Evidence per

Operating System & Device In-Depth



Battlefield Forensics



Analysis

FOR526

@sansforensics



Mac and iOS

Forensic Analysis and Incident Response



Incident Response

& Threat Hunting



GCTI



FOR610









Analysis In-Depth







for585.com/poster

FOR585: for585.com/course

The Most Relevant

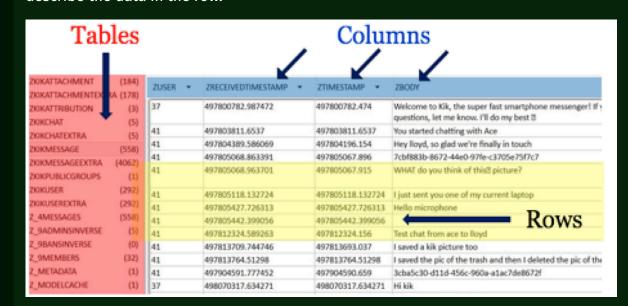
Gigabyte

Smartphone Forensic Analysis In-Depth

DFPS_FOR585_v3.1_0420

SQLite Database Basics

SQLite databases are a self-contained database stored as a file system file (but may have a few supporting files that will also be needed for analysis!) Files have the magic number "SQLite format 3." SQLite files correspond to a database that contains tables. Tables contain rows of data with corresponding columns that describe the data in the row.



Some temporary files may also be created, including Journal files and Write Ahead Logs. Journal files store original data before a transaction change so the database can be restored to a known state if an error occurs. They are created by default.

Write Ahead Logs (WAL) contain new data changes, leaving original database untouched. After a set number of page changes, the WAL is used to update the actual database. Write ahead logs are optional. Journal files – stores original data before a transaction change so the database can be restored to a known state if an error occurs (created by default).

SQLite

Timestamp Conversion Timestamps are stored in the databases as one of several numerical representations. (Timestamps are assumed to be stored in UTC, you may need to verify this.)

UNIX Epoch (10 digit number - number of seconds since 01/01/1970 00:00:00):

• SELECT datetime (TS COLUMN, 'unixepoch') Or in **local time** as suggested by the device settings (this can be done for all the following timestamps):

• SELECT datetime(TS COLUMN, 'unixepoch', 'localtime')

UNIX Epoch MILLISECONDS (13 digit number – number of milliseconds since 01/01/1970 00:00:00):

• SELECT datetime(TS_COLUMN/1000, 'unixepoch');

Mac Absolute time, number of seconds since 01/01/2001 00:00:00. In order to correctly convert this timestamp, first, add the number of seconds since UNIXEPOCH time to Mac Absolute Time (978307200), then convert.

• SELECT datetime (TS COLUMN + 978307200, 'unixepoch');

Chrome time accounts for time accurate to the MICROSECOND, which requires dividing

• SELECT datetime(TS COLUMN/1000000 + (strftime('%s','1601-01-01')),'UNIXEPOCH');

Basic Analysis Query Structure

Get everything from a single table: SELECT * FROM A TABLE;

Get two columns from a single table: SELECT COLUMN A, COLUMN B FROM A TABLE;

Table Joins

Taking data from two (or more!) tables that have a column in common and joining them into one table. Identify tables of interest that contain unique values. **LEFT JOIN** – Resulting rows are returned from the **LEFT** table even if there are no matches in the right. Using the **LEFT JOIN** returns all the text messages, including those with and without attachments.

SELECT ZVIBERMESSAGE.ZTEXT AS "Message Text", ZATTACHMENT.ZNAME AS "Attachment Filename", datetime(ZVIBERMESSAGE.ZDATE+978307200, 'unixepoch', 'localtime') AS "Message Date", ZVIBERMESSAGE. ZSTATE AS "Message Direction/State" FROM ZVIBERMESSAGE LEFT JOIN ZATTACHMENT on ZATTACHMENT.Z PK=ZVIBERMESSAGE.ZATTACHMENT

INNER JOIN – Resulting rows are returned when both items are a match. Using the **INNER JOIN** (also achieved by typing "**JOIN**" in the query) returned just the messages that included attachments.

Useful Stuff

Column Renaming:

A_TABLE.ZAWKWARDCOLUMNNAME AS "Chat Messages"

SELECT COUNT(*) FROM A TABLE;

Aggregating with GROUP BY and COUNT (Count chat messages per contact): SELECT MESSAGES, COUNT(*) FROM CHAT GROUP BY CONTACT;

Sorting with ORDER BY:

SELECT * FROM CHAT ORDER BY A TIMESTAMP ASC ASC = Ascending DESC = Descending

Searching with WHERE and LIKE:

SELECT CONTACT, MESSAGE FROM CHAT WHERE CONTACT LIKE '%Hank%'

Practitioners/Researchers Sarah Edwards https://www.mac4n6.com Heather Mahalik https://smarterforensics.com http://mattiaep.blogspot.com Mattia Epifani Adrian Leong Alexis Brignoni Jon B Mari DeGrazia Andrew Hoog

Ian Whiffin

Josh Hickman

http://cheeky4n6monkey.blogspot.com https://abrignoni.blogspot.com https://www.ciofecaforensics.com http://az4n6.blogspot.com https://www.hack42labs.com http://doubleblak.com/blogs.php https://thebinaryhick.blog

Vendors

Cellebrite BlackBag Technologies Sanderson Forensics

Elcomsoft

Oxygen Forensics https://blog.oxygen-forensic.com Magnet Forensics https://www.magnetforensics.com/blog https://www.cellebrite.com/en/blog

https://www.blackbagtech.com/blog https://sqliteforensictoolkit.com/ support-articles

Our Favorite Mobile Forensic Resources

Additional Resources DFRWS

https://dfrws.org/ iOS Jailbreaks https://www.theiphonewiki.com/wiki/Jailbreak

FOR585 Google *access granted to all 585 Alumni

DFIR mailing list DFIR@lists.sans.org

Mobile Malware and Spyware

play-services-auth-api-phone.properties

Signature-Based

Specification-Based

play-services-auth-base.properties

play-services-basement.properties

play-services-auth.properties

play-services-base.properties

play-services-drive.properties

play-services-gcm.properties play-services-iid.properties

https://blog.elcomsoft.com

Key Artifacts: Static Analysis

Requested Permissions: Granted to an application by the user (1) during installation or (2) upon execution/runtime. Found in the AndroidManifest.xml file.

through the User Interface (UI). **Services:** Tasks often running in the background and integrated into the application. User doesn't (normally) interact with

Services. Examples: music playing during a gaming application, or calculations performed in the background. **Broadcast Receivers:** Facilitates the exchange of information for applications, which can be delivered between app

components or between entirely different applications.

then delivered to the broadcast receivers using Intents. **Content Providers:** Refers to how information is stored within an application and shared between multiple applications. Example: a contact database often used by many native and third-party applications. The code would call the ContentResolver (the global instance that provides access to the content) that passes on the request to the

