TAKING BYTES OUT OF ANDROID NOUGAT FORENSIC ANALYSIS

A GUIDE TO ANDROID 7.0'S FILE-BASED ENCRYPTION, DIRECT BOOT, AND OTHER SECURITY FEATURES

MAGNET FORENSICS®

TAKING BYTES OUT OF ANDROID NOUGAT FORENSIC ANALYSIS

In a rapidly changing and uncertain world, consumers continue to demand secure devices that protect their data from prying hackers, data thieves, and even, in some cases, governments. Apple still leads the way, but Google's latest round of security features ensure that even cheap, free smartphones can be encrypted.

Marshmallow (v6.0) leveled up from Lollipop (v5.0) by implementing a number of new security measures, which required a change in forensic processes. These security measures included:

- Improved full-disk encryption
- Application permissions
- Supported fingerprint API
- Improved factory reset protection (FRP)
- Gatekeeper password storage
- Adoptable storage encryption

Nougat (v7.0) represents another step up. In addition to Marshmallow's features, its new changes include:

- File-based encryption
- Credential vs. device encrypted storage

These impact more than just the device; they also affect each user of the device, with new directories and new file paths to be aware of as well as—perhaps most of all—new forensic acquisition methods.

What Android Marketplace Changes Mean for Forensics

Unlike Apple, Google doesn't automatically push OS updates to its users. Instead, carriers tend to control Android updates to allow for testing and approvals. This means that users can purchase a device that comes pre-loaded with the new OS, wait for an official carrier release, opt to update for themselves, or upgrade their devices.

As a result, Android OS adoption rates are much slower than those seen for iOS, and it can take months for a new Android OS to peak—often more than a year following its initial release. For example, by January 2017—about 15 months following its October 2015 release—Android Community reported that Marshmallow's distribution had jumped to 30%, up from its 19% distribution three months previously.

Nougat is following much the same pattern. Released in August 2016, its adoption rate has steadily increased, coming in at nearly 18 percent as of October 2017, a figure which—based on historical data from previous operating systems — is only expected to rise throughout 2018... just in time for Android Oreo, released in August 2017, to gain its first foothold. By comparison, iOS 11, released in September 2017, had a 52 percent adoption rate as of November that same year.

Nougat shipped with Google NEXUS or Pixel devices as early as April 2017; by October, it had been released on Samsung Galaxy S7 and S7 Edge, along with various models from LG V20, Sony Xperia, HTC, Motorola, Huawei, ZTE, and others according to an October 2017 TechRadar article.

In some ways, these much slower market changes make life easier for forensic examiners than Apple's all-at-once iOS updates; there's more time to research the new operating system, including the way it interacts on different devices and with different apps, before it reaches the majority of the marketplace.

In other ways, however, the changes also mean that examiners—whose caseloads can vary dramatically—need to keep in mind the differences across several versions, not just the two most recent releases, at all times.

Full Disk Encryption in Nougat

Just as it was in Marshmallow, full disk encryption is enabled by default. Remember: if the device has a lockscreen, it must support encryption; if the AES performance is higher than 50MiB/S the device must be encrypted. Full disk encryption is enabled with an AES 128-bit Key (the default is AES-CBC-ESSIV).

However, Marshmallow's full disk encryption meant that the device couldn't boot to its lockscreen. Therefore, if a device rebooted unexpectedly—if its battery died, or the system updated—the device owner was cut off from notifications about missed calls and text messages, alarms, and calendar items until they logged in again.

This could be a particular problem overnight and at other times when reboots caught users unawares. The reason, according to Android Authority:

> "Apps cannot function normally until the device is decrypted, so [until the user enters their credentials—their password, PIN or pattern] the device cannot perform essential tasks such as receiving incoming calls, emails or messages. It also means apps can't deliver notifications, or act on scheduled alarms – in fact, the only thing an encrypted device can really do is burn through its remaining battery life."

Other issues: the need for device users to create both boot credentials and user credentials. From a forensic standpoint, the boot credential meant that any hope of obtaining data even from JTAG, in-system programming (ISP), or chip-off physical extraction was lost.

Nougat resolves these issues with Direct Boot, "that strange no-man's land where the device has finished booting but isn't fully initialized yet" (as Android Authority called it). Direct Boot, that article went on to state, "...allows applications to perform limited tasks and access specific sections of data, even when the device is encrypted." All 7.0 and higher devices must support Direct Boot, even if the device isn't encrypted.

