# Mobile Forensics Cheatsheet: iOS and Android System Artifacts

Belkasoft X
belkasoft.com/x

Belkasoft
forensics made easier

**Mobile system artifacts contain valuable data, ranging from device information and settings to detailed records of application usage.**

## Android system files

Typically only occur in "**file system**" images. The availability of artifacts depends on the models and versions of Android devices.

### Device information

| | |
|---|---|
| **IMEI** | \data\drm\pvt\ahrh |
| **Device shutdown timestamps and reasons** | \data\system\shutdown-checkpoints\checkpoints-%number% |
| **Last boot time** | \data\misc\bootstat\last_boot_time_utc |
| **Lock screen settings** | \data\system\locksettings.db |
| **Last factory reset time** | \data\misc\bootstat\factory_reset |
| **SIM card details** | \data\user_de\%usernumber%\com.android.providers.telephony\databases\telephony.db |
| **Android ID, Bluetooth name & address** | \data\system\users\%usernumber%\settings_secure.xml |
| **Battery percentage** | \data\user\%usernumber%\com.google.android.apps.turbo\databases\turbo.db |
| **Android OS version** | \data\system\usagestats\%usernumber%\version |

### ADB, Bluetooth & Wi-Fi connections

| | |
|---|---|
| **List of used ADB hosts** | \data\misc\adb\adb_keys |
| **Battery usage by Bluetooth devices** | \data\user\%usernumber%\com.google.android.apps.turbo\databases\bluetooth.db |
| **Bluetooth info** | \data\misc\bluedroid\bt_config.bak |
| **Bluetooth info & Paired Bluetooth devices** | \data\misc\bluedroid\bt_config.conf |
| **Wi-Fi connections** | \data\misc\wifi\softap.conf<br>\data\misc\wifi\WifiConfigStore.xml |

### Application usage

| | |
|---|---|
| **Accounts used in apps and services** | \data\system_de\0%usernumber%accounts_de.db |
| **App accounts with authentication tokens** | \data\system_ce\%usernumber%\accounts_ce.db |
| **App usage statistics** | \data\data\com.google.android.apps.turbo\shared_prefs\app_usage_stats.xml |
| **App activity with timestamps (Digital Wellbeing Google)** | \data\user\%usernumber%\com.google.android.apps.wellbeing\databases\app_usage |
| **App activity with timestamps (Digital Wellbeing Samsung)** | \data\data\com.samsung.android.forest\databases\dwbCommon.db |
| **Battery usage by apps** | \data\data\com.google.android.settings.intelligence\databases\battery-usage-db-v4 |
| **Notifications** | \data\data\com.google.android.gms\files\fcm_queued_messages.ldb |
| **Installed app packages with update timestamps** | \data\data\com.android.vending\databases\frosting.db |
| **App & device usage with timestamps** | \data\data\com.google.android.as\databases\reflection_gel_events.db |
| **Google Play search suggestions** | \data\data\com.android.vending\databases\suggestions.db |
| **Recent activity** | \data\system_ce\%usernumber%\recent_tasks\%number%_task |

### Application permissions

| | |
|---|---|
| **Runtime permission usage by apps** | \data\system\appops.xml |
| **Apps package details & granted runtime permissions** | \data\system\packages.xml |
| **Granted app runtime permissions** | \data\system\users\%usernumber%\runtime-permissions.xml |

Articles on Android system artifacts

Articles on iOS system artifacts

## iOS system files

Can be found in "**full file system**" (FFS) images, and many of them are also **part of backup images**.

### Device information

| | |
|---|---|
| **Bash command history** | FFS: \private\var\root\.bash_history |
| **Device product ID & serial number** | FFS: \private\var\containers\Data\System\%GUID%\Library\activation_records\activation_record.plist |
| **Unique device identifier (UDID)** | FFS: \private\var\root\Library\Caches\locationd\cache.plist<br>FFS: \private\var\mobile\Library\locationd\user.plist |
| **Directory Services Identifier (DSID)** | FFS: \private\var\mobile\Library\Preferences\com.apple.itunescloud.plist<br>Backup: \HomeDomain\Library\Preferences\com.apple.itunescloud.plist |
| **Last iTunes backup time** | FFS: \private\var\mobile\Library\Preferences\com.apple.mobile.ldbackup.plist<br>Backup: \HomeDomain\Library\Preferences\com.apple.mobile.ldbackup.plist |
| **AirDrop ID** | FFS: \private\var\mobile\Library\Preferences\com.apple.sharingd.plist<br>Backup: \HomeDomain\Library\Preferences\com.apple.sharingd.plist |
| **Device & iOS details** | FFS: \private\var\System\Library\CoreServices\SystemVersion.plist |