📤 jadx-gui - evernote.apk File View Navigation Tools Help Resources ⊞ 🏣 META-INF **Activities:** One or more activities comprise each application. ii assets Users can navigate to/from and interact with activities directly classes.dex classes2.dex firebase-abt.properties firebase-analytics-impl.properties firebase-analytics.properties firebase-appindexing.properties firebase-common.properties firebase-config.properties firebase-core.properties firebase-iid-interop.properties firebase-iid.properties firebase-measurement-connector-impl.properties firebase-measurement-connector.properties Applications can be programmed to "listen" for events that are okhttp3 play-services-ads-identifier.properties play-services-analytics-impl.properties play-services-analytics.properties play-services-audience.properties

↑ AndroidManifest.xml 💥 xml version="1.0" encoding="utf-8"?> manifest xmlns:android="http://schemas.android.com/apk/res/android" xmlns:app="http://schem <uses-sdk android:minSdkVersion="23" android:targetSdkVersion="28"/> <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/> <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/> <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/> <uses-permission android:name="android.permission.GET_ACCOUNTS"/> <uses-permission android:name="android.permission.INTERNET"/> <uses-permission android:name="android.permission.READ_SYNC_SETTINGS"/> <uses-permission android:name="android.permission.READ_SYNC_STATS"/> <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/> <uses-permission android:name="android.permission.USE_BIOMETRIC"/> <uses-permission android:name="android.permission.VIBRATE"/> <uses-permission android:name="android.permission.WAKE_LOCK"/> <uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS"/> <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/> <uses-permission android:name="android.permission.USE_FINGERPRINT"/p</p> <uses-permission android:name="android.permission.READ_CALENDAR"/> <uses-permission android:name="android.permission.CAMERA"/> <uses-permission android:name="android.permission.READ_CONTACTS"/> <uses-permission android:name="android.permission.MANAGE_ACCOUNTS"/> <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/> <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/> <uses-permission android:name="android.permission.RECORD_AUDIO"/> <uses-permission android:name="android.permission.READ_PHONE_STATE"/> <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/> <uses-permission android:name="com android vending BILLING"/> <uses-permission android:name="android.permission.USE_CREDENTIALS"/> <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/> <uses-permission android:name="com.sonvmobile.permission.CAMERA_ADDON"/

Mobile Malware Detection

Mobile Malware

Behavioral-Based

Data Mining

Cloud-Based

Common Signs and Symptoms

- for mobile malware infection
- Poor battery life

Sandboxes

proper Content Provider.

- Dropped calls and call disruptions • Unusually large phone bills
- Data plan spikes Device performance problems Unexplained application errors
- Android devices are most at risk
 Unexpected device behaviors - Unplanned reboots
 - Apps that close or open on their own - Unexplained settings changes
 - High-risk user behavior - Risky downloads, browsing or link-clicking
 - Spyware: Device was out of owner's control - Spyware installation requires possession of the device

Online Mobile Malware

Upload suspicious .apk files to the Internet for online sandbox analysis:

- https://www.joesandbox.com/
- https://amaaas.com/ https://github.com/pjlantz/droidbox

- Dex2Jar
- *Virtual machine environments for mobile malware analysis: Santoku

Local Static Malware Analysis Tools installed on the local machine for mobile malware analysis:

- Android SDK
- Dexter • JD-GUI

Malware action— do families behave **Bit Defender/** What activity is App store approach, dynamic analysis arching for patterns considered normal **Check installed Check downloads** Establish a folder(s) for applications for suspicious timeline application files suspicious files **Beyond Scanning for Check browser** Research error **Malware with Forensic** messages/notifications history for visits to for clues about infection suspicious sites and AV Tools **Examine other activity on** Check for links from phone around the SMS. MMS. and email suspected time of infection



Logs-Parser iOS Triage https://github.com/ahoog42/ios-triage Incident response tool for iOS devices Converts plist files to json, https://www.hack42labs.com/tools/fplist/details/ dot notation or csv iOS_sysdiagnose_ Scripts for parsing various iOS https://github.com/cheeky4n6monkey/iOS_ forensic_scripts sysdiagnose logs sysdiagnose_forensic_scripts

Parser for Android Usagestats files in Android Usagestats XML + xml or protobuf format Protobuf Parser Identifies, hashes and destructures all files recursively from any file system Extracts apk files from an **FAPK** Android device

Android Logs Events & Protobuf Parser

https://www.hack42labs.com/tools/ftree/details/ https://www.hack42labs.com/tools/fapk/

DFIR-SQL-SQLite-Deleted-Records-Parser SQLECmd sqlite_miner

4n6-scripts

fplist

ALEAPP

for digital forensics use by platform and application Recovers deleted entries from Automates the identification and processing of sqlite database files Mines SQLite databases for BLOBs and potential unparsed content of interest Collection of forensic and third-party scripts https://github.com/cheeky4n6monkey/4n6-scripts

Collection of SQL query templates https://github.com/abrignoni/DFIR-SQL-Query-Repo https://github.com/mdegrazia/SQLite-Deleted-

https://github.com/abrignoni/ALEAPP

Android-Usagestats-XML-Protobuf

https://github.com/abrignoni/

https://github.com/EricZimmerman/SQLECmd https://github.com/threeplanetssoftware/

Android Extraction Encryption Type? Full Disk Encryption File-Based Encryption In which state did the Is secure startup No Yes Cold Hot or Cold? **TO** Ÿ **TO** Device is in a live **Brute force is** decrypted state, Cold Device is in a live encryption keys are in memory, no brute encryption keys are force is needed in memory, no brute force is needed **Brute force is** Device is in a live decrypted state. needed encryption keys are in memory, no brute Graphic courtesy of Cellebrite

Poster Authors Heather Mahalik Domenica "Lee" Crognale hmahalik@gmail.com @heathermahalik @domenicacrognal

Mattia Epifani domenica.crognale@gmail.com mattia.epifani@realitynet.it @mattiaep

©2020 Heather Mahalik, Domenica "Lee" Crognale, and Mattia Epifani. All Rights Reserved.

