# SANS DFIR CURRICULUM

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

#### DIGITAL FORENSICS

INCIDENT RESPONSE & THREAT HUNTING

**FOR528** 

for Incident

**REM: Malware Analysis** 

**Tools & Techniques** 

those with and without attachments.





**GCFE** 



**Analysis & Incident Response** 



**Smartphone Forensic Analysis In-Depth** 

Evidence per Gigabyte

The Most Relevant

for585.com/poster

DFPS\_FOR585\_v3.9\_04-24

FOR585: In-Depth sans.org/for585

**Smartphone Forensic Analysis** 



**Advanced Incident Response, Threat Hunting** & Digital Forensics **GCFA** 



**FOR589** Cybercrime Intelligence





**Enterprise Cloud** 

Forensics &

**Incident Response** 

**Enterprise-Class Incident Response** & Threat Hunting



**FOR572 Advanced Network Forensics:** Ransomware Threat Hunting, Analysis & Responders **Incident Response GNFA** 

**Reverse-Engineering** 

**Malware: Advanced** 

**Code Analysis** 



**LINUX Incident Response and Threat** 



**SEC504** 

**Hacker Tools, Techniques** & Incident Handling

## **SQLite**

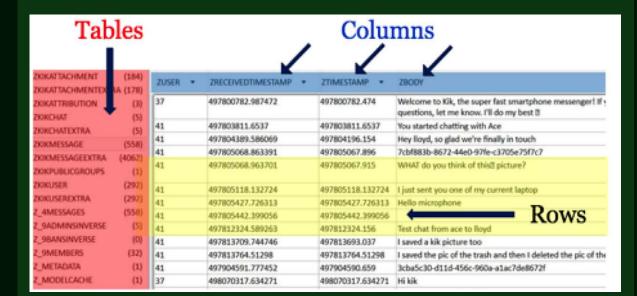
Cyber Threat

Intelligence

**GCTI** 

#### **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).

### **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 digits 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 digits number – number of milliseconds since 01/01/1970 00:00:00):

• SELECT datetime (TS COLUMN/1000, 'unixepoch');

**UNIX Epoch MICROSECONDS** (16 digits number – number of microseconds since 01/01/1970 00:00:00):

• SELECT datetime (TS COLUMN/1000000, 'unixepoch');

Mac Absolute (9 or 18 digits – number of seconds/nanoseconds 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** (17 digits – number of microseconds since 01/01/1601 00:00:00):

• 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'

DFIR-SQL-

SQLECmd

sqlite\_miner

4n6-scripts

**Education and** 

training

Query-Repo

SQLite-Deleted-

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

Apple Pattern of Life Lazy Output'er

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

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

## **Our Favorite Mobile Forensics Resources**

#### Practitioners/Researchers

Sarah Edwards Mattia Epifani Adrian Leong Alexis Brignoni Jon B Mari DeGrazia

**Andrew Hoog** 

Josh Hickman

Scott Koenig

Kevin Pagano

Jessica Hyde

Ian Whiffin

https://www.mac4n6.com Heather Barnhart https://smarterforensics.com https://blog.digital-forensics.it https://abrignoni.blogspot.com https://www.ciofecaforensics.com https://az4n6.blogspot.com https://www.hack42labs.com https://doubleblak.com https://thebinaryhick.blog

http://cheeky4n6monkey.blogspot.com https://theforensicscooter.com https://www.stark4n6.com https://www.hexordia.com/blog-1-1

**Vendors** Oxygen Forensics Magnet Forensics Cellebrite Elcomsoft MSAB Belkasoft

Grayshift Paraben MobilEdit

https://blog.oxygen-forensic.com https://www.magnetforensics.com https://www.cellebrite.com/en/blog Sanderson Forensics https://sqliteforensictoolkit.com/ support-articles

https://blog.elcomsoft.com https://belkasoft.com/articles https://www.grayshift.com https://paraben.com/forensic-impact

https://www.msab.com/resources/blog https://www.mobiledit.com

### **Additional Resources**

DFIR mailing list

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 Group \*access granted to all 585 Alumni