Credential vs. Device Encrypted Storage

To make some, but not all data available in Direct Boot, Android now contains two separate storage areas. Device Encrypted (DE) storage makes some data available after boot and as such, requires no password. Credential Encrypted (CE) storage makes data available only after the user credentials are entered.

Android now contains two separate storage areas. Device Encrypted (DE) storage makes some data available after boot and as such, requires no password. Credential Encrypted (CE) storage makes data available only after the user credentials are entered.

According to an Android Source piece, "This separation makes work profiles more secure because it allows more than one user to be protected at a time as the encryption is no longer based solely on a boot time password." It went on to note, however, "Although, without FBE, DE and CE storage will always be in the unlocked state."

SAMSUNG CONTINUES TO COMPLICATE EVERYTHING

In last year's "Demystifying Android Marshmallow Forensic Analysis" white paper, we noted how Samsung was following Apple's lead towards additional chip-level protection through:

- A different encryption algorithm.
- Strengthening its backup encryption.
- Encrypting handset PINs and passwords differently (before Gatekeeper's introduction).
- Putting its software through more iterations than other vendors.
- Manufacturing devices with the universal flash storage (UFS) chip rather than the industry standard eMMC chip.

In June, Samsung announced a new change: discontinued KNOX encryption software. Instead, according to a company statement, users of "Android N[ougat] OS or higher versions only" were encouraged to set up Secure Folder, a new app that "leverages the defense-grade Samsung Knox security platform to create a private, encrypted space.... Applications and data moved to Secure Folder are partitioned separately on the device and gain an additional layer of security and privacy."

Nougat, like Marshmallow, implements Google's standard dm-0 decrypted partition (a reference to its decryption tool, dm-crypt). (Nonetheless, in case of future changes, we still recommend using the "mount" command in the ADB shell to find the proper container within /dev/block.)

From a forensic standpoint, the dm-0 partition consists of all user data, decrypted and emulated. If you've performed a full physical extraction and have all partitions plus dm-0, you'll have both encrypted and decrypted containers. Note: you may not need the encrypted containers, especially with no obvious reason to take up storage with unusable data.

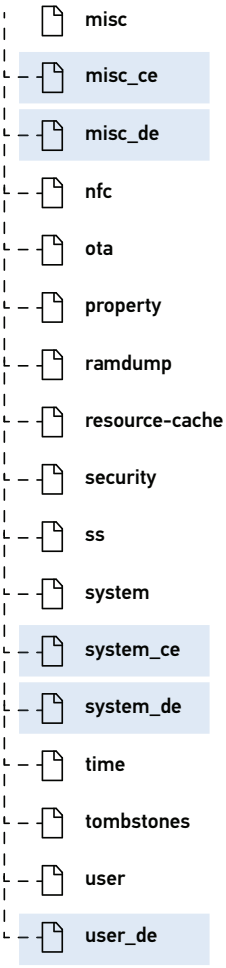
The associated file paths are misc_de and misc_ce, system_de and system_ce, and user_de (note: to protect user data, there is no user_ce directory. The file path is simply, for the primary user, /user/0). However, because of the new pathing—including new partition names to match the new CE/DE structure—some artifacts have moved:

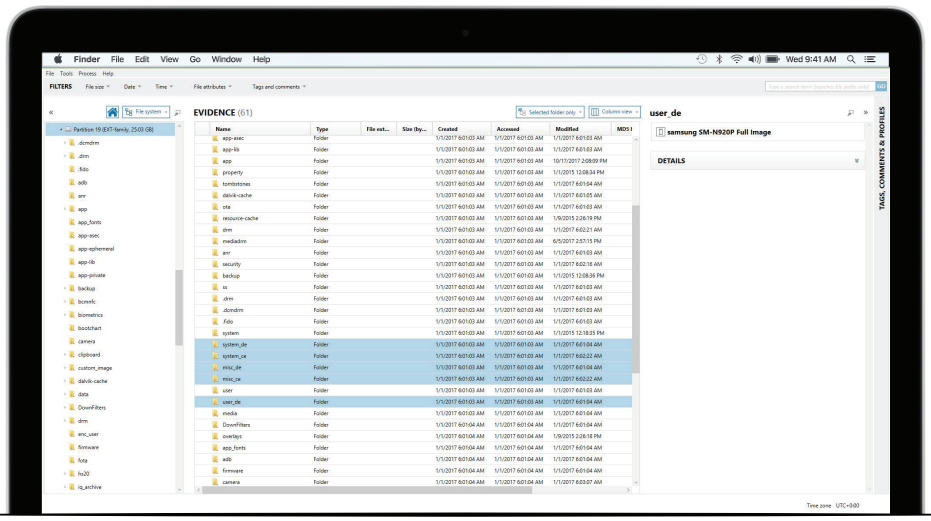
SMS/MMS
NEW /user_de/0/com.android.proiders.telephony/databases/smsmms.db
OLD /data/com.android.providers.telephony/databases/smsmms.db