iOS Cheatsheet

Path DEVICE INFORMATION	Description B	FU Backup Sysdiagnose	Path ADDI ICATION LICACE	Description BFU Backup Sysdiagnos
DEVICE INFORMATION /private/var/installd/Library/MobileInstallation/LastBuildInfo.plist /private/var/mobile/Library/CoreDuet/coreduetd.db	Operating system version Lock/Device Passcode Info (0=unlocked, 1=locked) (Up to iOS 9) N	Y N I N N	APPLICATION USAGE /private/var/installd/Library/Logs/MobileInstallation/mobile_installation.log.* /private/var/containers/Shared/SystemGroup/sGIJID>/Library/BatteryLife/CurrentPowerLog PL	Mobile Applications Installation Logs Y N Y SQL Battery life tracker N N Y
/private/var/mobile/Library/Logs/mobileactivationd/ /private/var/mobile/Library/Preferences/com.apple.AdLib.plist	MobileActivation Logs Y May show older iOS versions used Y Last BootTime Y	N Y N	/private/var/installd/Library/Logs/MobileInstallation/mobile_installation.log.* /private/var/containers/Shared/SystemGroup/ <guid>/Library/BatteryLife/CurrentPowerLog.PL /private/var/mobile/Library/AggregatedDictionary/ADDataStore.sqlitedb /private/var/mobile/Library/AppConduit/AvailableApps.plist</guid>	Application tracker N N Y Application traces Y N N Installed Apps and Apps Path Y N N
/private/var/mobile/Library/Preferences/com.apple.aggregated.plist /private/var/mobile/Library/Preferences/com.apple.mmcs.plist /private/var/mobile/Library/Preferences/com.apple.mobilegestalt.plist	IMSIs Y Device name Y	Y N Y N		
/private/var/mobile/Library/Preferences/com.apple.minics.ptist /private/var/mobile/Library/Preferences/com.apple.mobilegestalt.plist /private/var/mobile/Library/Preferences/com.apple.preferences.datetime.plist /private/var/mobile/Library/Preferences/com.apple.preferences.plist /private/var/mobile/Library/Preferences/com.apple.preferences.plist /private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist	Time settings Y Airplane mode (on/off) Y Disk usage Y	Y N Y N Y N	/private/var/mobile/Library/AppConduit/AvailableCompanionApps.pust /private/var/mobile/Library/Application Support/com.apple.remotemanagmentd/RMAdminSto /private/var/mobile/Library/ApplicationSync/AssetSortOrder.plist /private/var/mobile/Library/Assistant/knowledgeC.db /private/var/mobile/Library/com.apple.itunesstored/itunesstored2.sqlitedb /private/var/mobile/Library/com.apple.itunesstored/kvs.sqlitedb /private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db /private/var/mobile/Library/CoreDuet/People/interactionC.db /private/var/mobile/Library/CoreDuet/People/interactionC.db	Application traces N N N Application traces Y Y N Installed Applications Y Y N
/private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist /private/var/mobile/Library/Preferences/com.apple.timed.plist /private/var/preferences/SystemConfiguration/com.apple.petworkidentification.plist	Language, Country info, Device IDS Auto Time and Auto Time Zone settings Yetwork IP, WiFi, Cellular Information Y	Y N Y N	/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db /private/var/mobile/Library/CoreDuet/People/interaction.db	Application traces N N N Application traces N Y N
/private/var/mobile/Library/Preferences/com.apple.timed.plist /private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist /private/var/preferences/SystemConfiguration/com.apple.radios.plist /private/var/preferences/SystemConfiguration/com.apple.radios.plist /private/var/preferences/SystemConfiguration/verfurences.plist	Airplane mode (on/off) Y Wi-Fi Mac Addresses Y	Y N N Y	/private/var/mobile/Library/FrontBoard/applicationState.db /private/var/mobile/Library/Health/ActivitySharing/contacts2.dat /private/var/mobile/Library/Keyboard/langlikelihood.dat	Fitness Friends N N N Application traces Y Y N
/private/var/preferences/SystemConfiguration/preferences.plist /private/var/root/Library/Lockdown/escrow_records/	Network and VPN information Y Computer Trust/Pair certificates Y Computer Trust/Pair certificates Y	Y N N N N N	/private/var/mobile/Library/FrontBoard/applicationState.db /private/var/mobile/Library/Health/ActivitySharing/contacts2.dat /private/var/mobile/Library/Keyboard/langlikelihood.dat /private/var/mobile/Library/logs/AppConduit/ /private/var/mobile/Library/Logs/Mobile_installation_helper.log* /private/var/mobile/Library/Preferences/addaily.plist	Step/Stride Cadence, Pedometer Info N Y N Installed Apps and Apps Path Y N Y Application traces N Y N
/private/var/root/Library/Lockdown/pair_records/ /private/var/root/Library/Preferences/com.apple.preferences.network.plist /private/var/wireless/Library/Preferences/com.apple.commcenter.plist	Airplane mode (on/off) Device Info (IMEI, Phone Number, Network Carrier, ICCIDs, IMSIs, etc.)	Y N Y N	/private/var/mobile/Library/references/addaily.plist /private/var/containers/Shared/SystemGroup/ <guid>/Library/Logs/mobile_installation_helpe</guid>	Application traces V V N
PASSWORDS AND ACCOUNT INFORMATION /private/var/mobile/Library/Accounts/Accounts3.sqlite	Account information Y	Y N	/private/var/mobile/Library/Preferences/addany.ptist /private/var/containers/Shared/SystemGroup/ <guid>/Library/Logs/mobile_installation_helpe /private/var/mobile/Library/Preferences/com.apple.ActivitySharing.plist /private/var/mobile/Library/preferences/com.apple.AppStore.plist /private/var/mobile/Library/Preferences/com.apple.corespotlightui.plist /private/var/mobile/Library/TCC/TCC.db</guid>	Information about Fitness Friends Y Y N Last search on Apple Store Y Y N Application traces Y Y N
/private/var/mobile/Library/DataAccoss/	Account information used to set up apps (Email, #, etc) Email sync data iCloud Email account information Y	Y N Y N	/private/var/mobile/Library/TCC/TCC.db /private/var/networkd/netusage.sqlite /private/var/sqt/Library/Coches/Jecationd/clients-pliet	Network data usage per App N N N
/private/var/mobile/Library/DataAccess/AccountInformation.plist /private/var/mobile/Library/DataAccess/iCloud-[iCloud email account name]/.mboxCache.plist /private/var/mobile/Library/Health/healthdb.sqlite /private/var/mobile/Library/Health/lbalthdb_secure.sqlite /private/var/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/DeltaAccenters/mobile/Library/Medicall/Medicall/DeltaAccenters/mobile/Library/Medicall/Medicall/DeltaAccenters/mobile/Library/Medicall/Me	Health data, personal data, iOS version info, etc. Health data, personal data, iOS version info, etc. Medical Information (bloodtype, organ donor, name, DOB, etc.) N	I Y N	/private/var/networkd/netusage.sqlite /private/var/root/Library/Caches/locationd/clients.plist /private/var/root/Library/Logs/MobileContainerManager /private/var/root/Library/MobileContainerManager/containers.sqlite3	Application traces Y Y N MobileContainerManager logs Y N Y Installed Applications Y N N
