVERY

Physical, or "full," images—the bit-for-bit copies of a specified range, such as the user partition, of a mobile device's flash memory—have always been the gold standard of mobile forensics. Besides allowing you to find deleted data, physical imaging also:

- makes it possible to validate the source of evidence as it exists on the chip.
- helps to demonstrate your methodology and account for any changes that occurred.
- enables reverse engineering of new and/or unsupported apps and new operating systems, to determine where they store data, how this can change from version to version, and how it affects your forensic examinations.

However, as Apple, Google, and original equipment manufacturers (OEMs), such as Samsung, implement memory, file, and/or partition encryption in response to consumer demands for better security, physical images have become harder to acquire.

With a wide range of acquisition tools and methods to choose from, forensic examiners need a way to determine which works best for which device.

Digital forensics is nothing if not adaptable, though, and methods continue to adapt to this rapidly changing marketplace. With a wide range of acquisition tools and methods to choose from, forensic examiners need a way to determine which works best for which device. In some cases this will be a full/physical extraction; in others, though, the best option—assuming you have an unlocked device—will be a quick/logical acquisition. Either way, you should be prepared to document what you did, why you did it, and the steps you took.

LIVE EXPLOITS: ROOTING THE DEVICE

These methods exploit the device while it's booted, providing root access to its operating system; any physical acquisition via USB with Android running as a live system utilizes root access. Root access offers a full extraction, rather than a quick one, which requires only passcode and USB debugging enabled.

There are two types of root access:[1]

- "Shell root" returns the device to its original state following a reboot at the end of the process.
- "Permanent root" remains after reboot. It can be removed—the commercial tools that provide it allow this—but you have to remember to do so, not just to return the device to its original state, but also to prevent it from becoming vulnerable to malware.

Root access offers a full extraction, rather than a quick one, which requires only passcode and USB debugging enabled.

[1] Reiber, L. (2016). Mobile forensic investigations: a guide to evidence collection, analysis, and presentation. New York: McGraw-Hill Education.

THE PREVALENCE OF ANDROID (AND ESPECIALLY SAMSUNG) IN THE SMARTPHONE MARKET

In the fourth quarter of 2016, Gartner estimated that the Android operating system composed 82 percent of the worldwide market, with iOS making up the remaining 18 percent. Of all Android OEMs, Samsung made up the largest proportion at 57 percent. No other manufacturer, including Motorola, LG, Huawei, or HTC, breaks a double-digit percentage.[1] As of April 2015, 76 percent of Magnet Forensics customers' mobile device examinations involved iOS- or Android-powered smartphones or tablets. (Windows, BlackBerry, and basic feature phones made up the other 24 percent.)[2]

[1] Gartner, "Gartner Says Worldwide Sales of Smartphones Grew 7 Percent in the Fourth Quarter of 2016," February 15, 2017, https://www.gartner.com/newsroom/id/3609817 accessed July 31, 2017

[2] Magnet Forensics with MaCorr Research, "Digital Forensics," April 2015

COMMERCIAL ROOTING

Commercial exploits are less intrusive and take advantage of vulnerabilities within the Android OS to gain root access. One common method is to use a buffer overflow, such as Towel Root, that triggers embedded shell code. Since Android is a Linux variant, it is susceptible to Linux exploits as well.

To use an automated root, you must be able to get past the lockscreen to enable ADB. Roots, such as Towel Root, Kingo, and SafeRoot, are specific to make/model/OS combinations. They can also be specific to monthly security patches, which may plug exploits used for rooting

To use, verify device compatibility and always test on an exemplar—a device of the same make/model and OS/firmware (remember, for Android, you can update or rollback your device before using).[2]

Sometimes an evidence device comes to you already rooted. Device owners do this to get access to additional apps, to update their operating system, remove software skins or carrier bloatware, to increase speed and/or battery life, to create free wifi spots, or other customizations. Your documentation should state whether the device came to you already rooted.

ADB METHODS

These exploits enable examiners to obtain escalated privileges, such as system file modification or deletion, low level hardware access (e.g. using the dd command to duplicate data), full CPU and kernel control, or full application control—including the ability to backup, restore, or batch edit applications—to gain access to restricted Application Programming Interfaces (APIs).

USB debugging mode, when enabled, allows rooting to obtain administrative privilege. According to Yang et al. in their 2015 paper, "New acquisition method based on firmware update protocols for Android smartphones," either the ADB shell can be used for these acquisitions, or commercial forensic tools that incorporate the ADB method.

USB debugging mode, when enabled, allows rooting to obtain administrative privilege.

