Gigabyte

Evidence per

SANS DFIR CURRICULUM

(f) SANSForensics (D) @SANSForensics (D) dfir.to/DFIRCast (E) dfir.to/LinkedIn

DIGITAL FORENSICS



Digital Acquisition Digital Forensics and Rapid Triage **Essentials**



Windows Forensic Analysis GCFE



Mac and iOS Forensic Analysis & Incident Response



Smartphone Forensic Analysis In-Depth

GASF

for585.com/poster

FOR585: Smartphone Forensic Analysis In-Depth sans.org/for585



FOR508 Advanced Incident Response, Threat Hunting & Digital Forensics

Cyber Threat

Intelligence

GCTI



FOR509

FOR608 Enterprise-Class Incident Response & Threat Hunting



INCIDENT RESPONSE & THREAT HUNTING

FOR528 Ransomware for Incident Responders

FOR610

REM: Malware Analysis

Tools & Techniques

GREM

those with and without attachments.



Malware: Advanced

Code Analysis

Advanced Network Forensics: Threat Hunting, Analysis &



FOR710 Reverse-Engineering



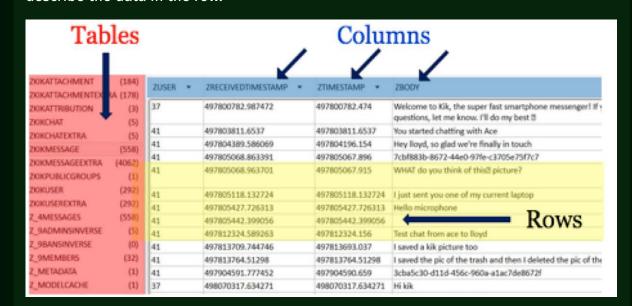
SEC504 Hacker Tools, Techniques & Incident Handling **GCIH**

DFPS_FOR585_v3.8_04-23

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.

The Most Relevant



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

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

DESC = Descending ASC = Ascending Searching with WHERE and LIKE:

Practitioners/Researchers Mattia Epifani Adrian Leong Alexis Brignoni Jon B Mari DeGrazia

Andrew Hoog Ian Whiffin

Josh Hickman

Sarah Edwards https://www.mac4n6.com Heather Mahalik https://smarterforensics.com http://mattiaep.blogspot.com https://abrignoni.blogspot.com https://www.ciofecaforensics.com http://az4n6.blogspot.com

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

Vendors Oxygen Forensics https://blog.oxygen-forensic.com Cellebrite

Sanderson Forensics Elcomsoft MSAB Belkasoft

Grayshift

Magnet Forensics https://www.magnetforensics.com https://www.cellebrite.com/en/blog support-articles https://blog.elcomsoft.com

https://sqliteforensictoolkit.com/ https://www.msab.com/resources/blog https://belkasoft.com/articles https://www.grayshift.com https://paraben.com/forensic-impact

Our Favorite Mobile Forensic Resources

Additional Resources

DFRWS https://dfrws.org iOS Jailbreaks https://www.theiphonewiki.com/wiki/Jailbreak **DFIR Review**

https://dfir.pubpub.org This Week in 4N6 https://thisweekin4n6.com IMEI.info https://www.imei.info **GSM** Arena https://www.gsmarena.com Phone DB https://phonedb.net

FOR585 Google *access granted to all 585 Alumni Group

DFIR mailing list DFIR@lists.sans.org

Mobile Malware and Spyware

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.

Users can navigate to/from and interact with activities directly through the User Interface (UI). **Services:** Tasks often running in the background and integrated into the application. User doesn't (normally) interact with

Activities: One or more activities comprise each 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.

Applications can be programmed to "listen" for events that are

Services. Examples: music playing during a gaming application,

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 proper Content Provider.

jadx-gui - evernote.apk File View Navigation Tools Help 🔓 🔓 🥰 # 🎤 🔍 🗘 🗘 🎯 📳 🥕 2 Resources AndroidManifest.xml 💥 # META-INF assets manifest xmlns:android="http://schemas.android.com/apk/res/android" xmlns:app="http://schema classes.dex <uses-sdk android:minSdkVersion="23" android:targetSdkVersion="28"/> <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/> classes2.dex <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/> <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/> firebase-analytics-impl.properties <uses-permission android:name="android.permission.GET_ACCOUNTS"/> firebase-analytics.properties <uses-permission android:name="android.permission.INTERNET"/> firebase-appindexing.properties <uses-permission android:name="android.permission.READ_SYNC_SETTINGS"/> firebase-common.properties <uses-permission android:name="android.permission.READ_SYNC_STATS"/> firebase-config.properties <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/> firebase-core.properties <uses-permission android:name="android.permission.USE_BIOMETRIC"/> firebase-iid-interop.properties <uses-permission android:name="android.permission.VIBRATE"/> <uses-permission android:name="android.permission.WAKE_LOCK"/</pre> firebase-measurement-connector-impl.properties <uses-permission android:name="android.permission.WRITE_SYNC_SETTINGS"/> firebase-measurement-connector.properties <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/</p> <uses-permission android:name="android.permission.USE_FINGERPRINT"/2</p> okhttp3 <uses-permission android:name="android.permission.READ_CALENDAR"/> play-services-ads-identifier.properties <uses-permission android name="android permission CAMERA"/> play-services-analytics-impl.properties <uses-permission android:name="android.permission.READ_CONTACTS"/> play-services-analytics.properties <uses-permission android:name="android.permission.MANAGE_ACCOUNTS"/> play-services-audience.properties <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/> play-services-auth-api-phone.properties <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/> play-services-auth-base.properties <uses-permission android:name="android.permission.RECORD_AUDIO"/> play-services-auth.properties <uses-permission android:name="android.permission.READ_PHONE_STATE"/> play-services-base properties <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/> play-services-basement.properties <uses-permission android:name="com.android.vending.BILLING"/> play-services-drive.properties <uses-permission android:name="android.permission.USE_CREDENTIALS"/> <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/> play-services-gcm.properties play-services-iid.properties <uses-permission android:name="com.sonymobile.permission.CAMERA_ADDON"/</p>

Specification-Based

Common Signs and Symptoms

- Android devices are most at risk
 Unexpected device behaviors for mobile malware infection
- Poor battery life • Dropped calls and call disruptions
- Unusually large phone bills
- Data plan spikes Device performance problems