/private/var/monite/Library/Preferences/com.apple.accountsettings.piist	Medical Information (bloodtype, organ donor, name, DOB, etc.) Email accounts pushed to device Blocked Dialers Y	I Y N Y N Y N	/private/var/wireless/Library/Databases/DataUsage.sqlite	Application traces Y N N
/private/var/mobile/Library/Preferences/com.apple.commcenter.shared.plist /private/var/mobile/Library/Preferences/com.apple.comference.plist /private/var/mobile/Library/Preferences/com.apple.contacts.donation-agent.plist /private/var/mobile/Library/Preferences/com.apple.contextstored.plist /private/var/mobile/Library/Preferences/com.apple.coreduetd.plist /private/var/mobile/Library/Preferences/com.apple.coreduetd.plist	Phone number Y Facetime phone number in use, SMS phone number, user accounts Y Last Metrics Attempts (usage information)	Y N Y N	Andraid Chast	ah a a t
/private/var/mobile/Library/Preferences/com.apple.contacts.donation-agent.plist /private/var/mobile/Library/Preferences/com.apple.contextstored.plist /private/var/mobile/Library/Preferences/com.apple.coreduetd.plist	Activity throttling Y Activity throttling Y	Y N Y N Y N	Android Cheats	sneet
/private/var/mobile/Library/Preferences/com.apple.corerecents.recentsd.plist /private/var/mobile/Library/Preferences/com.apple.FeedbackAssistant.plist /private/var/mobile/Library/Preferences/com.apple.homesharing.plist /private/var/mobile/Library/Preferences/com.apple.icloud.findmydeviced.FMIPAccounts.plist /private/var/mobile/Library/UserConfigurationProfiles/	iCloud login information Y Last successful email address used to login to cloud Y iCloud account information Y	Y N Y N	Partition Path	Tables of Interest Description
/private/var/mobile/Library/Preferences/com.apple.icloud.findmydeviced.FMIPAccounts.plist /private/var/mobile/Library/UserConfigurationProfiles/	Find My iPhone settings Y Profiles and restrictions Y	Y N Y N	DEVICE INFORMATION System /build.prop	N/A Device information (version, patches, etc.)
/private/var/preferences/SystemConfiguration/com.apple.accounts.exists.plist /private/var/root/Library/Lockdown/data_ark.plist /private/var/wireless/Library/preferences/com.apple.commcenter.callservices.plist	Account information Y Last backup computer, iCloud Backup Settings, Device info Y Last iCloud account Y	Y N N N N N	Userdata /data/com.android.providers.calendar/databases/calendar.db Userdata /data/com.android.providers.settings/databases/settings.db Userdata /data/com.android.providers.settings/databases/settings.db-WAL	* Calendar Items and Timezone information * Lock settings information * Lock settings information
SETTINGS – SYSTEM CONTROLLED – KEYBOARDS, DICTIONARY, LOG			Userdata /data/com.android.providers.settings/databases/locksettings.db Userdata /data/com.android.providers.settings/databases/locksettings.db-WAL Userdata /data/com.google.android.gms/shared_prefs/Checkin.xml	* Lock settings information * Lock settings information N/A Activity on device related to installed SIM
/private/installd/Library/Logs/MobileInstallation/mobile_installation.log.* /private/var/mobile/Containers/ /private/var/mobile/Library/BulletinBoard/ClearedSections.plist	Mobile Applications Installation Logs Y Application Folders Y Logs of cleared notifications Y	Y N Y N Y Y N Y N	Userdata /data/com.google.android.gsf/databases/gservices.db	(ICCIĎ and Google Account included) * Fitness settings, network settings, other settings
/private/var/mobile/Library/Keyboard/ <language>-dynamic.lm/dynamic-lexicon.dat /private/var/mobile/Library/Preferences/ /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist</language>	Auto correction / Predictive text Examine plists for more information Wi-Fi Mac Addresses Y	I N N	Userdata /misc/ Userdata /Property/persist.sys.timezone Userdata /Property/persistent_properties	N/A Bluetooth, VPN, Wi-Fi and more N/A Timezone (Up to Android 8) N/A Timezone (From Android 9)
SETTINGS – USER CONTROLLED – SYNC SETTINGS, SPRINGBOARD, I		N Y	Userdata /system/*.key Userdata /system/device_policies.xml Userdata /system/locksettings.db	N/A Files needed for password cracking N/A Passcode requirements and policies. Syncing info may exist * Lock settings information
/private/var/containers/Shared/SystemGroup/systemgroup.com.apple.configurationprofiles/Library/ ConfigurationProfilesCloudConfigurationDetails.plist	Cloud configurations	I N N	Userdata /system/locksettings.db-WAL Userdata /system/netpolicy.xml	* Lock settings information N/A Timezone
/private/var/mobile/Library/DoNotDisturb/DB/Settings.json /private/var/mobile/Library/Keyboard/UserDictionary.sqlite /private/var/mobile/Library/Mail/	Do not disturb settings Y User created auto-correct N Mail and settings N	Y N I N N I N N	Userdata /system/SimCard.dat Userdata /system/users/0/settings_global.xml Userdata /system/users/0/settings_secure.xml	N/A Sim card and phone number information N/A Global settings N/A Secure settings
/private/var/mobile/Library/Preferences/com.apple.assistant* /private/var/mobile/Library/Preferences/com.apple.assistant.backedup.plist	Siri Y Cloud sync settings Y	Y N Y N	Userdata /system/users/0/settings_secure.xml PASSWORDS AND ACCOUNT INFORMATION	N/A System settings
/private/var/mobile/Library/Preferences/com.apple.camera.plist /private/var/mobile/Library/Preferences/com.apple.celestial.plist /private/var/mobile/Library/Preferences/com.apple.cloudphotod.plist	Camera settings Y Camera, CarPlay, Volumes and other settings Y Cloud photo sync information Y	Y N Y N Y N	Userdata /data/com.android.email/databases/EmailProvider.db	Account, Email Email accounts, 3rd party app data, and messages associated with Email AddressCache, notifications, Email accounts, 3rd party app data, and messages
/private/var/mobile/Library/Preferences/com.apple.CoreDuet.plist /private/var/mobile/Library/Preferences/com.apple.imservice* /private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist	Cloud sync settings Y SMS, iMessage and FaceTime Y Time to keep messages Y	Y N Y N Y N	Usordata /data/som android providers control / 1 / 1	Mailbox* associated with Email notifications