CALL LOGS
NEW /data/com.android.providers.contacts/databases/calllog.db
OLD /data/com.android.providers.contacts/databases/contacts2.db

ACCOUNTS
NEW /system_ce/0/accounts_ce.db and /system_de/0/accounts_de.db
OLD /system/accounts.db

Note: while call logs have been moved out of contacts2.db, contacts still exist in the accounts database, which remains in the system partition, but now exists in CE and DE databases. To obtain data from the new calllog.db and from the CE and DE accounts containers, two new custom parsers are available in the Magnet Artifact Exchange. They enable you to search for fragments of data or run SQLite queries.





New in Nougat: File-Based Encryption

Direct Boot enables Nougat to add an entirely new layer of security to Android by offering the ability to encrypt not just the entire container, but also individual files within it. Shipped with Google Pixel and Pixel XL devices, file-based encryption (FBE) secures both:

- file contents (in AES with a key length of 256 bits [XTS mode])
- file names (in AES with a key length of 256 bits [CBC-CTS mode])

This enables apps to utilize Direct Boot APIs. To do so, however, "Keymaster/Keystore and Gatekeeper must be implemented in a Trusted Execution Environment (TEE) to provide protection for the DE keys so that an unauthorized OS (custom OS flashed onto the device) cannot simply request the DE keys," according to Android Source.

Moreover, states the article, "the Hardware Root of Trust and Verified Boot bound to the keymaster initialization is required to ensure that Device Encryption credentials are not accessible by an unauthorized operating system."

Credential Encryption must be bound to the user passcode; if there is none, it uses the device's default password. It must also be unique to the device, and can't match the key for another user.

For a Nougat device that's FBE-capable but not delivered with it enabled, the user can enable FBE from the Developer Options Menu. However, this causes a full wipe of the /data partition before encrypting data, so users who did not enable FBE during initial setup may opt out of enabling FBE at all.

An FBE-enabled device cannot have a shell or permanent root applied for acquisition purposes. Instead, custom recovery methodology is recommended because the recovery partition already has root privileges.

From a forensics perspective, this means an FBE-enabled device cannot have a shell or permanent root applied for acquisition purposes. Instead, custom recovery methodology is recommended because the recovery partition already has root privileges. As a result, it's unnecessary to make a user environment with root privileges. Note: sometimes it may only be possible to obtain logical extractions.

The Multi-User Environment in Android Nougat

Multiple users of a single device started to be supported by default in Android v5.0 (Lollipop). A June 2016 article from mobile technology review site Pocketnow explained that uptake has been primarily among family tablet users, perhaps less so on mobile phones.

Android Source lays out device administration in the following terms:

- A user is a distinct physical person with their own app data, certain settings, and user interface. User types consist of:
  - A primary user is the first added to a device, with privileges and settings available only to that user. Only a factory reset can remove this user, and the primary user always runs even in the background.
  - A secondary user can be added to or removed from the device and cannot affect other users. They can run in the background and still have network connectivity.
  - A guest is a temporary secondary user and can be deleted when no longer needed. Only one guest user at a time is allowed.
- An account is contained within a user, but neither accounts nor users link to or define one another. According to Android Source, "Users and profiles contain their own unique accounts but are not required to have accounts to be functional."
- A profile has separate app data, but shares system settings like connectivity. Unlike an account, a profile requires a user, and a user can have multiple profiles. There are two profile types:
  - Managed profiles are designed for corporate use. The profile owner—the app that created the profile—manages it as a container for work data and apps, and the profile shares a launcher, notifications, and recent tasks with the device's primary user. As of Nougat, users can disable the managed profile when it isn't needed.
  - Restricted profiles, available only for tablets and television devices, use accounts based on the primary user, who defines which apps are available to that profile.
- An app consists of data that exists within each associated user, sandboxing data from other apps within the same user.