Unexplained application errors

Online Mobile Malware

Upload suspicious .apk files to the

https://www.joesandbox.com

https://www.virustotal.com

Internet for online sandbox analysis:

https://github.com/pjlantz/droidbox

Sandboxes

- 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

Check installed Establish a applications for suspicious timeline application files **Beyond Scanning for** Research error **Malware with Forensic** messages/notifications

Signature-Based

Local Static Malware Analysis

- Android SDK
- Dex2Jar
- JD-GUI

Tools installed on the local machine for

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

Malware action— do families behave App store approach, dynamic analysis **Bit Defender/** What activity is arching for patterns considered normal **Check downloads** folder(s) for suspicious files **Check browser** 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

Mobile Malware Detection

Mobile Malware

Behavioral-Based

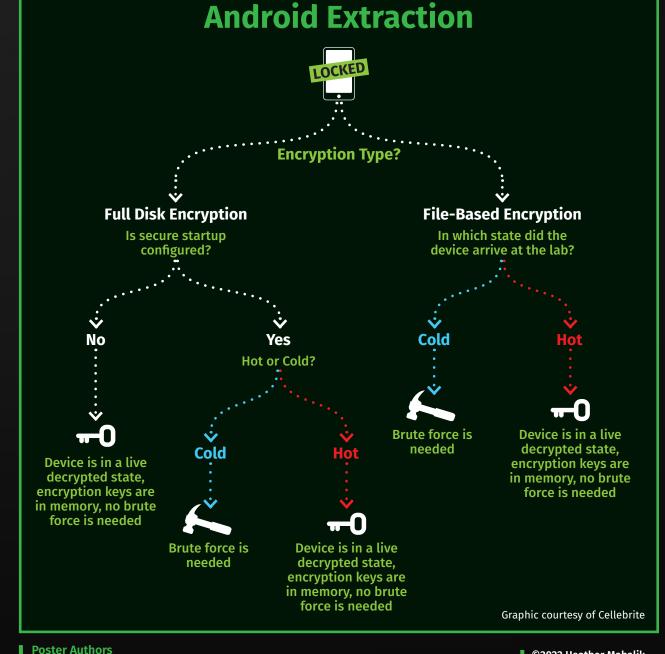
Data Mining

Cloud-Based

Free Scripts and Helpful Utilities

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

Ι.				
ш		APOLLO	Apple Pattern of Life Lazy Output'er	https://github.com/mac4n6/APOLLO
ш		İLEAPP	iOS Logs, Events, And Properties Parser	https://github.com/abrignoni/iLEAPP
08		iOS-Mobile- Installation- Logs-Parser	iOS installation and uninstallation log parser	https://github.com/abrignoni/iOS-Mobile- Installation- Logs-Parser
		iOS Triage	Incident response tool for iOS devices	https://github.com/RealityNet/ios_triage
П		fplist	Converts plist files to json, dot notation or csv	https://www.hack42labs.com/tools/fplist/details
П		iOS_sysdiagnose_ forensic_scripts	Scripts for parsing various iOS sysdiagnose logs	https://github.com/cheeky4n6monkey/iOS_ sysdiagnose_forensic_scripts
П		libimobiledevice		https://www.libimobiledevice.org
Ιſ	Aliuroiu	ALEAPP	Android Logs Events & Protobuf Parser	https://github.com/abrignoni/ALEAPP
		Android Usagestats XML + Protobuf Parser	Parser for Android Usagestats files in xml or protobuf format	https://github.com/abrignoni/ Android-Usagestats-XML-Protobuf
Android		ftree	Identifies, hashes and destructures all files recursively from any file system	https://www.hack42labs.com/tools/ftree/details/
Ιī	•	FAPK	Extracts apk files from an Android device	https://www.hack42labs.com/tools/fapk/
П		Andriller		https://github.com/den4uk/andriller
Ц		Android Triage		https://github.com/RealityNet/android_triage
	ı nırd-Party ications/SQLite	DFIR-SQL- Query-Repo	Collection of SQL query templates for digital forensics use by platform and application	https://github.com/abrignoni/DFIR-SQL-Query-Repo
artv-		SQLite-Deleted- Records-Parser	Recovers deleted entries from SQLite databases	https://github.com/mdegrazia/SQLite-Deleted- Records-Parser
hird-F		SQLECmd	Automates the identification and processing of sqlite database files	https://github.com/EricZimmerman/SQLECmd
		sqlite_miner	Mines SQLite databases for BLOBs and potential unparsed content of interest	https://github.com/threeplanetssoftware/ sqlite_miner
		4n6-scripts	Collection of forensic and third-party scripts	https://github.com/cheeky4n6monkey/4n6-scripts



Heather Mahalik Domenica "Lee" Crognale hmahalik@gmail.com domenica.crognale@gmail.com @heathermahalik @domenicacrognal

Mattia Epifani mattia.epifani@realitynet.it @mattiaep

©2022 Heather Mahalik, Domenica "Lee" Crognale, and Mattia Epifani. All Rights Reserved.