[2] Reiber (2016)

"However," the authors wrote, "because the rooting exploitation process is executed after the smartphone is booted; the integrity is damaged whenever data is acquired. In addition, existing rooting vulnerabilities are patched whenever the Android OS is updated with a new version; hence, a new rooting technique must be found whenever the Android OS is updated."[3]

ADB BACKUP

Available in Android 4.0 and later, this method requires you to unlock the lock screen and enable USB debugging. However, in the event there is no publicly available root for the device, you can create a logical or quick image via ADB Backup. You can use this method to backup individual apps or all apps except those protected by digital rights management (DRM); these backups include app data, cache, and internal storage.[4]

AGENT ACQUISITION

In some instances, to obtain additional data not included in ADB backups, some forensic software pushes a small application, known as an agent, to the user data partition to pull back additional logical data. This method also requires an unlocked device and USB debugging to be enabled and is often part of a quick/logical extraction. However, because it does leave a footprint, be sure your forensic tool's settings are such that the agent is removed when you're done, and document its use.

ADB PULL

The Pull command can be used to pull a specific folder, such as data/data.
It can create a quick/logical copy of a partition, or can be used to target a specific application; it does require root access and debugging enabled.[5]

DEAD EXPLOITS: WHEN ROOTING DOESN'T WORK

Some devices may be harder to root because it was programmed that way (often by a carrier seeking to limit device owners' ability to go off their network). Many times, however, rooting won't work simply because the device is locked and you can't get access:[6]

- The device owner wouldn't provide consent.
- The "smudge pattern" method, or guessing the PIN or pattern lock based on finger smudges on the screen, isn't possible.
- You don't want to risk bricking the device due to too many login attempts.
- You have no way to recover the passcode via flasher boxes and JTAG.
- You weren't able to remove the files that store the password hashes. (You didn't know this was possible? While in modified recovery mode via ADB without debugging enabled, you can bypass the lock, then attempt to enable USB debugging.)

[3] Yang, Seung Jei, Jung Ho Choi, Ki BomKim, & TaejooChang (2015), "New acquisition method based on firmware update protocols for Android smartphones," Digital Investigation 14:1, The Proceedings of the Fifteenth Annual DFRWS Conference, pp. S68-S72, http://www.sciencedirect.com/science/article/pii/S1742287615000535 accessed July 31, 2017
[4] Bommisetty, S., Tamma, R., & Mahalik, H. (2016). Practical mobile forensics. Birmingham: Packt Publishing.
[5] Bommisetty et al. (2016)
[6] Hyde, J. (2016- 2017), "CFRS 762 Mobile Device Forensics" [PDF], George Mason University MS Computer Forensics

In these cases, you can sometimes use a flasher box; or, you can boot the device into an alternative state through custom recovery or new, forensic bootloader.

Some devices may be harder to root because it was programmed that way (often by a carrier seeking to limit device owners' ability to go off their network). Many times, however, rooting won't work simply because the device is locked and you can't get access

FLASHER BOXES

"Flasher" boxes are hardware originally designed to upgrade or repair mobile device software. In the forensic world, they work by flashing a fresh bootloader to a device's RAM set to "rescue" or "download" mode. Flasher boxes work via jigs or cables without the need to solder.[7]

This method enables you to obtain memory areas and/or full dumps of devices that are otherwise unsupported. Alternatively, if you need a specific area of recovered memory and you know what it is, the box can obtain that specific range, too.

Flasher boxes allow for other adaptations on some devices, such as removing Android Factory Reset Protection (FRP) so that you can flash a custom recovery to a device for acquisition.[8]

Physical extraction for years has included hardware methods such as JTAG and in-system programming (ISP), as well as the more destructive hardware methods of chip-off and chip milling. Hardware methods, especially the destructive forms that require more time and effort, tend to be reserved for the most serious cases.[3]

[3] Yang et al. (2015)

[7] Reiber (2016)
[8] Hyde (2016-2017)

However, because they're service devices, flasher boxes carry risks:[9]

- They have both write and erase buttons available, so that you could erase or modify the data if you aren't careful.
- Not being forensic tools, flasher boxes don't have audit trails, logs, or hash verifications.
- Incorrect power/ground connections can lead to permanent device or memory damage.
- Their proprietary image format must be sent to the flasher box manufacturer so that they can return a dd or .bin image.
- They require internet connectivity to run, which may be against your lab procedures if you don't know what data is being sent over the internet.
- Many AV programs flag flasher boxes as malware; indeed, some flasher boxes are packaged with malware.

