DA FORENSICS
Digital Analysis you can Trust

I. Mobile Phone Forensic Examinations for Defense Attorneys and Investigations

Mobile phones frequently contain the most important digital evidence in modern investigations. Text messages, encrypted messaging applications, location data, internet activity, photos, system logs, and application records can reveal critical timelines and user behavior.

As a **licensed private investigator and digital forensic examiner**, I provide **independent mobile phone forensic analysis** for defense attorneys, civil litigation, and private investigations involving both **iPhone (iOS) and Android devices**.

Understanding what evidence can be recovered from a phone depends largely on **how the device was extracted and whether investigators had access to the device passcode at the time of the forensic acquisition**. The availability of a passcode significantly affects the type and amount of digital evidence that can be recovered.

Consent-Based Mobile Device Examinations

As a **Texas licensed private investigator**, my examinations must be conducted within the legal authority available to private parties. Unlike law enforcement agencies, which may obtain search warrants or court orders, private investigators conduct **consent-based forensic extractions**.

This means the device owner must authorize the examination and provide access to the device when required.

Because of this legal limitation, the most common extractions I perform for defense attorneys and clients are:

- **Logical+ Extractions**
- **Full File System (FFS) Extractions**

Both of these extraction methods require the **device passcode and owner consent**, but they also provide the most valuable forensic evidence available on a mobile device.

Why Passcodes Matter in Mobile Phone Forensics

In many criminal investigations, law enforcement may seize a phone but **not obtain the passcode**. When that occurs, investigators may only be able to perform limited extractions that provide minimal data.

This limitation can significantly affect the completeness of the digital evidence reviewed in a case.

For defense attorneys, this distinction is critical. If law enforcement only obtained a limited

DA Forensics, Inc.,300 Burnett Street, Suite 144, Fort Worth, TX 76102 | TX Lic# A10518901

extraction due to the lack of a passcode, **additional evidence may still exist on the device that was never examined**.

As part of my forensic work, I frequently review:

- The **type of extraction performed by law enforcement**
- The **state of the device (locked, BFU, AFU)**
- Whether a **more comprehensive extraction was possible**

When legally authorized, I can conduct an **independent forensic examination** to determine whether additional artifacts exist.

Differences Between Forensic Tools

Several forensic platforms are commonly used in mobile device investigations. Two of the most widely used tools are:

- **Magnet Forensics (AXIOM / Verakey)**
- **Cellebrite UFED / Physical Analyzer**

While these tools often recover similar types of digital artifacts, they **categorize and perform extractions differently**.

For example:

Magnet Forensics frequently describes extractions based on **device state**, such as:

- Quick Image
- BFU (Before First Unlock)
- Logical+
- AFU (After First Unlock)
- Full File System

Cellebrite tools typically categorize extractions by **method**, such as:

- Logical / Content Type extraction
- User Data extraction
- File System extraction
- Physical extraction

Despite these differences in terminology, the underlying concept is the same:

The more access the forensic tool has to the device, the more digital evidence can be recovered.

Both platforms also depend heavily on factors such as:

- Device model
- Operating system version
- Security patch level

- Encryption state
- Whether the passcode is known

Independent Digital Forensic Analysis of iPhone and Android Devices

My laboratory utilizes **industry-recognized digital forensic tools** capable of analyzing data from both **Apple iOS devices and Android mobile phones**.

These tools allow for detailed examination of:

- Text messages and iMessage records
- Encrypted messaging applications (such as Signal and similar platforms)
- Call logs and voicemail records
- Location artifacts and GPS history
- Internet browsing activity
- Application usage data
- Photos, videos, and metadata
- System logs and device activity records

When a **Full File System extraction** is available, additional encryption material stored on the device—such as credentials and encryption keys—may allow forensic access to protected application databases.

This can be particularly important when analyzing **secure messaging applications**, which often store their encryption keys within the device's secure storage system.

Why Independent Mobile Phone Forensics Matters

Digital evidence recovered from mobile devices is often central to criminal cases and civil litigation. However, the **scope of the evidence examined may depend entirely on how the device was extracted and whether the passcode was available**.

An independent forensic review can help determine:

- Whether law enforcement conducted a **complete extraction**
- Whether **additional artifacts exist** on the device
- Whether **location data supports or contradicts investigative conclusions**
- Whether **application data or communications were overlooked**
- Whether **digital evidence supports the defense timeline**

Mobile Phone Forensic Services

I provide forensic examinations and consulting services involving:

- **iPhone forensic analysis**
- **Android forensic analysis**
- **Cell phone data extraction and review**

- **Encrypted messaging application analysis**
- **Location data and GPS artifact analysis**
- **Independent review of law enforcement forensic reports**
- **Expert witness testimony in digital evidence cases**

Understanding Mobile Phone Extraction Types

The amount of data available from a phone depends on the **type of forensic extraction performed**.