/private/var/mobile/Library/Preferences/com.apple.mobilesms.plist /private/var/mobile/Library/Preferences/com.apple.preferences.network.plist /private/var/mobile/Library/Preferences/com.apple.springboard.plist /private/var/mobile/Library/Preferences/com.apple.weather.plist	Airplane Mode Settings Y User created restrictions/Remote wipe settings Y	Y N Y N	Userdata /data/com.android.providers.contacts/databases/contacts2.db Userdata /data/com.android.providers.settings/* Userdata /data/com.android.vending/shared_prefs/lastaccount.xml	accounts Login info N/A Username and passwords N/A Last account used on Google PlayStore (Android 9 and above)
/private/var/mobile/Library/Preferences/com.apple.weather.plist /private/var/mobile/Library/SpringBoard/HomeBackground.cpbitmap /private/var/mobile/Library/SpringBoard/HomeBackgroundThumbnail.jpg /private/var/mobile/Library/SpringBoard/IconState.plist	Weather (including current city) Wallpaper Wallpaper Y	Y N Y N Y N	Userdata /data/com.google.android.gms/shared_prefs/BackupAccount.xml Userdata /data/com.google.android.googlequicksearchbox/databases/app_icons.db Userdata /data/com.google.android.googlequicksearchbox/databases/launcher.db Userdata /data/com.google.android.googlequicksearchbox/databases/opa_history	N/A Backup account email address * Google Account Information * Google Account Information
/private/var/mobile/Library/SpringBoard/IconState.plist /private/var/mobile/Library/SpringBoard/LockBackground.cpbitmap	Homescreen icon layout Y Wallpaper Y	Y N Y N	Userdata /data/com.google.android.gst/databases/gservices.db	* Google Account Information * Fitness settings, network settings, other settings
/private/var/mobile/Library/SpringBoard/LockBackground.cpbitmap /private/var/mobile/Library/SpringBoard/LockBackgroundThumbnail.jpg /private/var/mobile/Library/SpringBoard/LockBackgroundThumbnaildark.jpg /private/var/mobile/Library/SpringBoard/PushStore/ /private/var/mobile/Library/UserConfigurationProfiles/UserSettings.plist	Wallpaper Y Wallpaper Y Notifications N	Y N Y N I N N	Userdata /system_ce/0/accounts_ce.db Userdata /system_de/0/accounts_de.db Userdata /misc/wifi/softap.conf	* Additional accounts (could also be system_de or accounts_de) * Additional accounts (could also be system_de or accounts_de) N/A Hotspot Passwords
/private/var/modile/Library/UserNotifications/	User Created restrictions User Notifications Y Last backup computer, iCloud Backup Settings, Device info Y	Y N Y N	Userdata /misc/wifi/wpa_supplicant.conf Userdata /system/accounts*.db	N/A Wi-Fi Network Password * User account information
/private/var/root/Library/Lockdown/data_ark.plist /private/var/root/Library/Preferences/com.apple.preferences.network.plist	Last backup computer, iCloud Backup Settings, Device info Airplane Mode Settings Y	Y N	Userdata /system/sync/accounts.xml Userdata /system/users/0/0.xml	N/A User account information N/A User information
COMMUNICATIONS – SMS, CALLS, EMAIL /private/var/mobile/Library/CallLhistory/call_history.db	Call log (Up to iOS 7)	I Y N	SYSTEM SETTINGS Userdata /data/com.google.android.gms/shared_prefs/*	N/A Preference files
/private/var/mobile/Library/CallHistoryDB/CallHistory.storedata /private/var/mobile/Library/CallHistoryDB/CallHistoryTemp.storedata /private/var/mobile/Library/Mail/	Call log (From iOS 8) N Call History Temporary storage (Before First Unlock) Y Mail and settings N	I Y N ' N N	Userdata /data/com.google.android.gsf/databases/gservices.db Userdata /system/recent_images/*.png Userdata /system_ce/recent_images/*.png	* Fitness settings, network settings, other settings N/A Application snapshots Application snapshots
/private/var/mobile/Library/Mail/ /private/var/mobile/Library/Preferences/com.apple.madrid.plist /private/var/mobile/Library/Preferences/com.apple.mobilephone:* /private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist	SMS, iMessage and FaceTime Y List of contacts added to the phone application's favorites list N	Y N I Y N	Userdata /system/users/0/settings_global.xml Userdata /system/users/0/settings_secure.xml	N/A Global settings N/A Secure Settings
/private/var/mobile/Library/Recents/	SMS, iMessage and FaceTime Y Recents communications N MMS File N	Y N I N N I Y N	Userdata /system/users/0/settings_system.xml USER SETTINGS	N/A System Settings
/private/var/mobile/Library/SMS/Attachments/* /private/var/mobile/Library/SMS/Drafts/* /private/var/mobile/Library/SMS/sms.db	SMS/MMS Drafts N SMS/MMS messages N	I Y N I Y N	Userdata /data/com.android.providers.calendar/databases/calendar.db Userdata /data/com.android.providers.userdictionary/databases/user_dict.db	* Calendar Items and Timezone information * Dictionary Files (Keylogging)
/private/var/mobile/Library/SMS/sms-temp.db /private/var/mobile/Library/Suggestions/query_predictions.db /private/var/mobile/Library/Voicemail/voicemail.db /private/var/mobile/Media/Recordings/*	SMS Temporary storage (Before First Unlock) Contains iMessage/SMS traces Voicemail Y	N N I N N	Userdata /data/com.google.android.gms/databases/NetworkUsage.db Userdata /data/com.google.android.gms/databases/ns.db Userdata /data/com.google.android.gms/databases/reminders.db	* Application, User and Location traces * Application, User and Location traces * Application, User and Location traces
/private/var/mobile/Media/Recordings/* BROWSER ACTIVITY	Voice Memos N	I Y N	Userdata /data/com.google.android.gsf/databases/googlesettings.db Userdata /data/com.google.android.gsf/databases/gservices.db Userdata /data/com.sec.android.inputmethod/Swiftkey/user/dynamic.lm	* Google preferences – location, maps, wallet, etc1=true * Fitness settings, network settings, other settings N/A Dictionary Files (Keylogging) SwiftKey folder name may vary
/private/var/mobile/Containers/Data/Application/ <apple <="" caches="" com.apple.mobilesafari="" guid="" library="" safari="" td=""><td>Safari Cache files N Safari Cache database N</td><td>I N N I N N</td><td>COMMUNICATIONS – SMS, CALLS, EMAILS</td><td>W/A Dictionally rites (Reylogging) swiftney lotter flame may vary</td></apple>	Safari Cache files N Safari Cache database N	I N N I N N	COMMUNICATIONS – SMS, CALLS, EMAILS	W/A Dictionally rites (Reylogging) swiftney lotter flame may vary
/private/var/mobile/Containers/Data/Application/ <apple applicationcache.d<br="" caches="" com.apple.webappcache="" guid="" library="" safari="">/private/var/mobile/Containers/Data/Application/<apple cookies="" cookies.binarycookies<="" guid="" library="" safari="" td=""><td>b Safari Website cache N Safari Cookies N</td><td>I N N</td><td>Cache * Userdata /data/com.android.providers.contacts/databases/calllog.db</td><td>* Gmail attachments, Downloads and Browser data calls Call logs (From Android 7)</td></apple></apple>	b Safari Website cache N Safari Cookies N	I N N	Cache * Userdata /data/com.android.providers.contacts/databases/calllog.db	* Gmail attachments, Downloads and Browser data calls Call logs (From Android 7)
