

Common Smartphone Evidence Locations

Some of the artifacts listed for the iPhone and Android may be recoverable from all dumps or just physical access depending on the device."

Partition	File	Description
Data	/com.android.providers.contacts/databases/contacts2.db /com.android.providers.contacts/databases/calling.db /com.sec.android.provider.logsprovider/databases/Logs.db	Call logs Call logs (OS 7) Call logs and more!
Data	/system/accounts*.db	User account information
Data	/com.android.providers.contacts/databases/contacts2.db /com.android.providers.contacts/databases/contacts3.db	Contacts Contacts (OS 7)
Data	/com.android.providers.telephony/databases/mmssms.db	SMS/MMS
Data	/com.google.android.apps.maps/*	Maps
Data	/com.sec.android.daemonapp/db/weatherClock	Location artifacts
Data	/com.google.android.gm/databases/<mail-name>.db	Gmail snippets
Data	/com.google.android.gms/databases/herrevad	Wireless and MAC addresses
Data	/system/locksettings.db and locksettings.db-WAL	Lock settings information
Data	/com.android.providers.settings/databases/settings.db and settings.db-WAL	Lock settings information
Data	/com.android.providers.media/external*.db and external*.db-WAL	Traces to SD card used in the device.
Data	/com.android.vending/databases/localappstate.db	Application traces
Data	/com.samsung.android.providers.context.databases.ContextLog_0.db (OS 7)	Application traces for Samsung devices
Data	/com.google.android.gms/databases/NetworkUsage.db /com.google.android.gms/databases/ns.db /com.google.android.gms/databases/reminders.db	Application, User and Location traces
Data	/com.android.providers.settings/*	Great place for username and passwords
Data	/system/*.key	Files needed for password cracking
Data	/system/device_policies.xml	Password requirements and policies.
Data	/system.SimCard.dat	Sim card and phone number information

Rooted Android Devices		
Partition	File	Description
Data	/system/accounts*.db	User account information
Data	/com.google.android.gm/databases/<mail-name>.db	Gmail snippets
Data	/com.android.email/databases/EmailProvider.db	Email artifacts
Data	/com.google.android.gms/databases/herrevad	Wireless and MAC addresses
Data	/system/locksettings.db and locksettings.db-WAL	Lock settings information
Data	/com.android.providers.media/external*.db and external*.db-WAL	Traces to SD card
Data	/com.android.vending/databases/localappstate.db	Application traces
Data	/com.google.android.locations/files/cache.cell /com.google.android.locations/files/cache.wifi	Cellular and WiFi
Data	/com.samsung.android.providers.context.databases.ContextLog_0.db (OS 7)	Application traces for Samsung devices
Data	/com.google.android.gms/databases/NetworkUsage.db /com.google.android.gms/databases/ns.db /com.google.android.gms/databases/reminders.db	Application, User and Location traces
Data	/system/packages.xml /system/packages.list /system/metpolicy.xml	Application permissions
Data	/system/usagestats/0/*various directories*.xml	Application Usage
Data	/system/batterystats.bin /system/batterystats-daily.xml /system/batterystats-checkin.bin	Application Usage (may be difficult to parse)
Data	/com.sec.android.app.launcher/databases/launcher.db /com.android.providers.downloads/databases/downloads.db	Application artifacts (even after deleted)
Data	/system/dmappmgr.db	Application Usage
Data	/com.android.providers.settings/*	Great place for username and passwords
Data	/data/*	Application directories include more data
Data	/system/recent_images/*.png	Application snapshots may exist here

FOR585: Advanced Smartphone Forensics

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!"