Finally, flasher boxes aren't one-size-fits-all; there are specific flasher boxes for different manufacturers, so multiple boxes and jigs are needed. While this isn't expensive because they're so cheap, they can get cumbersome especially in smaller lab spaces.

BOOTLOADERS

Consisting of code loaded from recovery or download mode and run in a runtime environment or operating system, forensic bootloaders replace an unlocked bootloader and sometimes the ROM. They allow access to the device without modifying it because they enable you to obtain evidence through a different boot mode. They don't require USB debugging or for the device to be unlocked; however, they're hardware dependent.

Bootloaders are most commonly incorporated directly into vendor tools, saving time and bypassing security mechanisms without flashing the device and risking the data. Rather than flash the device's RAM, the tool sends the bootloader to the device's RAM during the initial boot. The forensic bootloaders then execute "read only" actions that don't boot into the OS, but instead extract evidence from the device without leaving artifacts behind.

Different flasher boxes serve different purposes. Besides those made for the various manufacturers, there are also boxes made for JTAG communication, boxes made to communicate with counterfeit devices, and even some boxes designed to simply unlock phones from their current carrier or to perform PIN code/lock bypass.[4]

[4] Reiber (2016)

[9] Thackray, J, "Flasher Boxes: Back to Basics in Mobile Phone Forensics," Forensic Magazine, June 15, 2016, https://www.forensicmag.com/product-release/2010/07/flasher-boxes-back-basics-mobile-phone-forensics, accessed August 09, 2017

Forensic bootloaders allow access to the device without modifying it because they enable you to obtain evidence through a different boot mode. They don't require USB debugging or for the device to be unlocked; however, they're hardware dependent.

However, bootloaders have their own risks:

- Third-party, "black box" bootloaders used by some vendors have no access to the device's source code, so you can't be sure the tool isn't in some way modifying the evidence or causing the device to malfunction.
- Some vendors design their own bootloaders in-house around individual device platforms. This proprietary method eliminates the "black box" problem, but makes it impossible for you to explain how the tools work.
- Forensic bootloaders don't work when a device bootloader is locked.

Yang et al. (2015) described the following problems with existing physical acquisition methods:

- The Android kernel vulnerabilities that were exploited for acquisition were patched, requiring researchers to find new vulnerabilities.
- New security technologies, including both secure boot and Samsung KNOX in 2014, were introduced. (Since this paper was presented at DFRWS, of course, the introduction of Android 6.0—Marshmallow—and Android 7.0—Nougat—have only layered on these technologies.)
- The physical acquisition method based on flashing the custom recovery image was the only one to account for user data integrity; however, the authors wrote, "this method cannot guarantee the integrity of the entire flash memory dump because it also flashes the custom recovery image."
- The ADB protocol employed by many forensic tools doesn't work when disabled by pattern or password locks.

BOOTLOADER FLASHING

A locked bootloader doesn't mean the device has a password. Rather, it's a manufacturer setting that stops users from flashing new firmware unapproved by the vendor. As displayed in the diagram, during any attempted boot, a locked device boots into the green, yellow, or red states, part of Android's Verified Boot process. An unlocked device, on the other hand, is not intended to be verified and can therefore be flashed freely. An unlocked device always boots to the orange boot state.[10]