/private/var/mobile/Containers/Data/Application/ <apple <="" <apple="" application="" com.apple.mobilesafari.plist="" containers="" data="" downloads="" downloads.plist="" favicons="" guid="" library="" mobile="" preferences="" private="" safari="" td="" thumbnails="" var=""><td>Safari Website favicons Safari Configuration Safari Download History N</td><td>I N N I Y N I Y N</td><td>Userdata /data/com.android.providers.contacts/databases/contacts2.db Userdata /data/com.android.providers.telephony/databases/mmssms.db Userdata /data/com.google.android.apps.messaging/databases/bugle_db Userdata /data/com.google.android.dialer/databases/dialer.db</td><td>calls Call logs (Up to Android 6) sms and part SMS/MMS * RCS/Android Messages (refer to notebook for query)</td></apple>	Safari Website favicons Safari Configuration Safari Download History N	I N N I Y N I Y N	Userdata /data/com.android.providers.contacts/databases/contacts2.db Userdata /data/com.android.providers.telephony/databases/mmssms.db Userdata /data/com.google.android.apps.messaging/databases/bugle_db Userdata /data/com.google.android.dialer/databases/dialer.db	calls Call logs (Up to Android 6) sms and part SMS/MMS * RCS/Android Messages (refer to notebook for query)
/private/var/mobile/Containers/Data/Application/ <apple <br="" guid="" library="" safari="" thumbnails="">/private/var/mobile/Containers/Data/Application/<apple *<br="" guid="" library="" localstorage="" safari="" webkit="" websitedata="">/private/var/mobile/Library/Assistant/knowledgeC.db</apple></apple>	Safari Tabs Screenshots (PNG or KTX format) Safari WebKit Localstorage Safari History information N	I Y N Y N	Userdata /data/com.google.android.dialer/databases/dialer.db Userdata /data/com.google.android.gm/databases/ <mail-name>.db</mail-name>	* Call logs conversations Gmail snippets and messages
/private/var/mobile/Library/Safari/Bookmarks.ob /private/var/mobile/Library/Safari/BrowserState.db	Safari Bookmarks N Safari Suspended State Tab N	I Y N I N N	Userdata /data/com.google.android.gm/databases/bigTopDataDB. <user-id>Userdata /data/com.google.android.gm/databases/EmailProvider.db</user-id>	Email information Email information
/private/var/mobile/Library/Safari/CloudTabs.db /private/var/mobile/Library/Safari/History.db	Safari Cloud Tabs N Safari History N	I N N I N N	Userdata /data/com.google.android.gms/databases/icing_mmssms.db Userdata /data/com.google.android.gms/databases/ipa_mmssms.db Userdata /data/com.sec.android.provider.logsprovider/databases/logs.db	* SMS/MMS * SMS/MMS logs Call logs
MULTIMEDIA *.ktx	Application Snapshots	I N N	MULTIMEDIA Userdata /data/com.android.providers.media/databases/external*.db	* Traces to SD card used in the device. This is stored on the phone.
/private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb /private/var/mobile/Library/Preferences/com.apple.mobileslideshow.plist /private/var/mobile/Library/SMS/Attachments/	Contacts pictures N Photos Y MMS File N	I Y N Y N I Y N	Userdata /data/com.android.providers.media/databases/external*.db-WAL Userdata /data/com.google.android.apps.photos/databases/gphotos0.db	* Traces to SD card used in the device. This is stored on the phone. Camera Photos information
/private/var/mobile/Media/DCIM/1*APPLE /private/var/mobile/Media/iTunes_Control/iTunes/MediaLibrary.sqlitedb /private/var/mobile/Media/PhotoData/*.ithmb	User Created/Saved Photos N iTunes Media Library Y Thumbnails databases N	Y N Y N	Userdata /data/com.samsung.cmh/databases/cmh.db Userdata /data/com.samsung.storyservice/databases/dme.db Userdata /data/com.samsung.visionprovider/databases/visionprovider.db	files Camera Photo - Samsung Devices info Camera Photo - Samsung Devices files Camera Photo - Samsung Devices
, private/var/mobile/Media/PhotoData/AlbumsMetadata/ /private/var/mobile/Media/PhotoData/CPL/	Photo Albums Metadata N Cloud Photo Library N	I Y N I Y N	Userdata /media/ BROWSER ACTIVITY	N/A Acts like SD card
/private/var/mobile/Media/PhotoData/Photos.sqlite /private/var/mobile/Media/PhotoData/V2/	Photos/Videos Database Photos saved from Live Video and SMS photo capture N	I Y N I Y N	Cache * Userdata /data/com.android.browser/app_databases/*	N/A Gmail attachments, Downloads and Browser data * Internet History
NETWORK CONNECTIONS /private/var/db/dhcpclient/leases/	DHCP Lease Y	, N N	Userdata /data/com.android.browser/app_geolocation/GeolocationPermissions.db Userdata /data/com.android.browser/databases/Browser.db	* Internet History
/private/var/mobile/Library/Preferences/com.apple.preferences.network.plist /private/var/networkd/netusage.sqlite	Airplane mode ON/OFF Y Network data usage per App N	Y N I N N	Userdata /data/com.android.browser/databases/browser2.db Userdata /data/com.android.browser/databases/webview.db Userdata /data/com.android.browser/databases/webviewCache.db	* Internet History * Internet History * Internet History
/private/var/preferences/com.apple.networkextension.plist /private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist /private/var/preferences/SystemConfiguration/com.apple.wifi.plist	Network Extension Y Network IP, Wi-Fi, Cellular Y Wi-Fi Y	Y N Y N Y Y	Userdata /data/com.android.email/webviewCache.db NETWORK CONNECTIONS	* Internet History
/private/var/preferences/SystemConfiguration/com.apple.wifi.plist /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist /private/var/preferences/SystemConfiguration/preferences.plist	Wi-Fi Mac Addresses Wi-Fi, VPN, Certs and more Y	N Y Y N	Userdata /data/com.android.connectivity.metrics/databases/events.db	completed_events_ USB, Bluetooth, NFC and other connects - Acquisition connection tracked he requests
/private/var/root/Library/Preferences/com.apple.preferences.network.plist /private/var/wireless/Library/Databases/CellularUsage.db /private/var/wireless/Library/Preferences/com.apple.CommCenter.counts.plist	Wi-Fi ON/OFF SIMs used in device, including most recent Pata and Cellular network statistics Y	Y N Y N	Userdata /data/com.google.android.gms/databases/herrevad Userdata /data/com.google.android.locations/files/cache.cell Userdata /data/com.google.android.locations/files/cache.wifi	* Wireless network and MAC addresses * Cellular and WiFi * Cellular and WiFi
/private/var/wireless/Library/Preferences/com.apple.commcenter.device_specific_nobackup.plist /private/var/wireless/Library/Preferences/com.apple.commcenter.plist	Device IMEI Y SIM Card ICCID Y	Y N Y N	Userdata /misc/wifi/WifiConfigStore.xml	N/A Wireless network