				_		
$oldsymbol{\cap}$	5		ea			

iOS Cheatsheet	Description	BFU	Backup	Sysdiagnose
DEVICE INFORMATION /private/var/installd/Library/MobileInstallation/LastBuildInfo.plist /private/var/mobile/Library/CoreDuet/coreduetd.db /private/var/mobile/Library/Logs/mobileactivationd/ /private/var/mobile/Library/Preferences/com.apple.AdLib.plist /private/var/mobile/Library/Preferences/com.apple.aggregated.plist	Operating system version Lock/Device Passcode Info (0=unlocked, 1=locked) (Up to iOS 9) MobileActivation Logs May show older iOS versions used Last BootTime	Y N Y Y	Y N N Y Y	N N Y N
/private/var/mobile/Library/Preferences/com.apple.mmcs.plist /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.network.plist /private/var/mobile/Library/Preferences/com.apple.Preferences.plist /private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist /private/var/mobile/Library/Preferences/com.apple.timed.plist /private/var/mobile/Library/Preferences/com.apple.timed.plist	IMSIs Device name Time settings Airplane mode (on/off) Disk usage Language, Country info, Device IDs Auto Time and Auto Time Zone settings	Y Y Y Y Y	Y Y Y Y Y	N N N N N
/private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist /private/var/preferences/SystemConfiguration/com.apple.radios.plist /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist /private/var/preferences/SystemConfiguration/preferences.plist /private/var/root/Library/Lockdown/escrow_records/ /private/var/root/Library/Lockdown/pair_records/ /private/var/root/Library/Preferences/com.apple.preferences.network.plist	Network IP, WiFi, Cellular Information Airplane mode (on/off) Wi-Fi Mac Addresses Network and VPN information Computer Trust/Pair certificates Computer Trust/Pair certificates Airplane mode (on/off)	Y Y Y Y Y	Y Y N Y N	N N Y N N
/private/var/wireless/Library/Preferences/com.apple.commcenter.plist /private/var/mobile/MobileSoftwareUpdate/restore.log PASSWORDS AND ACCOUNT INFORMATION /private/var/mobile/Library/Accounts/Accounts3.sqlite /private/var/mobile/Library/DataAccess/ /private/var/mobile/Library/DataAccess/ /private/var/mobile/Library/DataAccess/AccountInformation.plist	Device Info (IMEI, Phone Number, Network Carrier, ICCIDs, IMSIs, etc.) Mobile Software Update Account information Account information used to set up apps (Email, #, etc) Email sync data	Y Y Y	Y N Y Y	N N N N
/private/var/mobile/Library/DataAccess/iCloud-[iCloud email account name]/.mboxCache.plist /private/var/mobile/Library/Health/healthdb.sqlite /private/var/mobile/Library/Health/healthdb_secure.sqlite /private/var/mobile/Library/MedicalID/MedicalIDData.Archive /private/var/mobile/Library/Preferences/com.apple.accountsettings.plist /private/var/mobile/Library/Preferences/com.apple.cmfsyncagent.plist /private/var/mobile/Library/Preferences/com.apple.commcenter.shared.plist /private/var/mobile/Library/Preferences/com.apple.commcenter.shared.plist	iCloud Émail account information Health data, personal data, iOS version info, etc. Health data, personal data, iOS version info, etc. Medical Information (bloodtype, organ donor, name, DOB, etc.) Email accounts pushed to device Blocked Dialers Phone number	Y N N Y	Y Y Y Y Y	N N N N N
/private/var/mobile/Library/Preferences/com.apple.conference.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.corerecents.recentsd.plist /private/var/mobile/Library/Preferences/com.apple.FeedbackAssistant.plist	Facetime phone number in use, SMS phone number, user accounts Last Metrics Attempts (usage information) Activity throttling Activity throttling iCloud login information Last successful email address used to login to cloud	Y Y Y Y Y	Y Y Y Y Y	N N N N N
/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/ /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	iCloud account information Find My iPhone settings Profiles and restrictions Account information Last backup computer, iCloud Backup Settings, Device info Last iCloud account	Y Y Y Y Y	Y Y Y Y N	N N N N N
SETTINGS - SYSTEM CONTROLLED - KEYBOARDS, DICTIONARY, LOGS, BT ADDRESS, ETC. /private/installd/Library/Logs/MobileInstallation/mobile_installation.log.* /private/var/mobile/Containers/ /private/var/mobile/Library/BulletinBoard/ClearedSections.plist /private/var/mobile/Library/Keyboard/ <language>-dynamic.lm/dynamic-lexicon.dat /private/var/mobile/Library/Preferences/ /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist</language>	Mobile Applications Installation Logs Application Folders Logs of cleared notifications Auto correction / Predictive text Examine plists for more information Wi-Fi Mac Addresses	Y Y Y N Y	N Y Y N Y	Y N N N N
SETTINGS - USER CONTROLLED - SYNC SETTINGS, SPRINGBOARD, ETC. /private/var/containers/Shared/SystemGroup/systemgroup.com.apple.configurationprofiles/Library/ConfigurationProfiles/ CloudConfigurationDetails.plist /private/var/mobile/Library/DoNotDisturb/DB/Settings.sqlite /private/var/mobile/Library/Keyboard/UserDictionary.sqlite /private/var/mobile/Library/Mail/ /private/var/mobile/Library/Preferences/com.apple.assistant*	Cloud configurations Do not disturb settings User created auto-correct Mail and settings Siri	N Y N N	N Y N N	N N N
/private/var/mobile/Library/Preferences/com.apple.assistant.backedup.plist /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 /private/var/mobile/Library/Preferences/com.apple.CoreDuet.plist /private/var/mobile/Library/Preferences/com.apple.imservice*	Cloud sync settings Camera settings Camera, CarPlay, Volumes and other settings Cloud photo sync information Cloud sync settings SMS, iMessage and FaceTime	Y Y Y Y Y	Y Y Y Y Y	N N N N N
/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 /private/var/mobile/Library/SpringBoard/HomeBackground.cpbitmap /private/var/mobile/Library/SpringBoard/HomeBackgroundThumbnail.jpg /private/var/mobile/Library/SpringBoard/IconState.plist	Time to keep messages Airplane Mode Settings User created restrictions/Remote wipe settings Weather (including current city) Wallpaper Wallpaper Homescreen icon layout	Y Y Y Y Y	Y Y Y Y Y	N N N N N