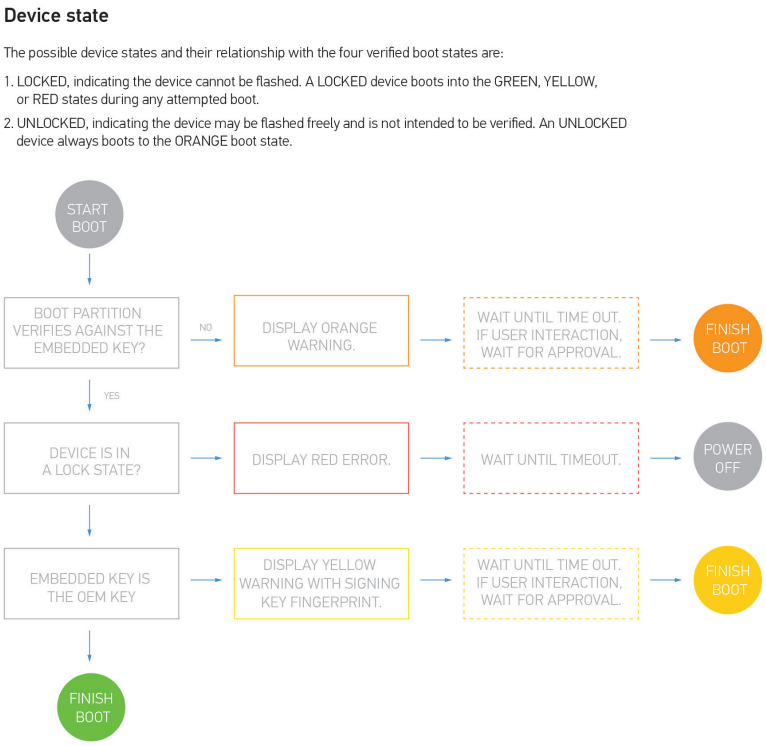

Figure 1. Verified boot flow

In bootloader flashing, the forensic software replaces the bootloader to grant root access by initializing the OS with elevated permissions. However, besides certain wireless providers, such as AT&T and Verizon, locking the bootloader, Android Verified Boot signs the boot chain so no part of it can be modified.

Flashing a locked bootloader naturally carries some risks:

- The device may not boot.
- The device may require a re-flash of stock ROM.
- User data may be lost.

Additionally, some vendors use clients to obtain a temporary root as part of bootloader methodology. As with agents, it's often necessary to uninstall the client.

[10] Android Source, "Verifying Boot," https://source.android.com/security/verifiedboot/verified-boot last updated July 7, 2017, accessed July 31, 2017

CUSTOM RECOVERY

Alternate recovery modes rely on providing full root access, using ADB to obtain a dd image. Android flash memory partitioning relies on the /recovery partition—an alternative boot partition on every Android device that allows you to boot the device into a recovery console to perform advanced recovery and maintenance. As with many other methods, this is risky: on some devices it involves factory resetting the devices, which wipes the user partition.

This is comparable to recovery partitions used for computers to help reset or restore factory settings. Android's /recovery partition contains its own Linux kernel, separate from the kernel of the main Android system so that it can boot into recovery mode even if the main system is broken.

Flashing a recovery image to an Android device will work on a phone even if it has a passcode lock, bypassing it completely and allowing you to acquire a full physical image of the device.

The /recovery partition is completely independent of the Android system, which offers a forensic advantage. Because recovery flashing allows you to replace the software in the recovery partition, you can put additional tools on the device—"custom recovery"—which can be accessed when the device is booted into recovery mode. Flashing a recovery image to an Android device will work on a phone even if it has a passcode lock, bypassing it completely and allowing you to acquire a full physical image of the device.

The /recovery partition stands in contrast to:

- the /boot partition, which enables the device to boot normally
- the /system partition, which contains the Android OS and preinstalled system applications
- the /data partition, which holds the majority of evidence
- the /cache partition, which holds frequently accessed app data
- /misc, which contains settings like carrier ID and some hardware settings
- /sdcard, the partition to which the external SD card is mounted. On a device that doesn't accept external SD cards, this partition may reflect the device's internal eMMC card.

One example of custom recovery that has been useful to forensic examiners is ClockWorkMod (CWM), which some device owners use to change the file system partition (usually to speed it up). Another is Team Win Recovery Project (TWRP), an open source community project that has become the leading open custom recovery for Android phones, supporting more than 500 devices at twrp.me/devices. The installation for both varies by device.

Flashing a new recovery partition requires the device to be put into download mode. Samsung's proprietary ODIN protocol, used for firmware updates, can also flash the device. For most other Android devices, the Google FASTBOOT protocol is used.

As evidenced by TWRP's popularity, flashing custom recoveries works on many models, but can be challenging. First, you must know the exact model of Android phone for it to work. Similar to loading your own recovery images to your forensic tools, the wrong recovery image will likely brick the device. In addition, with CWM, sometimes to install the custom recovery, you need to select to wipe the user partition.[11]

Finally, recovery images might bypass passcodes, but won't disable encryption. Even if you get a physical image of an encrypted device running Android 6.0 or 7.0, in all likelihood it won't contain usable evidence

[11] Lohrum, M, "Why not load ClockworkMod or TWRP to image a device?" Free Android Forensics, April 2, 2015, http://freeandroidforensics.blogspot.ca/2015/04/why-not-load-clockworkmod-or-twrp-to.html accessed August 9, 2017

When not to flash recoveries

Whether you're using custom recoveries or Magnet Forensics recovery images, you can expect two limitations: locked bootloaders (by carriers), and factory reset protection (FRP) (by OEMs). Many carriers such as Verizon and AT&T lock the bootloaders to prevent recovery methods like this, so just because you have the same model of phone for another carrier, doesn't mean it will work for all carriers. Make sure you double check to ensure that the device you're examining does not have a locked bootloader.