**SMARTPHONE DATA CAN'T HIDE FOREVER –
IT'S TIME TO OUTSMART THE MOBILE DEVICE!**

Jailbroken iOS Devices	
Database	Description
/Library/CoreDuel/*	Device lock state (1=Locked, 0=Unlocked)
/Library/AggregateDictionary/ADDataStore.sqlite	Dictionary
/Library/BatteryLife/CurrentPowerLog.PLSQL	Battery life tracker, Application traces
/private/var/network/rltusage.sqlite	Network artifacts
/Library/Health/Healthdb.sqlite	Activity, Personal information, more
/Library/Health/Healthdb_secure.sqlite	
/Library/Caches/com.apple.routined/cache_encrypted*.db	Frequent Locations (https://github.com/mac4n6/iOS-Frequent-Locations-Dumper)
/Library/Caches/com.apple.routined/StateModel*.archive	
/Library/Caches/cache_encrypted*.db	Cell and WiFi locations
/Library/Caches/lockCache_encrypted*.db	
/Applications/*	Examine relevant app directories to obtain additional data
/Library/BulletinBoard/ClearedSections.plist	Logs of cleared notifications
/Library/Keyboard/UserDictionary.sqlite	User created auto-correct
/Library/Accounts/Accounts3.sqlite	Accounts, user information, etc.
/Library/Databases/CellularUsage.db	SIMs used in device, including most recent
/Library/TCC/TCC.db	Applications permissions
/Library/Databases/Datausage.sqlite	Application traces
/Library/com.apple.itunesstored/itunesstored2.sqlite	Application traces
plist	
/Lockdown/device_values.plist	Activated state, BT address and more
/Preferences/com.apple.homesharing.plist	iCloud account information
/Preferences/com.apple.assistant.backedup.plist	Cloud sync settings
/Preferences/com.apple.coreduel.plist	Sync devices
com.apple.commcenter.plist	Device phone number, Network carrier, ICCIDs and IMSIs
com.apple.identityservices.idstustcache.plist	iCloud sync, Email, FaceTime, Email, more
com.apple.accounts.plist	Email accounts pushed to device
com.apple.Maps.plist	Last latitude and longitude, map search history
/Library/Maps/Bookmarks.plist	Maps bookmarks
com.apple.Maps/Maps	History.mapsdata (iOS 7)
com.apple.MobileBluetooth.devices.plist	GeoHistory.mapsdata (iOS 8 - iOS 11) *Pull cloud if possible
CloudConfigurationDetails.plist	Synced devices
/SystemConfiguration/com.apple.wifi.plist	Cloud configurations
/SystemConfiguration/preferences.plist	WiFi
/Library/DataAccess/AccountInformation.plist	WiFi and more
/Library/DataAccess/iCloud-[iCloud email account name]*	Email sync data
Files of Interest	
/Library/Preferences/*	Examine plist for more information
/Library/DataAccess	Account information used to set up apps (Email, #, etc)
/var/mobile/Library/Keyboard	dynamic-text.dat

iOS Devices	
Database	Description
Library/CallHistory/call_history.db	Call logs
Library/CallHistory/DB/CallHistory.storedata	Call record (iOS 8 - iOS 10)
Library/AddressBook/AddressBook.sqlite	Contacts
Library/AddressBook/AddressBookImages.sqlite	Contact images
Library/SMS/sms.db	SMS messages
Library/SMS/Attachments/*	MMS file
Library/Calendar/Calendar.sqlite	Calendar
Library/Notes/notes.sqlite	Notes
Library/Safari/*	Safari activity
Library/Accounts/Accounts3.sqlite	Account information
Library/BulletinBoard/ClearedSections.plist	Logs of cleared notifications
Media/PhotoData/Photos.sqlite	Metadata about multimedia files
Library/TCC/TCC.db	Application permissions
Library/Databases/DataUsage.sqlite	Application information and usage details
Library/ADDataStore.sqlite	iOS unlock data repository (Refer to mac4n6.com)
Library/CoreDuel/coreduel.db	unlock data repository (Refer to mac4n6.com)
plist	
com.apple.commcenter.plist	Device phone number, network carrier, ICCIDs, and IMSIs
com.apple.accounts.plist	Email accounts pushed to device
com.apple.Maps.plist	Last latitude and longitude, map search history
Library/Maps/Bookmarks.plist	Maps bookmarks
com.apple.Maps/Maps	History.mapsdata (iOS 7)
com.apple.Maps/Maps	GeoHistory.mapsdata (iOS 8 - iOS 10)
SystemConfiguration/com.apple.wifi.plist	WiFi
SystemConfiguration/preferences.plist	WiFi and more
Library/Preferences/com.apple.mobilenotes.plist	Notes
Library/SpringBoard/IconState.plist	Homescreen icon layout
Library/ConfigurationProfiles/UserSettings.plist	User-created restrictions
Library/Preferences/com.apple.springboard.plist	User-created restrictions
Library/Preferences/com.apple.WebFoundation.plist	Safari activity
Library/Preferences/com.apple.MobileSMS.plist	SMS, iMessage and FaceTime
Library/Preferences/com.apple.madrid.plist	SMS, iMessage and FaceTime
Library/DataAccess/AccountInformation.plist	Email sync data
Library/DataAccess/iCloud-[iCloud email account name]/.mboxCache.plist	iCloud email account information
Library/DataAccess/iCloud-[iCloud email account name]/.OfflineCache/number*	iCloud offline cache