/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 /private/var/mobile/Library/UserNotifications/ /private/var/root/Library/Lockdown/data_ark.plist	Wallpaper Wallpaper Wallpaper Notifications User created restrictions User Notifications Last backup computer, iCloud Backup Settings, Device info	Y Y Y N Y Y	Y Y Y N Y Y	N N N N N N
/private/var/root/Library/Preferences/com.apple.preferences.network.plist /private/var/mobile/Library/DuetExpertCenter/streams/userNotificationEvent/local COMMUNICATIONS - SMS, CALLS, EMAIL /private/var/mobile/Library/CallHistory/call_history.db /private/var/mobile/Library/CallHistoryDB/CallHistory.storedata /private/var/mobile/Library/CallHistoryDB/CallHistoryTemp.storedata	Airplane Mode Settings iOS Notifications Call log (Up to iOS 7) Call log (From iOS 8) Call History Temporary storage (Before First Unlock)	N N N Y	Y N Y Y	N N N N N
/private/var/mobile/Library/CallHistoryTransactions/SGUID>.log /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 /private/var/mobile/Library/Recents/ /private/var/mobile/Library/SMS/Attachments/*	Call log traces Mail and settings SMS, iMessage and FaceTime List of contacts added to the phone application's favorites list SMS, iMessage and FaceTime Recents communications MMS File	N N Y N Y N	N N Y Y Y	N N N N N
/private/var/mobile/Library/SMS/Drafts/* /private/var/mobile/Library/SMS/sms.db /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/MMS Drafts SMS/MMS messages SMS Temporary storage (Before First Unlock) Contains iMessage/SMS traces Voicemail Voice Memos	N N Y N Y	Y Y N N N	N N N N N
BROWSER ACTIVITY /private/var/mobile/Containers/Data/Application/ <apple guid="" safari="">/Library/Caches/com.apple.mobilesafari/ /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/Caches/com.apple.mobilesafari/Cache.db /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/Caches/com.apple.WebAppCache/ApplicationCache.db /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/Favicons/Favicons/ /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/Preferences/com.apple.mobilesafari.plist</apple></apple></apple></apple></apple>	Safari Cache files Safari Cache database Safari Website cache Safari Cookies Safari Website favicons Safari Configuration	N N N N N	N N N Y N	N N N N
/private/var/mobile/Containers/Data/Application/ <apple guid="" safari="">/Library/Safari/Downloads/Downloads.plist /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/Safari/Thumbnails/ /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/WebKit/WebsiteData/LocalStorage/* /private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db /private/var/mobile/Library/Safari/Bookmarks.db /private/var/mobile/Library/Safari/BrowserState.db /private/var/mobile/Library/Safari/CloudTabs.db</apple></apple></apple>	Safari Download History Safari Tabs Screenshots (PNG or KTX format) Safari WebKit Localstorage Safari History information Safari Bookmarks Safari Suspended State Tab Safari Cloud Tabs	N N Y N N	Y Y Y N Y	N N N N N
/private/var/mobile/Library/Safari/History.db /private/var/mobile/Library/Safari/SafariTabs.db MULTIMEDIA *.ktx /private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb /private/var/mobile/Library/Preferences/com.apple.mobileslideshow.plist /private/var/mobile/Library/SMS/Attachments/	Safari History Safari Tabs Application Snapshots Contacts pictures Photos MMS File	N N N N Y	N N Y Y	N N N N
/private/var/mobile/Media/DCIM/1*APPLE /private/var/mobile/Media/iTunes_Control/iTunes/MediaLibrary.sqlitedb /private/var/mobile/Media/MediaAnalysis/mediaanalysis.db /private/var/mobile/Media/PhotoData/Thumbnails/*.ithmb /private/var/mobile/Media/PhotoData/AlbumsMetadata/ /private/var/mobile/Media/PhotoData/CPL/ /private/var/mobile/Media/PhotoData/Photos.sqlite	User Created/Saved Photos iTunes Media Library Media analysis and classification Thumbnails databases Photo Albums Metadata Cloud Photo Library Photos/Videos Database	N Y N N N	Y Y Y Y Y	N N N N N
/private/var/mobile/Media/PhotoData/Thumbnails/V2/ NETWORK CONNECTIONS /private/var/db/dhcpclient/leases/ /private/var/mobile/Library/homed/datastore.sqlite /private/var/mobile/Library/Preferences/com.apple.preferences.network.plist /private/var/networkd/netusage.sqlite	Photos saved from Live Video and SMS photo capture DHCP Lease Apple Home information Airplane mode ON/OFF Network data usage per App	Y N Y N	N Y Y N	N N N N
/private/var/preferences/com.apple.networkextension.plist /private/var/preferences/com.apple.wifi.known-networks.plist /private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist /private/var/preferences/SystemConfiguration/com.apple.wifi.plist /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist /private/var/preferences/SystemConfiguration/preferences.plist /private/var/preferences/SystemConfiguration/preferences.plist /private/var/root/Library/Application Support/com.apple.wifianalyticsd/DeviceAnalyticsModel.sqlite	Network Extension Wi-Fi Network IP, Wi-Fi, Cellular Wi-Fi Wi-Fi Mac Addresses Wi-Fi, VPN, Certs and more Wi-Fi information	Y N Y Y Y	Y Y Y Y N	N Y N Y Y N
/private/var/root/Library/Application Support/WiFiNetworkStoreModel.sqlite /private/var/root/Library/Caches/com.apple.wifid/ThreeBars.sqlite /private/var/root/Library/Preferences/com.apple.preferences.network.plist /private/var/wireless/Library/Databases/CellularUsage.db /private/var/wireless/Library/Databases/DataUsage.sqlite /private/var/wireless/Library/Preferences/com.apple.CommCenter.counts.plist /private/var/wireless/Library/Preferences/com.apple.commcenter.data.plist	Wi-Fi information Wi-Fi information Wi-Fi ON/OFF SIMs used in device, including most recent Network data usage per App Data and Cellular network statistics SIM Card ICCID	N N Y Y N Y	N N Y Y Y Y	N N N N N
/private/var/wireless/Library/Preferences/com.apple.commcenter.device_specific_nobackup.plist /private/var/wireless/Library/Preferences/com.apple.commcenter.plist /private/var/preferences/SystemConfiguration/com.apple.wifi-private-mac-networks.plist 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>	Device IMEI SIM Card ICCID WiFi Networks Scanned Seen Bluetooth devices Paired Bluetooth devices	Y Y N N	Y Y Y	N N N