### System settings

| | |
|---|---|
| **Language, locale & keyboards** | FFS: \private\var\mobile\Library\Preferences\.GlobalPreferences.plist<br>Backup: \HomeDomain\Library\Preferences\.GlobalPreferences.plist |
| **Accounts used with iOS services & apps** | FFS: \private\var\mobile\Library\Accounts\Accounts3.sqlite<br>Backup: \HomeDomain\Library\Accounts\Accounts3.sqlite |
| **Time zone** | FFS: \private\var\mobile\Library\Preferences\com.apple.AppStore.plist<br>Backup: \HomeDomain\Library\Preferences\com.apple.AppStore.plist |
| **Find My iPhone preferences** | FFS: \private\var\mobile\Library\Preferences\com.apple.icloud.findmydeviced.FMIPAccounts.plist<br>Backup: \HomeDomain\Library\Preferences\com.apple.icloud.findmydeviced.FMIPAccounts.plist |
| **Location Services preferences** | FFS: \private\var\mobile\Library\Preferences\com.apple.locationd.plist<br>Backup: \HomeDomain\Library\Preferences\com.apple.locationd.plist |
| **SMS retention preferences** | FFS: \private\var\mobile\Library\Preferences\com.apple.mobileSMS.plist |
| **Device name & iOS version** | FFS: \private\var\root\Library\Lockdown\data_ark.plist |
| **iOS version and build** | \private\var\installd\Library\MobileInstallation\LastBuildInfo.plist |

### SIM information

| | |
|---|---|
| **ICCID & Phone Number** | FFS: \private\var\wireless\Library\Preferences\com.apple.commcenter.plist<br>Backup: \WirelessDomain\Library\Preferences\com.apple.commcenter.plist |
| **ICCID, Phone number & Cell provider** | FFS: \private\var\wireless\Library\Preferences\com.apple.commcenter.device_specific_nobackup.plist |
| **Details of used SIMs** | FFS: \private\var\wireless\Library\Databases\CellularUsage.db<br>Backup: \WirelessDomain\Library\Databases\CellularUsage.db |

### Bluetooth, Wi-Fi & Cell usage

| | |
|---|---|
| **Paired Bluetooth devices** | FFS: \private\var\containers\Shared\SystemGroup\%GUID%\Library\Preferences\com.apple.MobileBluetooth.devices.plist<br>Backup: \SysSharedContainerDomain-systemgroup.com.apple.bluetooth\Library\Preferences\com.apple.MobileBluetooth.devices.plist |
| **Paired low energy Bluetooth devices** | FFS: \private\var\containers\Shared\SystemGroup\%GUID%\Library\Database\com.apple.MobileBluetooth.ledevices.paired.db<br>Backup: \SysSharedContainerDomain-systemgroup.com.apple.bluetooth\Library\Database\com.apple.MobileBluetooth.ledevices.paired.db |
| **Observed low energy Bluetooth devices** | FFS: \private\var\containers\Shared\SystemGroup\%GUID%\Library\Database\com.apple.MobileBluetooth.ledevices.other.db<br>Backup: \SysSharedContainerDomain-systemgroup.com.apple.bluetooth\Library\Database\com.apple.MobileBluetooth.ledevices.other.db |
| **Network usage details** | FFS: \private\var\preferences\SystemConfiguration\preferences.plist |
| **Cell tower locations & Wi-Fi details** | FFS: \private\var\System\Library\Caches\locationd\cache_encryptedB.db |
| **Wi-Fi connections** | FFS: \private\var\preferences\SystemConfiguration\com.apple.wifi-private-mac-networks.plist |
| **Wi-Fi Mac addresses** | FFS: \private\var\preferences\SystemConfiguration\NetworkInterfaces.plist |
| **Device serial number & GeoFences** | FFS: \private\var\root\Library\Caches\locationd\consolidated.db<br>Backup: \RootDomain\Library\Caches\locationd\consolidated.db |

### Application usage

| | |
|---|---|
| **Device lock records & more** | FFS: \private\var\mobile\Library\AggregateDictionary\ADDataStore.sqlitedb |
| **Application usage timestamps & traffic** | FFS: \private\var\wireless\Library\Databases\DataUsage.sqlite<br>Backup: \WirelessDomain\Library\Databases\DataUsage.sqlite |
| **Detailed application & device usage records** | FFS: \private\var\mobile\Library\CoreDuet\Knowledge\knowledgeC.db<br>FFS: \private\var\mobile\Library\Biome\streams |
| **Notifications** | FFS: \private\var\mobile\Library\UserNotifications\%GUID%\PendingNotifications.plist<br>FFS: \mobile\Library\DuetExpertCenter\streams\userNotificationEvents\local\%number% |
| **Photos app information** | FFS: \private\var\mobile\Media\PhotoData\Photos.sqlite<br>Backup: \CameraRollDomain\Media\PhotoData\Photos.sqlite |

**On-demand course "Android Forensics with Belkasoft"**

**On-demand course "iOS Forensics with Belkasoft"**

**Belkasoft X** helps acquire "file system" and backup images from iOS and Android devices. It automatically extracts data from the listed mobile system artifacts and from many other operating system-specific and third-party apps.

In **Belkasoft X**, you can locate extracted system data in the "Artifacts" window under the System files node and partially under the Mobile applications node. Alternatively, you can find them grouped by the type of information they contain in the "Overview" window.

You can examine data extracted from system files by **Belkasoft X** and explore source files using convenient raw data viewers: SQLite, Plist, and Hex.