SYNCING ARTIFACTS /private/var/containers/Shared/SystemGroup/ <guid>/Library/Database/com.apple.MobileBluetooth.ledevices.other.db /private/var/containers/Shared/SystemGroup/<guid>/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db</guid></guid>	Seen Bluetooth devices	I Y N	SYNCING ARTIFACTS Userdata /data/com.google.android.apps.docs.editors.docs/databases/* Userdata /data/com.google.android.apps.docs.editors.sheets/databases/*	* Google Docs * Google Docs
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db /private/var/containers/Shared/SystemGroup/<guid>/Library/Preferences/com.apple.MobileBluetooth.devices.plist /private/var/mobile/Library/DataAccess/icloud-ficloud email.account.pamel/.OfflineCache/fourmberl</guid></guid>	Paired Bluetooth devices Y Paired Bluetooth devices N iClould offline cache Y	Y N I Y N Y N	Userdata /data/com.google.android.apps.docs.editors.slides/databases/* Userdata /data/com.google.android.apps.docs/databases/*	* Google Docs * Google Docs
/private/var/mobile/Library/DeviceRegistry.state/activeStateMachine.plist /private/var/mobile/Library/DeviceRegistry.state/historySecureProperties.plist	Apple Watch pairing information Apple Watch information (also previously paired Apple Watch) N	Y N I Y N	Userdata /data/com.google.android.apps.genie.geniewidget/databases/newsweather.db Userdata /data/com.google.android.gms/databases/peoplelog.db Userdata /data/com.google.android.gms/shared_prefs/com.google.android.gms.auth.	* Sync activity * Sync activity - contacts N/A Sync Activity
private/var/mobile/Library/DeviceRegistry.state/stateMacnine- <guid>.plist /private/var/mobile/Library/DeviceRegistry/<guid>/ /private/var/mobile/Library/DeviceRegistry/<guid>/NanoAppRegistry/Applications/</guid></guid></guid>	Apple Watch pairing information (also previously paired Apple Watch) N Apple Watch data Y Apple Watch Applications Y	Y N Y N Y N	authzen.cryptauth.SyncManager.proximity_features.xml Userdata /system/sync/accounts.xml	Synced Accounts
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Preferences/com.apple.MobileBluetooth.ledevices.paired.db /private/var/containers/Shared/SystemGroup/<guid>/Library/Preferences/com.apple.MobileBluetooth.devices.plist /private/var/mobile/Library/DataAccess/iCloud-[iCloud email account name]/.OfflineCache/[number] /private/var/mobile/Library/DeviceRegistry.state/activeStateMachine.plist /private/var/mobile/Library/DeviceRegistry.state/historySecureProperties.plist /private/var/mobile/Library/DeviceRegistry/state/stateMachine-<guid>.plist /private/var/mobile/Library/DeviceRegistry/<guid>/NanoAppRegistry/Applications/ /private/var/mobile/Library/DeviceRegistry/<guid>/NanoAppRegistry/Applications/ /private/var/mobile/Library/DeviceRegistry/<guid>/NanoPasses/nanopasses.sqlite3 /private/var/mobile/Library/DeviceRegistry/<guid>/NanoPreferencesSync/Backup/Files/ /private/var/mobile/Library/Health/NanoSync/com.apple.private.alloy.health.sync.db /private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.plist</guid></guid></guid></guid></guid></guid></guid>	Apple Watch Mail application Apple Watch Wallet Passes Apple Watch Faces Y	Y N I Y N	LOCATION ARTIFACTS Userdata /data/com.google.android.apps.maps/databases/da_destination_history	destination history Maps
/private/var/mobile/Library/Health/NanoSync/com.apple.private.alloy.health.sync.db /private/var/mobile/Library/homed/datastore.sqlite	AppleWatch Health data sync Apple HomeKit Devices N	I Y N I Y N	Userdata /data/com.google.android.apps.maps/databases/gmm_storage.db Userdata /data/com.google.android.apps.maps/databases/search_history.db	* Search history Maps history & suggestions Maps
/private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.plist /private/var/mobile/Library/NanoBackup/ /private/var/mobile/Library/NanoMusicSync/ /private/var/mobile/Library/NanoPreferencesSync/ /private/var/mobile/Library/NanoTimeKit/	Seen Bluetooth devices Y Apple Watch information Y Apple Watch information Y	Y N Y N N N	Userdata /data/com.google.android.apps.maps/databases/gmm_sync.db Userdata /data/com.sec.android.daemonapp/db/weatherClock Userdata /Media/0/DCIM/Camera	* Syncing * Location artifacts * EXIF data with location info
/private/var/mobile/Library/NanoPreferencesSync/ /private/var/mobile/Library/NanoTimeKit/	Apple Watch information Y Apple Watch information Y	N N N N	APPLICATION USAGE	
/private/var/mobile/Library/Preferences/com.apple.carplay.plist /private/var/mobile/Library/Preferences/com.apple.cloud.quota.plist /private/var/mobile/Library/Preferences/com.apple.CoreDuet.OueuedDenials.plist	Apple CarPlay configuration iCloud quota information Cloud Sync denials and dates Y	Y N Y N Y N	Userdata /app/* Userdata /dalvik-cache Userdata /data/"Application Folder"	N/A .dex/.oat/.art files for installed applications N/A Application Data Files*
/private/var/mobile/Library/Preferences/com.apple.coreduetd.plist /private/var/mobile/Library/Preferences/com.apple.identityservices.idstatuscache.plist /private/var/mobile/Library/Preferences/com.apple.mobile.ldbackup.plist	sync devices Y iCloud sync, Email, FaceTime, Email, more Y Last iTunes and last iCloud backup date and timezone. Y	Y N Y N Y N	Userdata /data/com.android.vending/databases/data_usage.db Userdata /data/com.android.vending/databases/frosting.db Userdata /data/com.android.vending/databases/install_queue.db	app_data_usage Application traces frosting Application traces install_requests Application traces
/nrivate/var/mobile/Library/Preferences/com apple nano* plist	Apple Watch preferences Y Device AirDrop ID Y	Y N Y N	Userdata /data/com.android.vending/databases/library.db Userdata /data/com.android.vending/databases/localappstate.db	ownership Application traces appstate Application traces
/private/var/mobile/Library/Preferences/com.apple.sharingd.plist /private/var/mobile/Library/Springboard/ <guid>-CarDisplay[Desired]IconState.plist /private/var/mobile/Media/iTunesControl/iTunes/iTunesPrefs /private/var/root/Library/Lockdown/data_ark.plist</guid>	Apple CarPlay per car App Icon configuration Y List of computer where the device was connected to Y Last backup computer, iCloud Backup Settings, Device info Y	Y N Y N N N	Userdata /data/com.android.vending/databases/notification_cache Userdata /data/com.android.vending/databases/package_verification.db Userdata /data/com.android.vending/databases/suggestions.db	notifications Application traces verification_cache Application traces suggestions Application traces