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Preferences/com.apple.MobileBluetooth.devices.plist /private/var/mobile/Library/Application Support/CloudDocs/backup/backup_manifest.db /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>/</guid></guid></guid>	Paired Bluetooth devices Cloud Documents details iClould offline cache Apple Watch pairing information Apple Watch information (also previously paired Apple Watch) Apple Watch pairing information (also previously paired Apple Watch) Apple Watch data	N N Y Y N N	Y N Y Y Y	N N N N N
/private/var/mobile/Library/DeviceRegistry/ <guid>/NanoAppRegistry/Applications/ /private/var/mobile/Library/DeviceRegistry/<guid>/NanoMail/registry.sqlite /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/homed/datastore.sqlite /private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.plist</guid></guid></guid></guid>	Apple Watch Applications Apple Watch Mail application Apple Watch Wallet Passes Apple Watch Faces Apple Watch Health data sync Apple HomeKit Devices Seen Bluetooth devices	Y Y N Y N N	Y Y Y Y Y	N N N N N
/private/var/mobile/Library/NanoBackup/ /private/var/mobile/Library/NanoMusicSync/ /private/var/mobile/Library/NanoPreferencesSync/ /private/var/mobile/Library/NanoTimeKit/ /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.QueuedDenials.plist /private/var/mobile/Library/Preferences/com.apple.CoreDuet.QueuedDenials.plist	Apple Watch information Apple Watch information Apple Watch information Apple Watch information Apple CarPlay configuration iCloud quota information Cloud Sync denials and dates	Y Y Y Y Y	Y N N N Y Y	N N N N N
/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 /private/var/mobile/Library/Preferences/com.apple.nano*.plist /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</guid>	sync devices iCloud sync, Email, FaceTime, Email, more Last iTunes and last iCloud backup date and timezone. Apple Watch preferences Device AirDrop ID Apple CarPlay per car App Icon configuration List of computer where the device was connected to	Y Y Y Y Y	Y Y Y Y Y	N N N N N
/private/var/root/Library/Lockdown/data_ark.plist /private/var/wireless/Library/Databases/DataUsage-watch.sqlite LOCATION ARTIFACTS /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 guid="" maps="">/Library/Maps/History.mapsdata</apple></apple_maps_guid></guid>	Last backup computer, iCloud Backup Settings, Device info Watch Application Usage Seen Bluetooth devices Apple Maps history Apple Maps history	N N N N	N N Y Y	N N N N
/private/var/mobile/Containers/Data/Application/ <apple_maps_guid>/Library/Preferences/com.apple.Maps.plist /private/var/mobile/Containers/Data/Application/<apple_maps_guid>/Library/SyncedPreferences/com.apple.Maps-com.apple.Maps.recents.pli /private/var/mobile/Containers/Data/Application/<apple_maps_guid>/Library/SyncedPreferences/com.apple.Maps-com.apple. MapsSupport.bookmarks.plist /private/var/mobile/Containers/Data/Application/<apple_maps_guid>/Library/SyncedPreferences/com.apple.Maps-com.apple. MapsSupport.history.plist /private/var/mobile/Containers/Shared/AppGroup/<apple_maps_guid>/Library/Preferences/group.com.apple.Maps.plist</apple_maps_guid></apple_maps_guid></apple_maps_guid></apple_maps_guid></apple_maps_guid>	Last latitude and longitude, map search history ist Apple Maps recents Apple Maps bookmarks Apple Maps history Last latitude and longitude, map search history	Y Y Y	Y N N	N N N
/private/var/mobile/Containers/Shared/AppGroup/ <apple_maps_guid>/Maps/MapsSync_0.0.1 /private/var/mobile/Library/Caches/com.apple.routined/Cache.sqlite /private/var/mobile/Library/Caches/com.apple.routined/Cloud-V2.sqlite /private/var/mobile/Library/Caches/com.apple.routined/Local.sqlite /private/var/mobile/Library/PersonalizationPortrait/PPSQLDatabase.db /private/var/mobile/Library/Preferences/com.apple.locationd.plist</apple_maps_guid>	Apple Maps history Location information Location information Location information Personalization Portrait "Location Services" setting (Enabled = 1; Disabled = 0)	N N N N N Y	N N N N Y	N N N N N
/private/var/mobile/Library/Preferences/com.apple.preferences.datetime.plist /private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist /private/var/mobile/Media/PhotoData/Caches/GraphService/CLSPublicEventCache.sqlite /private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist /private/var/preferences/SystemConfiguration/preferences.plist /private/var/root/Library/Caches/locationd/Cache.sqlite /private/var/root/Library/Caches/locationd/cache_encryptedA.db	Time settings Language, Country info, Device IDs Queried events Network IP, WiFi, Cellular Network and VPN information Location information Location information	Y Y N Y Y	Y Y N Y Y	N N N N N
/private/var/root/Library/Caches/locationd/cache_encryptedB.db /private/var/root/Library/Caches/locationd/cache_encryptedC.db /private/var/root/Library/Caches/locationd/consolidated.db /private/var/root/Library/Caches/locationd/significant.plist /private/var/root/Library/Caches/locationd/significantVisitAuth.plist /private/var/root/Library/Caches/locationd/significantVisitInterest.plist	Location information Location information Application Traces and GeoFence information Significant Location Significant Location Significant Location	N N Y N Y	N N Y Y Y	N N N N N
TRACES OF DESTRUCTION - WIPING, ETC. /private/var/db/diagnostics/ /private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist /private/var/root/.obliterated /private/var/root/Library/Logs/MobileContainerManager /private/var/root/Library/Preferences/com.apple.MobileBackup.plist BATTERY/POWER	Language, Country info, Device IDs Creation time stamp -> Device reset time Container Manager Logs Restore information (timestamp, local vs. iCloud)	N Y Y N Y	N Y N N Y	N Y N Y
BATTERY/POWER /private/var/containers/Shared/SystemGroup/ <guid>/Library/BatteryLife/CurrentPowerLog.PLSQL /private/var/mobile/Library/CoreDuet/coreduetd.db /private/var/mobile/Library/Preferences/com.apple.BatteryCenter.BatteryWidget.plist /private/var/mobile/Library/Preferences/com.apple.coreduetd.batterysaver.state.plist</guid>	Battery life tracker Powering Events (0=unplugged, 1=plugged in) Battery icon status Battery Saver state	N N N Y	N N Y	Y N N