DFIR@lists.sans.org

## **Mobile Malware and Spyware**

Signature-Based

### **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.

**Activities:** One or more activities comprise each application. 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 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. Applications can be programmed to "listen" for events that are 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 ile View Navigation Tools Help 29 Resources ↑ AndroidManifest.xml 🗶 META-INF assets nanifest xmlns:android="http://schemas.android.com/apk/res/android" xmlns:app="http://schem 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"/> firebase-abt.properties <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 suses-permission android:name="android.permission.USE\_BIOMETRIC"/ firebase-iid-interop.properties <uses-permission android:name="android.permission.VIBRATE"/> suses-permission android:name="android.permission.WAKE\_LOCK"/> firebase-iid.properties firebase-measurement-connector-impl.properties <uses-permission android:name="android.permission.WRITE\_SYNC\_SETTINGS"/> suses-permission android:name="com.android.launcher.permission.INSTALL\_SHORTCUT" firebase-measurement-connector.properties suses-permission android:name="android.permission.USE\_FINGERPRINT"/> uses-permission android:name="android.permission.READ\_CALENDAR"/> play-services-ads-identifier.properties suses-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"/s</p> <uses-permission android:name="android.permission.WRITE\_EXTERNAL\_STORAGE"/> play-services-base.properties play-services-basement.properties <uses-permission android:name="com.android.vending.BILLING"/> <uses-permission android:name="android.permission.USE\_CREDENTIALS"/> play-services-drive.properties play-services-gcm.properties suses-permission android:name="android.permission.AUTHENTICATE\_ACCOUNTS"/> play-services-iid.properties

**Specification-Based** 

### **Common Signs and Symptoms**

- Android devices are most at risk for Unexpected device behaviors mobile malware infection
- Dropped calls and call disruptions • Unusually large phone bills

Poor battery life

- Data plan spikes
- Device performance problems Unexplained application errors

**Online Mobile Malware** 

- Unplanned reboots

High-risk user behavior

of the device

- Apps that close or open on their own

• Spyware: Device was out of owner's control

- Risky downloads, browsing or link-clicking

- Spyware installation requires possession

- Unexplained settings changes

- Upload suspicious .apk files to the
- https://www.virustotal.com

https://metadefender.opswat.com

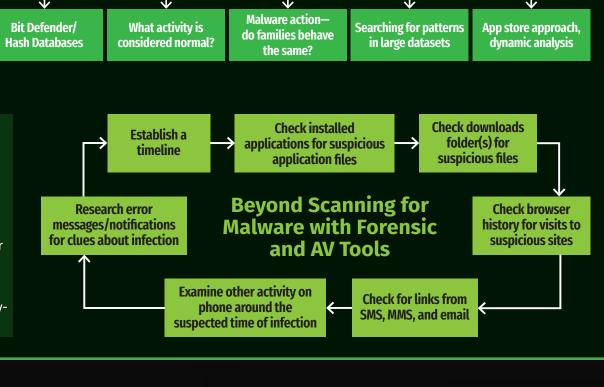
## Sandboxes

- https://www.joesandbox.com
- https://koodous.com
- Internet for online sandbox analysis:
- https://opentip.kaspersky.com

#### **Local Static Malware Analysis** Tools installed on the local machine for mobile

malware analysis: Android SDK https://developer.android.com/studio

- https://github.com/pxb1988/dex2jar • Dex2Jar Drozer https://github.com/WithSecureLabs/drozer JADX https://github.com/skylot/jadx
- JD-GUI https://java-decompiler.github.io/ https://github.com/MobSF/Mobile-Security- MobFs Framework-MobSF



**Mobile Malware Detection** 

**Mobile Malware** 

**Behavioral-Based** 

**Data Mining** 

**Cloud-Based** 

# **Free Scripts and Helpful Utilities**

https://github.com/mac4n6/APOLLO

iOS Logs, Events, And Properties Parser https://github.com/abrignoni/iLEAPP iOS-Mobile-InstallationiOS installation and uninstallation https://github.com/abrignoni/iOS-Mobile-Installation-Logs-Parser Logs-Parser log parser iOS Triage Incident response tool for iOS devices https://github.com/RealityNet/ios\_triage Converts plist files to json, dot notation or csv https://www.hack42labs.com/tools/fplist/details iOS\_sysdiagnose\_ Scripts for parsing various iOS https://github.com/cheeky4n6monkey/iOS\_ forensic\_scripts sysdiagnose logs sysdiagnose\_forensic\_scripts libimobiledevice https://www.libimobiledevice.org https://doubleblak.com/app.php?id=ArtEx2 ArtEx Hexordia Evanole https://www.hexordia.com/evanolece iOS Unified Logs collector https://www.ios-unifiedlogs.com/downloads **ALEAPP** Android Logs Events & Protobuf Parser https://github.com/abrignoni/ALEAPP Parser for Android Usagestats files in Android Usagestats https://github.com/abrignoni/ xml or protobuf format Android-Usagestats-XML-Protobuf https://www.hack42labs.com/tools/ftree/details Identifies, hashes and destructures all files recursively from any file system **FAPK** Extracts apk files from an Android device https://www.hack42labs.com/tools/fapk Andriller https://github.com/den4uk/andriller **Android Triage** https://github.com/RealityNet/android\_triage **Avilla Forensics** https://github.com/AvillaDaniel/AvillaForensics Mobile Revelator https://github.com/bkerler/MR/tree/master/ MobileRevelator