/private/var/wireless/Library/Databases/DataUsage-watch.sqlite	Watch Application Usage	I N N	Userdata /data/com.android.vending/databases/verify_apps.db Userdata /data/com.google.android.gms/databases/config.db Userdata /data/com.google.android.gms/databases/gass.db	* Application traces main Application traces app_info Application traces
LOCATION ARTIFACTS /private/var/containers/Shared/SystemGroup/ <guid>/Library/Database/com.apple.MobileBluetooth.ledevices.other.db /private/var/mobile/Containers/Data/Application/sApple_Mans_GUID>/Library/Mans/GeoHistory_mansdata</guid>	Seen Bluetooth devices N Apple Maps history N	I Y N	Userdata /data/com.google.android.gms/databases/gcm_registrar.db Userdata /data/com.google.android.gms/databases/google_app_measurement.db	packages Application traces * Application traces
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Database/com.apple.MobileBluetooth.ledevices.other.db /private/var/mobile/Containers/Data/Application/<apple_maps_guid>/Library/Maps/GeoHistory.mapsdata /private/var/mobile/Containers/Data/Application/<apple_maps_guid>/Library/Maps/History.mapsdata /private/var/mobile/Containers/Data/Application/<apple_maps_guid>/Library/Preferences/com.apple.Maps.plist</apple_maps_guid></apple_maps_guid></apple_maps_guid></guid>	Apple Maps history N Last latitude and longitude, map search history Y	I Y N Y N	Userdata /data/com.google.android.gms/shared_prefs/batterystats.xml Userdata /data/com.google.android.googlequicksearchbox/* Userdata /data/com.samsung.android.providers.context.databases.ContextLog_0.db	N/A Battery Usage Stats - Contains Application Usage information N/A Google App searches, installed applications and more * Application traces (Samsung devices)
/private/var/mobile/Containers/Data/Application/ <apple_maps_guid>/Library/SyncedPreferences/com.apple. Maps-com.apple.Maps.recents.plist /private/var/mobile/Containers/Data/Application/<apple_maps_guid>/Library/SyncedPreferences/com.apple.</apple_maps_guid></apple_maps_guid>	Apple Maps recents Apple Maps bookmarks Y	N N	Userdata /data/com.sec.android.app.launcher/databases/launcher.db Userdata /data/data/com.google.android.gms/files/batterystatsdumpsystask.gz	N/A Application artifacts (even after deleted) N/A Battery Usage Stats - Contains Application Usage information
Maps-com.apple.MapsSupport.bookmarks.plist /private/var/mobile/Containers/Data/Application/ <apple_maps_guid>/Library/SyncedPreferences/com.apple.</apple_maps_guid>	Apple Maps history Y	N N	Userdata /system/appops.xml Userdata /system/batterystats.bin Userdata /system/batterystats-checkin.bin	N/A Application permissions N/A Battery Usage Stats - Contains Application Usage information N/A Battery Usage Stats - Contains Application Usage information
Maps-com.apple.MapsSupport.history.plist /private/var/mobile/Containers/Shared/AppGroup/ <apple_maps_guid>/Library/Preferences/group.com.apple.Maps.plist /private/var/mobile/Library/Caches/com.apple.routined/Caches.glite</apple_maps_guid>	Last latitude and longitude, map search history Y Location information	Y N I N N	Userdata /system/batterystats-daily.xml Userdata /system/dmappmgr.db Userdata /system/job/jobs.xml	N/A Battery Usage Stats - Contains Application Usage information N/A Application Usage N/A Application Usage
/private/var/mobile/Library/Preferences/com.apple.locationd.plist	Location information N "Location Services" setting (Enabled = 1; Disabled = 0) Y	I N N Y N Y N	Userdata /system/notification_log.db Userdata /system/packages.list	N/A Application notifications N/A Application permissions and metadata
/private/var/mobile/Library/Preferences/com.apple.preferences.datetime.plist /private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist /private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist /private/var/preferences/SystemConfiguration/preferences.plist	Time settings Y Language, Country info, Device IDs Y Network IP, WiFi, Cellular Y	Y N Y N Y N	Userdata /system/packages.xml Userdata /system/usagestats/0/* Userdata /system/users/0/app_idle_stats.xml	N/A Application permissions N/A Application Usage Stats N/A Application Usage
/private/var/preferences/SystemConfiguration/preferences.plist /private/var/root/Library/Caches/locationd/Cache.sqlite /private/var/root/Library/Caches/locationd/cache_encryptedA.db	Network and VPN information Y Location information N Location information N	Y N I N N	Userdata /system_ce/0/recent_images/*.png Userdata /system_ce/0/recent_tasks/*.xml	N/A Application snapshots N/A Recent Tasks
/private/var/root/Library/Caches/locationd/cache_encryptedB.db /private/var/root/Library/Caches/locationd/cache_encryptedC.db	Location information N Location information N	N N N N N N	Userdata /log/sdp_log - valid and invalid lockscreen code attempts NATIVE APPLICATIONS	N/A Valid and invalid lockscreen code attempts
/private/var/root/Library/Caches/locationd/consolidated.db /private/var/root/Library/Caches/locationd/significant.plist /private/var/root/Library/Caches/locationd/significantVisitAuth.plist	Application Traces and GeoFence information Y Significant Location N Significant Location Y	Y N I Y N Y N	Userdata /data/com.android.providers.calendar/databases/calendar.db Userdata /data/com.android.providers.contacts/databases/contacts2.db	* Calendar Items contacts & raw contacts Contacts
/private/var/root/Library/Caches/locationd/significantVisitInterest.plist	Significant Location Y	Y	Userdata /data/com.android.providers.contacts/databases/contacts2.db Userdata /data/com.android.providers.contacts/databases/calllog.db Userdata /data/com.android.providers.downloads/databases/downloads.db	calls Call Logs calls Call Logs * Downloads
TRACES OF DESTRUCTION — WIPING, ETC. /private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist /private/var/root/.obliterated	Language, Country info, Device IDs Creation time stamp -> Device reset time Y	Y Y	Userdata /data/com.google.android.gms/databases/icing_contacts.db Userdata /data/com.google.android.gms/databases/icing_mmssms.db Userdata /data/com.google.android.gms/databases/ipa_mmssms.db	* Contacts MMS/SMS * MMS/SMS
/private/var/root/Library/Preferences/com.apple.MobileBackup.plist	Restore information (timestamp, local vs. iCloud)	Y Y	Userdata /data/com.google.android.gms/databases/ipa_mmssms.db Userdata /data/com.google.android.gms/databases/android_pay Userdata /data/com.google.android.gms/databases/pluscontacts.db	wallet Android Pay * Google+ Contacts