Path	Description	BFU	Backup	Sysdiagnose
APPLICATION USAGE				
/private/var/containers/Shared/SystemGroup/ <guid>/Library/BatteryLife/CurrentPowerLog.PLSQL /private/var/containers/Shared/SystemGroup/<guid>/Library/Logs/mobile_installation_helper.log.* /private/var/installd/Library/Logs/MobileInstallation/mobile_installation.log.* /private/var/mobile/Library/AggregatedDictionary/ADDataStore.sqlitedb /private/var/mobile/Library/AppConduit/AvailableApps.plist /private/var/mobile/Library/AppIcation Support/com.apple.remotemanagmentd/RMAdminStore-Cloud.sqlite</guid></guid>	Battery life tracker	N	N	Υ
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Logs/mobile_installation_helper.log.*</guid>	Application traces	N	Υ	N
/private/var/installd/Library/Logs/MobileInstallation/mobile_installation.log.*	Mobile Applications Installation Logs	Υ	N	Υ
/private/var/mobile/Library/AggregatedDictionary/ADDataStore.sqlitedb	Application traces	Υ	N	N
/private/var/mobile/Library/AppConduit/AvailableApps.plist	Installed Apps and Apps Path	Υ	N	N
/private/var/mobile/Library/AppConduit/AvailableCompanionApps.plist	Installed Apps and Apps Path	Υ	N	N
/private/var/mobile/Library/Application Support/com.apple.remotemanagmentd/RMAdminStore-Cloud.sqlite	Screen time	N	N	N
/DITVALE/VAL/HIUDHE/EIDIALV/ADDIICALIOH SUDDULL/COHLADDIE/EHIDLEHIAHAYHIEHLU/KWAUHHISUUE-LUCALSUHE	Screen time	N	N	N
/private/var/mobile/Library/ApplicationSync/AssetSortOrder.plist	Application order on the SpringBoard	Υ	N	N
/private/var/mobile/Library/Assistant/knowledgeC.db	Application traces	N	N	N
/private/var/mobile/Library/Caches/com.apple.Pasteboard/.*	Pasteboard	N	N	N
/private/var/mobile/Library/com.apple.itunesstored/itunesstored2.sqlitedb	Application traces	Υ	Υ	N
/private/var/mobile/Library/com.apple.itunesstored/kvs.sqlitedb /private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db	Installed Applications	Y	Y	N
/private/var/mobile/Library/CoreDuet/Knowledge/knowledgeC.db	Application traces	N	N	N
/private/var/mobile/Library/CoreDuet/People/interactionC.db	Application traces	N	Y	N
/private/var/mobile/Library/FrontBoard/applicationState.db	Application traces	Y	Y	N
/private/var/mobile/Library/Health/ActivitySharing/contacts2.dat	Fitness Friends	N	N	N
/private/var/mobile/Library/Keyboard/langlikelihood.dat	Application traces	Y	Y	N
/private/var/mobile/Library/locationd/user.plist	Step/Stride Cadence, Pedometer Info	N	Y	N Y
/private/var/mobile/Library/Logs/AppConduit/	Installed Apps and Apps Path	Y	N	
/private/var/mobile/Library/Logs/mobile_installation_helper.log* /private/var/mobile/Library/Preferences/addaily.plist	Application traces	N	Y	N
/private/var/mobile/Library/Preferences/addaily.plist	Application traces	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.ActivitySharing.plist	Information about Fitness Friends	Y	Y	N
/private/var/mobile/Library/preferences/com.apple.AppStore.plist	Last search on Apple Store	Y	Y	N N
/private/var/mobile/Library/Preferences/com.apple.corespotlightui.plist	Application traces	Y	Y	IN N
/private/var/mobile/Library/Preferences/com.apple.mt.lastLaunch.plist	Application Execution Traces	N	Y	N
/private/var/mobile/Library/TCC/TCC.db	Applications permissions	Y	Y	Y
/private/var/networkd/netusage.sqlite	Network data usage per App	N	N	N
/private/var/root/Library/Caches/locationd/clients.plist	Application using location services	Y	Y	IN V
/private/var/root/Library/Logs/MobileContainerManager /private/var/root/Library/MobileContainerManager/containers.sqlite3	MobileContainerManager logs	Y	N N	Y N
/private/var/root/Library/Databases/DataUsage.sqlite	Installed Applications Application traces	Y	IN V	N N
/private/var/mobile/Library/Biome	iOS Suggestions (Biome)	N	Y N	N N
/private/var/mobile/Library/Biorite /private/var/db/biome	iOS Suggestions (Biome)	N N	N N	N N
/ private/ vai/au/ bionie	103 3uggestions (biolite)	IV	IV	IV