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 SQL query templates for digital https://github.com/abrignoni/DFIR-SQL-Query-Repo

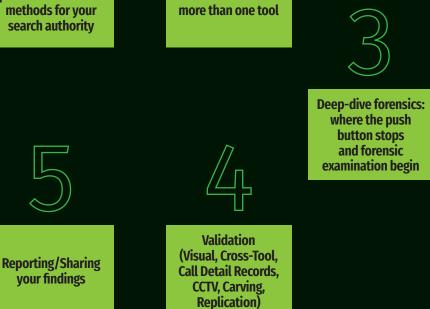
Collection of forensic and third-party scripts https://github.com/cheeky4n6monkey/4n6-scripts

https://github.com/mdegrazia/SQLite-Deleted-

https://github.com/EricZimmerman/SQLECmd

https://github.com/threeplanetssoftware/





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

Mattia Epifani mattia.epifani@realitynet.it @mattiaep

©2024 Heather Barnhart, Domenica "Lee" Crognale, and Mattia Epifani. All Rights Reserved.

-00				
105	lea	1e	<b>e</b>	

iOS Cheatsheet	Description	neu nul	C. P	5.4		
Path  DEVICE INFORMATION  /private/var/containers/Data/System/ <guid>/Library/activation_records/activation_record.plist /private/var/containers/Shared/SystemGroup/sGUID&gt;/Library/Caches/com apple Isdidentifiers plist</guid>	Retail name, Serial Number, UDID Advertising ID	N N N	Sysdiagnose N	/private/var/	RKS AND CONNECTIONS  (containers/Shared/SystemGroup/ <guid>/Library/Database/com.apple.MobileBluetooth.ledevicontainers/Shared/SystemGroup/<guid>/Library/Database/com.apple.MobileBluetooth.ledevicontainers/Shared/SystemGroup/<guid>/Library/Database/com.apple.MobileBluetooth.ledevicontainers/Shared/SystemGroup/</guid></guid></guid>	vices.other.db S
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Caches/com.apple.lsdidentifiers.plist /private/var/installd/Library/MobileInstallation/LastBuildInfo.plist /private/var/mobile/Library/Health/healthdb_secure.sqlite /private/var/mobile/Library/Logs/mobileactivationd/</guid>	iOS and Build Version Historically used devices and iOS version info UDID, Serial Number, IMEI	Y N N Y Y N	N N Y	/private/var/ /private/var/ /private/var/	/containers/Shared/SystemGroup/ <guid>/Library/Preferences/com.apple.MobileBluetooth /db/dhcpclient/leases/ /db/dhcpd_leases</guid>	n.devices.plist Po
/private/var/mobile/Library/Preferences/com.apple.aggregated.plist /private/var/mobile/Library/Preferences/com.apple.itunescloud.plist /private/var/mobile/Library/Preferences/com.apple.sharingd.plist /private/var/preferences/SystemConfiguration/NetworkInterfaces.plist	Last Boot Time DSID Airdrop ID Wi-Fi Mac Addresses	Y Y Y Y Y Y Y Y Y Y N	N N N Y	/private/var /private/var /private/var	/mobile/Library/Biome/sync/sync.db /mobile/Library/Caches/com.apple.findmy.fmipcore/Devices.data /mobile/Library/Caches/com.apple.findmy.fmipcore/FamilyMembers.data /mobile/Library/Caches/com.apple.findmy.fmipcore/Items.data	S! Fi Fi Fi
/private/var/preferences/SystemConfiguration/preferences.plist /private/var/root/Library/Lockdown/data_ark.plist /private/var/root/Library/Lockdown/escrow_records/ /private/var/root/Library/Lockdown/pair_records/	Model, Retail Name, Model number, Model identifier iOS version and device phone name Computer Trust/Pair certificates Computer Trust/Pair certificates	Y Y Y N Y N Y N Y N	N N N	/private/var	/mobile/Library/Caches/com.apple.findmy.fmipcore/Owner.data /mobile/Library/DeviceRegistry.state/historySecureProperties.plist /mobile/Library/DeviceRegistry/ <guid>/</guid>	Fi A
/private/var/wireless/Library/Databases/CellularUsage.db /private/var/wireless/Library/Preferences/com.apple.commcenter.data.plist /private/var/wireless/Library/Preferences/com.apple.commcenter.device_specfic_nobackup.plist /private/var/wireless/Library/Preferences/com.apple.commcenter.plist	SIMs used in device, including most recent ICCID(s) and Phone Number(s) IMEI ICCID(s), IMSI(s) and Phone Number(s)	Y Y Y Y Y Y N Y Y	N N N	/private/var /private/var /private/var	/mobile/Library/DeviceRegistry/ <guid>/NanoAppRegistry/Applications/ /mobile/Library/DeviceRegistry/<guid>/NanoMail/registry.sqlite /mobile/Library/DeviceRegistry/<guid>/NanoPasses/nanopasses.sqlite3 /mobile/Library/DeviceRegistry/<guid>/NanoPreferencesSync/Backup/Files/</guid></guid></guid></guid>	Α Α Α