Flashing the recovery partition does not affect the user partition, but is a viable method for bypassing passwords and getting physical images of some of the most popular devices.

FRP affects Samsung devices running OS 5.1 or later. Once FRP is activated, it prevents use of a device following a factory data reset, until you log in using a Google username and password previously set up on the device. Further, FRP is not activated until you enter a Google account.

If you flash a recovery when the bootloader is locked or when FRP is on, the device may not boot, or will require a re-flash of stock ROM. In addition, you may lose user data. Bootloader lock status varies by device, so Google the device's physical key combination, then use Samsung's ODIN to determine the FRP lock status. If you see **FRP LOCK: ON, don't flash the device.**

Flashing the recovery partition does not affect the user partition, but is a viable method for bypassing passwords and getting physical images of some of the most popular devices.

DOES RECOVERY FLASHING CHANGE EVIDENCE?

Flashing recovery images does change the device—but only its recovery partition, and not the user area. You can document this using a test device of the same make, model, and Android OS version, pre-loaded with sample data. Because you'll know the device's passcode, you can acquire physical images both before and after flashing the recovery image. You can then compare the user data from each image to show that user data remains unchanged.

It's also important to document the fact that the recovery image remains on the recovery partition and that, on Samsung devices, you'll have tripped the KNOX Warranty Bit;[12] but that will not impact device usage.

Once your forensic acquisition is complete, restart the phone as you normally would, and the user area will load as it should. This is especially useful when imaging a victim's device that needs to be returned to them.

ANDROID RECOVERY ACQUISITIONS WITH MAGNET AXIOM

In previous versions of Magnet AXIOM, you were required to unlock and enable USB debugging for Android device acquisitions or use Magnet ACQUIRE to load your own custom recovery images. Now, we've built this acquisition into AXIOM, adding more than 650 recovery profiles for Samsung devices with plans to add more in the future, as new devices appear.

Besides retaining the ability for you to flash any custom recovery, such as TWRP, using AXIOM, Magnet Forensics has developed custom recoveries for 650+ Samsung devices to enable seamless physical imaging via Magnet AXIOM.

[12] Samsung Knox, "What is a Knox Warranty Bit and how is it triggered?" https://www.samsungknox.com/en/qa/what-knox-warranty-bit-and-how-it-triggered accessed July 31, 2017

Besides retaining the ability for you to flash any custom recovery, such as TWRP, using AXIOM, Magnet Forensics has included custom recoveries for 650+ Samsung devices to enable seamless physical imaging via Magnet AXIOM. Based on stock Android recovery partitions, this method:

- Bypasses device passwords without affecting the user data partition.
- Allows you to flash any device for which you have a recovery partition, provided the bootloader is unlocked.

The binary executable, a single program that can execute anything that AXIOM needs to do (such as querying device info to full imaging), enables root access to the memory blocks and contains proprietary imaging commands that allow physical imaging. This executable is fairly small and doesn't overwrite any user data; rather, it's part of the newly flashed recovery partition.

You can find a complete device list and Magnet Recovery Installer at: magnetforensics.com/downloadrecoveryimages

AS IMPORTANT AS EVER: DOCUMENTATION

No matter which mobile forensic method you use, document whatever you do.

- Start with what your search warrant or other legal authority allows you to get, as well as appropriate chain of custody logging.
- Validate what forensic tools claim to do, which can mean testing on a test device of the same make, model, operating system, and firmware version (and preferably after receiving the proper training).
- Where possible, use methods that don't alter user data; but either way, document your methods, including the steps you took to acquire the device and what data your method accesses.
- Record whether you performed a quick/logical or full/physical extraction, and what tool(s) and their version(s) you used.
- Device information:
  - Make
  - Model
  - Operating system and firmware version
  - Relevant apps (and their versions)
- Connection method used for each extraction:
  - Cable
  - USB
  - Bluetooth protocol API
  - Wi-Fi
  - Serial protocol (mostly for older devices)
- Finally, document your footprint: the changes your method makes to the device, based on observations from previous testing.

FIND OUT HOW MAGNET AXIOM CAN HELP

If you'd like to learn more about Magnet AXIOM and how it can help find decrypted and obfuscated evidence you may be missing with other solutions, visit magnetaxiom.com. While you're there, you can learn more about the product, request an in-depth personal demo from an AXIOM expert, and request a free 30-day trial version.

Learn more at magnetforensics.com

For more information call us at 1-844-638-7884
or email sales@magnetforensics.com