Android Cheatsheet

Partition	Path	Tables of Interest	Description
DEVICE IN System Userdata Userdata Userdata Userdata	FORMATION /build.prop /data/com.android.providers.calendar/databases/calendar.db /data/com.android.providers.settings/databases/settings.db /data/com.android.providers.settings/databases/settings.db-WAL /data/com.android.providers.settings/databases/locksettings.db	N/A * *	Device information (version, patches, etc.) Calendar Items and Timezone information Lock settings information Lock settings information Lock settings information
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.android.providers.settings/databases/locksettings.db-WAL /data/com.google.android.gms/databases/MdpSimBasedDatabase /data/com.google.android.gms/shared_prefs/Checkin.xml /data/com.google.android.gsf/databases/gservices.db /misc/ /Property/persist.sys.timezone	* * N/A N/A N/A	Lock settings information Sim card information Activity on device related to installed SIM (ICCID and Google Account included) Fitness settings, network settings, other settings Bluetooth, VPN, Wi-Fi and more Timezone (Up to Android 8)
Userdata Userdata Userdata Userdata Userdata	/Property/persistent_properties /system/*.key /system/device_policies.xml /system/locksettings.db /system/locksettings.db-WAL	N/A N/A N/A *	Timezone (From Android 9) Files needed for password cracking Passcode requirements and policies. Syncing info may exist Lock settings information Lock settings information
Userdata Userdata Userdata Userdata Userdata Userdata	/system/netpolicy.xml /system/SimCard.dat /system/users/0/settings_global.xml /system/users/0/settings_secure.xml /system/users/0/settings_system.xml /user_de/0/com.android.providers.telephony/databases/telephony.db	N/A N/A N/A N/A N/A N/A	Timezone Sim card and phone number information Global settings Secure settings System settings Sim card information
Userdata Userdata Userdata	DS AND ACCOUNT INFORMATION /data/com.android.email/databases/EmailProvider.db /data/com.android.providers.contacts/databases/contacts2.db /data/com.android.providers.settings/*	Account, Email AddressCache, Mailbox* accounts N/A	Email accounts, 3rd party app data, and messages associated with Email notifications, Login info Username and passwords
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.android.vending/shared_prefs/lastaccount.xml /data/com.google.android.gms/shared_prefs/BackupAccount.xml /data/com.google.android.googlequicksearchbox/databases/app_icons.db /data/com.google.android.googlequicksearchbox/databases/launcher.db /data/com.google.android.googlequicksearchbox/databases/opa_history /data/com.google.android.gsf/databases/gservices.db	N/A N/A * *	Last account used on Google PlayStore (Android 9 and above) Backup account email address Google Account Information Google Account Information Google Account Information Fitness settings, network settings, other settings
Userdata Userdata Userdata Userdata Userdata Userdata	/misc/apexdata/com.android.wifi/softap.conf /misc/wifi/softap.conf /misc/wifi/wpa_supplicant.conf /system/accounts*.db /system/sync/accounts.xml /system/users/0/0.xml	N/A N/A N/A * N/A N/A	Hotspot Passwords [From Android 11] Hotspot Passwords [Up to Android 10] Wi-Fi Network Password User account information User information User information
Userdata Userdata SYSTEM S Userdata Userdata Userdata	/system_ce/0/accounts_ce.db /system_de/0/accounts_de.db	N/A *	Additional accounts (could also be system_de or accounts_de) Additional accounts (could also be system_de or accounts_de) Preference files Fitness settings, network settings, other settings
Userdata Userdata Userdata Userdata Userdata	/system/recent_images/*.png /system/users/0/settings_global.xml /system/users/0/settings_secure.xml /system/users/0/settings_system.xml /system_ce/recent_images/*.png	N/A N/A N/A N/A	Application snapshots Global settings Secure Settings System Settings Application snapshots
USER SET Userdata Userdata Userdata Userdata Userdata Userdata	FINGS /data/com.android.providers.calendar/databases/calendar.db /data/com.android.providers.userdictionary/databases/user_dict.db /data/com.google.android.gms/databases/NetworkUsage.db /data/com.google.android.gms/databases/ns.db /data/com.google.android.gms/databases/reminders.db	* * * *	Calendar Items and Timezone information Dictionary Files (Keylogging) Application, User and Location traces Application, User and Location traces Application, User and Location traces
Userdata Userdata Userdata COMMUNI Cache	/data/com.google.android.gsf/databases/googlesettings.db /data/com.google.android.gsf/databases/gservices.db /data/com.sec.android.inputmethod/Swiftkey/user/dynamic.lm CATIONS - SMS, CALLS, EMAILS *	* * N/A	Google preferences – location, maps, wallet, etc1=true Fitness settings, network settings, other settings Dictionary Files (Keylogging) SwiftKey folder name may vary Gmail attachments, Downloads and Browser data
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.android.providers.contacts/databases/calllog.db /data/com.android.providers.contacts/databases/contacts2.db /data/com.android.providers.telephony/databases/mmssms.db /data/com.google.android.apps.dynamite/dynamite.db /data/com.google.android.apps.messaging/databases/bugle_db /data/com.google.android.dialer/databases/dialer.db	calls calls sms and part * *	Call logs (From Android 7) Call logs (Up to Android 6) SMS/MMS Google Chat (formerly Hangouts) RCS/Android Messages (refer to notebook for query) Call logs
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.google.android.gm/databases/ <mail-name>.db /data/com.google.android.gm/databases/bigTopDataDB.<user-id> /data/com.google.android.gm/databases/limallProvider.db /data/com.google.android.gms/databases/icing_mmssms.db /data/com.google.android.gms/databases/ipa_mmssms.db /data/com.sec.android.provider.logsprovider/databases/logs.db</user-id></mail-name>	conversations & messages * * logs	Gmail snippets Email information Email information SMS/MMS [Up to Android 11] SMS/MMS Call logs [Up to Android 9]
Userdata MULTIMEI Userdata Userdata Userdata Userdata	/data/user_de/0/com.android.providers.telephony/app_parts DIA /data/com.android.providers.media.module/databases/external.db /data/com.android.providers.media/databases/external.db /data/com.google.android.apps.maps/databases/ugc_photos_location_data.db	* * photos_top_feature	MMS Attachments Traces to SD card used in the device. This is stored on the phone. [From Android 11] Traces to SD card used in the device. This is stored on the phone. [Up to Android 10] Photos and Videos metadata
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.google.android.apps.photos/databases/gphotos0.db /data/com.samsung.android.providers.media/databases/media.db /data/com.samsung.cmh/databases/cmh.db /data/com.samsung.storyservice/databases/dme.db /data/com.samsung.visionprovider/databases/visionprovider.db /media/	local_media files and location files info files N/A	Camera Photos information Media file metadata (only Samsung devices running Android 11 or above) Camera Photo – Samsung Devices Camera Photo – Samsung Devices Camera Photo – Samsung Devices Acts like SD card
Userdata Userdata Userdata Userdata Userdata	/data/com.android.browser/app_databases/* /data/com.android.browser/app_geolocation/GeolocationPermissions.db /data/com.android.browser/databases/Browser.db /data/com.android.browser/databases/browser2.db	* * * * * * * * * * * * * * * * * * * *	Internet History Internet History Internet History Internet History Internet History
Userdata Userdata Userdata NETWORK Userdata Userdata Userdata	/data/com.android.browser/databases/webview.db /data/com.android.browser/databases/webviewCache.db /data/com.android.email/webviewCache.db CONNECTIONS /data/com.android.connectivity.metrics/databases/events.db /data/com.google.android.gms/databases/herrevad	*	Internet History Internet History Internet History Internet History USB, Bluetooth, NFC and other connects – Acquisition connection tracked Wireless network and MAC addresses