The following sections explain the **primary categories of mobile device extractions**, the type of data available from each method, and how the presence or absence of a device passcode can affect the results of a forensic examination.

This information is intended to help **defense attorneys, investigators, and legal professionals understand the differences between extraction methods and the potential evidence available from mobile devices.**

II. iOS Extraction Types (Incremental Evidence Access)

1. Quick Image / Backup

Passcode Required: No

Provides limited data obtained from backups or trusted device pairings.

Artifacts may include:

- Device identifiers - Basic device identifiers such as model, serial number, and OS version.
- Basic system usage data - Limited system statistics showing general device activity patterns.
- Partial SMS databases - Basic text message records if present in backup data.
- Backup message records - Backup copies of text and multimedia messages stored through device backups.
- Limited media files - Some photos or media files included in backups or accessible areas.

Summary

Provides very limited evidence and often relies on backup data rather than the device itself.

2. Before First Unlock (BFU)

Passcode Required: No

Occurs when the device has been powered on but **not unlocked since reboot**.

Artifacts may include:

- Voicemail Metadata - Records identifying voicemail messages and timestamps.
- Media Metadata - Information describing media files such as creation times and file properties.
- System Metadata - Limited system configuration and activity information.
- Partial Application Data - Small portions of app data accessible without user authentication.
- Partial Account Data - Basic account identifiers without full account databases.

Summary

Apple encryption prevents access to most user data until the device is unlocked.

3. Logical+ Extraction

Passcode Required: Yes

Provides substantial user activity artifacts including:

- User Accounts - Accounts configured on the device such as Apple ID or email accounts.
- SMS Databases - More complete text messaging records.
- Media Catalog - Expanded access to photos and videos stored on the device.
- Notes Database - User-created notes stored in Apple Notes.
- Installed Apps - List of installed applications and basic app information.
- Device Information - Detailed device configuration information.
- Calendar - User calendar entries and scheduled events.
- Web History - Browsing history from Safari or other browsers.
- Web Searches - Records of searches performed in browsers.
- App Intents - Records of application usage interactions.
- KnowledgeC Database - Apple's activity database recording device usage behavior.
- Cached Locations - Recently stored GPS-based location records.
- Significant Locations - Locations frequently visited by the user.
- Wi-Fi Locations - Location estimates derived from Wi-Fi access points.
- Cellular Locations - Location approximations derived from cellular towers.

Summary

Logical+ extraction provides **substantial user activity evidence**, particularly related to **communications and location history**.

4. After First Unlock (AFU)

Passcode Required: Not necessarily

Occurs when the phone has been unlocked at least once after reboot.

Artifacts may include:

- Biome Database - Apple behavioral activity database showing user interactions with the device.
- File System Events - - Logs showing file creation, deletion, and modification activity.
- Internet History Artifacts - Expanded browsing and network history data.
- Network Usage - Statistics showing how apps use network connections.
- Account Records - More detailed account information.
- Third-Party App Data - Additional application data from installed apps.
- Location Metadata - Additional device location records.
- Screen Time Usage - Detailed statistics on how apps were used.
- Apple Notes Database - Expanded notes data and metadata.
- iMessage/SMS/MMS - More complete messaging artifacts.
- Call Logs - Records of phone calls placed or received.
- Voicemail Data - Expanded voicemail artifacts.
- Contacts - Full contact list stored on the device.
- Media Files - Expanded access to photos, videos, and attachments.
- Partial Keychain - Limited access to stored credentials and authentication tokens.

Summary

AFU allows investigators to access **protected user data classes** that become available once the phone has been unlocked after boot.

5. Full File System (FFS)

Passcode Required: Usually Yes

Provides the most comprehensive forensic access, including:

- Full Filesystem - Complete directory structure of the device storage.
- System Event Logs - Logs showing system processes and device activity.
- Screenshot Usage - Records of screenshot activity and files.
- First-Party App Databases - Full databases from Apple applications such as Photos, Messages, and Mail.
- Apple Email - Email content and metadata stored locally.
- Apple Health - Health and fitness records such as steps, heart rate, and workouts.
- Full Keychain - Stored credentials, authentication tokens, and encrypted secrets.
- Cached Apple Locations - Additional Apple system location artifacts.
- Application Containers - Complete data from installed applications.
- System Configuration Files - System settings and configuration artifacts.
- Deleted/Hidden Artifacts - Files and artifacts recoverable from the complete filesystem.

Full iOS Keychain

The **Full Keychain** contains encryption keys used by many third-party applications (such as Signal), and these keys are often required to decrypt protected application databases during forensic analysis.