"By default," Android Source explains, "only the primary user has full access to phone calls and texts. The secondary user may receive inbound calls but cannot send or receive texts. The primary user must enable these functions for others." However, in a multi-user environment, the following may affect forensic investigations:

- Notifications appear for all accounts of a single user at once.
- Notifications for other users do not appear until active.
- Each user gets a workspace to install and place apps.
- No user has access to the app data of another user.
- Any user can affect the installed apps for all users.
- The primary user can remove apps or even the entire workspace established by secondary users.

While this directory structure conveniently segments or sandboxes user data, "putting the user behind the keyboard" may not be any easier than in a single-user environment. A user who knows another user's credentials can still use that account for illicit activity, so just because a suspect may have their own account on a device, doesn't mean the others shouldn't be investigated.

A user who knows another user's credentials can still use that account for illicit activity, so just because a suspect may have their own account on a device, doesn't mean the others shouldn't be investigated

In turn, this may run afoul of privacy protections designed to protect innocent users from overreach, so search warrants may need to specify particular time/date ranges rather than individual accounts or directories. As always, double check with an attorney on the best way to adapt search warrants to these latest features.

Regardless of where you find multiple user accounts, you can expect directory paths that follow a binary pattern. /user/0 is the default directory (comparable to /data/data); the second user will be /user/10; the third, /user/11; and so on. Moreover, each user will have their own CE and DE partitions. "Direct Boot even provides separate encryption contexts for different users on the phone," wrote Matthew Green in a blog post about Nougat encryption.

A full physical extraction should show the paths that demonstrate whether multiple users exist. Be aware, however, that this may not be the same as having access to the data within those containers. You may need to perform multiple acquisitions per each profile (and its appropriate password or PIN) to obtain CE data unencrypted.

Adapting and Evolving Your Forensic Skill Set

Like Marshmallow before it, Nougat offers the ability to improve your forensic skill set by applying new extraction and analysis methods, expanding your toolbox and the expertise to use it. By eliminating the boot password, implementing Direct Boot, and preventing FBE from being enabled on rooted devices, Google does continue to limit the ability to obtain full physical extractions.

Therefore, although it's still ideal to obtain a device's pattern or PIN lock in order to perform a full physical extraction, without one it should be possible to obtain at least minimal information from device-encrypted storage with a logical extraction.

At the same time, however, maintaining awareness of new file paths and multiple users is necessary to ensure you're pointing your forensic tool at the correct partitions to capture all the data—especially as you may be relying on newer, recovery-based acquisition methods.

EFFECTIVE ANDROID FORENSIC EXAMINATIONS WITH MAGNET AXIOM

Magnet AXIOM is comprehensive digital forensics software that can ingest and analyze data from a variety of smartphones and operating systems, including Android Nougat:

- Easily ingest images from other tools, JTAG, chip-off and other third-party processes. Note: physical extractions of encrypted data will be unreadable by any processing tool without device/user credentials.
- Acquire data from hundreds of smartphones through AXIOM's custom recovery images, integration of TWRP images, backup methods, and other means.
- Recover more artifacts from unallocated space by extracting data from fragmented files and databases that are not sequential, out of order, or missing entirely.
- Queue multiple devices and device types for image acquisition through AXIOM automation.
- Aggregate data from multiple devices and the cloud into one case file to create a fully interactive, exportable timeline with all known data.
- Trace app and file artifact evidence back to its source location with one click to quickly verify the evidence's existence in the source data.
- Retrieve multiple artifacts from apps that go beyond just chat. Layer in filters for geotag information, dates and times, browsing history, and more.
- Access and analyze digital evidence data from the artifacts database, the file system or the registry.
- Leverage more than eight evidence views including World Map, Histogram, Timeline, Chat Thread, and more to tell the evidentiary story.
- Identify possible child luring intent in chat messages with integrated Magnet.AI.
- Import and export pictures between AXIOM and Project VIC and ICSE (formerly CAID) to process them against known hash sets; and between AXIOM and Griffeye to integrate uncategorized-to-categorized data back into AXIOM.
- Use Connections in AXIOM to quickly connect artifacts and files to show relationships: Where was the artifact found? How did it get on the system? How was it shared? Was there intent? Share all found or a targeted subset of evidence in a Portable Case to stakeholders at all technical skill levels – whether they have a license or not. Merge their comments and tags back in quickly and easily for the best collaboration.
- Take our four-day Magnet AXIOM Advanced Mobile Forensics (AX300) training course to learn how to maximize these capabilities for your investigations. Skilled trainers bring context and value of their extensive practical experience.

Find out how Magnet AXIOM can help

If you'd like to learn more about Magnet AXIOM and how it can help you acquire, analyze, and present digital evidence most effectively, 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