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.google.android.locations/files/cache.cell /data/com.google.android.locations/files/cache.wifi /log/wifi/iwc/iwc_dump.txt /misc/apexdata/com.android.wifi/WiFiConfigStore.xml /misc/wifi/WifiConfigStore.xml	* * N/A N/A N/A	Cellular and WiFi Wireless network and mAC addresses Cellular and WiFi Wireless network connections Wireless network [From Android 11] Wireless network [Up to Android 10]
SYNCING A Userdata Userdata Userdata Userdata Userdata	ARTIFACTS /data/com.google.android.apps.docs.editors.docs/databases/* /data/com.google.android.apps.docs.editors.sheets/databases/* /data/com.google.android.apps.docs.editors.slides/databases/* /data/com.google.android.apps.docs/databases/* /data/com.google.android.apps.genie.geniewidget/databases/newsweather.db	* * * *	Google Docs Google Docs Google Docs Google Docs Sync activity
Userdata Userdata Userdata Userdata Userdata	/data/com.google.android.apps.turbo/databases/bluetooth.db /data/com.google.android.gms/databases/peoplelog.db /data/com.google.android.gms/shared_prefs/com.google.android.gms.auth. authzen.cryptauth.SyncManager.proximity_features.xml /data/com.google.android.gms/shared_prefs/nearbysharing/service/state.xml /misc/bluedroid/bt_config.conf	* * N/A N/A	Bluetooth connections Sync activity – contacts Sync Activity Nearby Share Bluetooth adapter info and connections
Userdata	/system/sync/accounts.xml ARTIFACTS /data/com.google.android.apps.maps/app_tts-temp/tts-%UNIXEPOCH% /data/com.google.android.apps.maps/databases/da_destination_history /data/com.google.android.apps.maps/databases/gmm_storage.db	N/A N/A destination history	Synced Accounts Google Maps turn-by-turn directions [On Anroid 10 and above] Maps Search history Maps
Userdata Userdata Userdata Userdata Userdata	/data/com.google.android.apps.maps/databases/gmm_sync.db /data/com.google.android.apps.maps/databases/search_history.db /data/com.google.android.apps.turbo/databases/turbo.db /data/com.sec.android.daemonapp/db/weatherClock /Media/0/DCIM/Camera	* history & suggestions battery_event *	Syncing Maps Timezone [From Android 8] Location artifacts EXIF data with location info
Userdata Userdata Userdata Userdata Userdata Userdata Userdata	ON USAGE /app/* /dalvik-cache /data/"Application Folder" /data/com.android.vending/databases/data_usage.db /data/com.android.vending/databases/frosting.db	N/A N/A N/A app_data_usage frosting	APK files for installed applications .dex/.oat/.art files for installed applications Application Data Files* Application traces Application traces
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.android.vending/databases/install_queue.db /data/com.android.vending/databases/library.db /data/com.android.vending/databases/localappstate.db /data/com.android.vending/databases/notification_cache /data/com.android.vending/databases/package_verification.db /data/com.android.vending/databases/suggestions.db	install_requests ownership appstate notifications verification_cache suggestions	Application traces
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.android.vending/databases/verify_apps.db /data/com.google.android.apps.turbo/databases/turbo.db /data/com.google.android.apps.wellbeing/databases/app_usage /data/com.google.android.gms/databases/cost.db /data/com.google.android.gms/databases/config.db	battery_event DeviceInfo main app_info	Application traces Battery Level [From Android 8] Digital Wellbeing Cast devices Application traces
Userdata Userdata Userdata Userdata Userdata	/data/com.google.android.gms/databases/gass.db /data/com.google.android.gms/databases/gcm_registrar.db /data/com.google.android.gms/databases/google_app_measurement.db /data/com.google.android.gms/shared_prefs/batterystats.xml /data/com.google.android.googlequicksearchbox/* /data/com.google.android.settings.intelligence/databases/battery-usage-db-v4	N/A N/A BatteryState	Application traces Application traces Application traces Application traces Battery Usage Stats – Contains Application Usage information Google App searches, installed applications and more Battery Usage [From Android 12]
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.samsung.android.providers.context.databases.ContextLog_0.db /data/com.sec.android.app.launcher/databases/launcher.db /data/data/com.google.android.gms/files/batterystatsdumpsystask.gz /data/semclipboard /misc_de/0/apexdata/com.android.permission/runtime-permissions.xml /system/appops.xml	* N/A	Application traces (Samsung devices) [Up to Android 10] Application artifacts (even after deleted) Battery Usage Stats – Contains Application Usage information Clipboard content Runtime permissions [Android 11 and 12] Application permissions
Userdata Userdata Userdata Userdata Userdata Userdata	/system/appops/discrete /system/batterystats.bin /system/batterystats-checkin.bin /system/batterystats-daily.xml /system/dmappmgr.db /system/job/jobs.xml	N/A N/A N/A N/A N/A N/A	Privacy dashboard [From Android 12] – ABX Format Battery Usage Stats – Contains Application Usage information Battery Usage Stats – Contains Application Usage information Battery Usage Stats – Contains Application Usage information Application Usage Application Usage Application Usage
Userdata Userdata Userdata Userdata Userdata Userdata	/system/notification_log.db /system/packages.list /system/packages.xml /system/shutdown-checkpoints /system/usagestats/0/* /system/users/0/app_idle_stats.xml	N/A N/A N/A N/A N/A	Application notifications [Up to Android 10] Application permissions and metadata Application permissions Shutdown Checkpoints Application Usage Stats Application Usage
Userdata Userdata Userdata Userdata Userdata	/system/users/0/runtime/runtime-permissions.xml /system_ce/0/recent_images/*.png /system_ce/0/recent_tasks/*.xml /user/0/com.google.android.as/databases/SimpleStorage /misc_de/0/apexdata/com.android.permission/roles.xml	N/A N/A N/A * N/A	Runtime permissions [Android 10] Application snapshots Recent Tasks Application Launch Report Application Roles Report
Userdata NATIVE AF Userdata Userdata Userdata Userdata Userdata	/user/0/com.google.android.apps.turbo/shared_prefs/app_usage_stats.xml PPLICATIONS /data/com.android.providers.calendar/databases/calendar.db /data/com.android.providers.contacts/databases/calllog.db /data/com.android.providers.contacts/databases/calllog.db /data/com.android.providers.contacts/databases/contacts2.db	* calls calls contacts and raw contacts	Application Usage Report Calendar Items Call Logs [Up to Android 6] Call Logs [From Android 7] Contacts
Userdata Userdata Userdata Userdata Userdata	/data/com.android.providers.downloads/databases/downloads.db /data/com.google.android.gms/databases/android_pay /data/com.google.android.gms/databases/icing_contacts.db /data/com.google.android.gms/databases/icing_mmssms.db /data/com.google.android.gms/databases/ipa_mmssms.db	contacts and raw contacts * wallet *	Downloads Android Pay Contacts SMS/MMS [Up to Android 11] MMS/SMS
Userdata Userdata Userdata Userdata Userdata	/property/persistent_properties /misc/bootstat/factory_reset /misc/bootstat/last_boot_time_utc	N/A N/A N/A	Reboot, Factory Reset Check modified timestamp Check modified timestamp Only Sameura devices
Userdata Userdata Userdata Userdata	/system/user/service/data/eRR.p /data/com.android.providers.media/databases/internal.db /data/com.samsung.android.forest/databases/dwbCommon.db /data/com.google.android.apps.wellbeing/databases/app_usage	N/A * *	Only Samsung devices Internal system files timestamps Only Samsung devices Digital Wellbeing