Summary

FFS provides the most comprehensive forensic access, enabling recovery of complete application data, credentials, system logs, and potentially deleted artifacts.

Simplified Forensic Comparison

Extraction	Passcode Needed	Evidence Level
Quick Image	No	Very limited backup data
BFU	No	Minimal metadata
Logical+	Yes	Communications and user activity
AFU	Not always	Expanded protected user data
FFS	Usually yes	Full forensic access

III. Android Device Extraction Types (Incremental Evidence Access)

1. Quick Image / Backup

Passcode Required: No

Artifacts may include:

- Limited ADB Backup Data - Small subset of application data obtained through Android Debug Bridge backup commands.
- ADB Pull Command Data - Files that can be copied directly from accessible directories using Android debugging tools.
- Logcat Data - System logging records showing device activity, errors, and application events.
- Dumpsys Output - Diagnostic system information describing device services, running processes, and system status.

Summary

Provides **limited system-level information and partial app data**, often used for quick triage or preliminary analysis.

2. Before First Unlock (BFU)

Passcode Required: No

Artifacts may include:

- Partial Multimedia - Some media files stored in areas accessible before device unlock.
- Account Information - Limited user account identifiers stored on the device.
- Wi-Fi Profiles - Information about previously connected wireless networks.
- Installed Applications - List of applications installed on the device.
- Android Usage History - Records of device usage and application activity.
- Bluetooth Profiles - Records of paired Bluetooth devices.

Summary

Encryption protects most user data until the device is unlocked, so only **limited configuration and usage artifacts** are available.

3. After First Unlock (AFU) – Locked
Partial

Passcode Required: Not always

Artifacts may include:

- 3rd Party Application Data - Partial data from installed applications.
- Partial User Accounts (CE & DE) - Data from credential-encrypted and device-encrypted storage areas.
- Wi-Fi Information - Detailed records of wireless network connections.
- Installed Applications - Expanded application metadata and configuration.
- Android Keystore (possible) - Encrypted key storage used by applications.
- Android Usage History - Expanded records of user activity and application launches.
- Internet History - Browser activity and visited websites.
- Calendar Entries - Calendar events stored locally or synced accounts.
- Web Searches - User search history from browsers or system services.
- App History & Screenshots - Records of application activity and screenshots.
- Location Metadata - Device location records from GPS, Wi-Fi, or network sources.
- Notes - User-created notes stored on the device.
- SMS/MMS - Text and multimedia messaging records.
- Call Logs & Voicemail - Phone call history and voicemail metadata.
- Contacts - Stored contact information.
- Email - Email metadata or locally stored messages.

Summary

Once the device has been unlocked after boot, Android allows access to **many additional user data artifacts**, even if the phone is later locked.

4. Full Filesystem (FFS)

Passcode Required: Usually Yes

Provides the most comprehensive Android forensic access, including:

- Full Application Data - Complete databases and files from installed applications.
- Multi-User Account Data - Data from all user profiles stored on the device.
- Wi-Fi Profiles - Full wireless connection history and configuration.
- Installed Applications - Complete application packages and data directories.
- Android Keystore - Encryption keys used by applications and system services.
- Android Usage History - Detailed records of user interactions and application launches.
- Internet History - Full browser databases and web activity records.
- Calendar Entries - Complete calendar data from Android or Google accounts.
- Web Search History - Detailed records of search activity.
- App History & Screenshots - System-level records of application usage.
- Location Metadata - Complete location databases and metadata.
- Notes - Local and application-based notes databases.
- SMS/MMS - Complete messaging databases and attachments.
- Call Logs & Voicemail - Full call history records.
- Contacts - Complete address book databases.
- Email - Email databases and attachments stored on the device.
- Multimedia Files - Photos, videos, audio files, and associated metadata.
- Account CE & DE Data - Credential-encrypted and device-encrypted storage areas.

Summary

A Full Filesystem extraction provides the most complete forensic access to an Android device, allowing investigators to examine full application databases, user activity artifacts, system records, and potentially recover additional evidence from application storage areas.

Simplified Android Extraction Comparison

Extraction	Passcode Needed	Evidence Level
Quick Image / Backup	No	Minimal system data
BFU	No	Limited device configuration
AFU Locked Partial	Not always	Expanded user artifacts
Full Filesystem (FFS)	Usually yes	Complete application and user data

Final Observations

Mobile device evidence can vary dramatically depending on **how the device was extracted and whether the passcode was available**.

For defense attorneys, understanding these differences is essential. In many cases, a limited extraction performed by investigators may not represent the **full amount of digital evidence that exists on a device**.

An independent forensic examination can help determine whether additional artifacts exist that may be relevant to the investigation or defense strategy.