/System/Library/CoreServices/SystemVersion.plist  SYSTEM SETTINGS /private/var/containers/Shared/SystemGroup/systemgroup.com.apple.configurationprofiles/Library/ConfigurationProfiles/	System Version  Cloud configuration	Y Y N	Y N	/private/var /private/var /private/var	/mobile/Library/Health/NanoSync/com.apple.private.alloy.health.sync.db /mobile/Library/homed/datastore.sqlite /mobile/Library/NanoBackup/	A A A
CloudConfigurationDetails.plist /private/var/db/timezone/localtime /private/var/mobile/Library/ControlCenter/ModuleConfiguration.plist /private/var/mobile/Library/DoNotDisturb/DB/Settings.sqlite	Timezone Control Center settings Do not disturb settings	Y Y Y Y	N N	/private/var /private/var /private/var	/mobile/Library/NanoPreferencesSync/ /mobile/Library/NanoTimeKit/ /mobile/Library/Preferences/com.apple.carplay.plist /mobile/Library/Preferences/com.apple.CarPlayApp.plist	A A A A
/private/var/mobile/Library/Preferences/ /private/var/mobile/Library/Preferences/.GlobalPreferences.plist /private/var/mobile/Library/Preferences/com.apple.AppStore.plist	Examine plists for more information Language, locale and keyboards Timezone	Y Y Y Y	N N	/private/var /private/var /private/var	/mobile/Library/Springboard/ <guid>-CarDisplay[Desired]IconState.plist /mobile/Media/iTunesControl/iTunes/iTunesPrefs /networkd/netusage.sqlite /preferences/com.apple.networkextension.plist</guid>	A L N
/private/var/mobile/Library/Preferences/com.apple.assistant.backedup.plist /private/var/mobile/Library/Preferences/com.apple.atc.plist /private/var/mobile/Library/Preferences/com.apple.BatteryCenter.BatteryWidget.plist /private/var/mobile/Library/Preferences/com.apple.camera.plist	Siri and cloud sync settings Disk usage Battery icon status Camera settings	Y Y Y Y Y N Y Y Y	N N N	/private/var /private/var /private/var	/preferences/com.apple.wifi.known-networks.plist /preferences/systemConfiguration/com.apple.wifi.plist /preferences/SystemConfiguration/com.apple.wifi-private-mac-networks.plist /preferences/SystemConfiguration/preferences.plist	W W
/private/var/mobile/Library/Preferences/com.apple.cloud.quota.plist /private/var/mobile/Library/Preferences/com.apple.cloudphotod.plist /private/var/mobile/Library/Preferences/com.apple.coreduetd.batterysaver.state.plist /private/var/mobile/Library/Preferences/com.apple.Home.ControlCenter.plist	iCloud quota information Cloud photo sync information Battery Saver state Control Center settings	Y Y Y Y Y N N N	N N N	/private/var /private/var /private/var	/root/Library/Application Support/com.apple.wifianalyticsd/DeviceAnalyticsModel.sqlite /root/Library/Application Support/WiFiNetworkStoreModel.sqlite /root/Library/Caches/com.apple.wifid/ThreeBars.sglite	VV VV V
/private/var/mobile/Library/Preferences/com.apple.imservice* /private/var/mobile/Library/Preferences/com.apple.mobile.ldbackup.plist /private/var/mobile/Library/Preferences/com.apple.MobileBackup.plist	SMS, iMessage and FaceTime settings Last iTunes and last iCloud backup date and timezone Backup information	Y Y Y Y Y Y	N N N	/private/var	/root/Library/Preferences/com.apple.preferences.network.plist /wireless/Library/Databases/DataUsage.sqlite /wireless/Library/Preferences/com.apple.CommCenter.counts.plist	W N D
/private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist /private/var/mobile/Library/Preferences/com.apple.mobiletimer.plist /private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist /private/var/mobile/Library/Preferences/com.apple.springboard.plist	SMS/iMessage Settings (time to keep) Time settings Language, country info, device IDs User created restrictions/remote wipe settings	Y Y Y Y Y Y Y Y Y Y	N N N N	Λn	droid Cheatsheet	
/private/var/mobile/Library/SpringBoard/HomeBackground.cpbitmap /private/var/mobile/Library/SpringBoard/HomeBackgroundThumbnail.jpg /private/var/mobile/Library/SpringBoard/IconState.plist /private/var/mobile/Library/SpringBoard/LockBackground.cpbitmap	Wallpaper Wallpaper Homescreen icon layout Wallpaper	Y Y Y Y Y Y Y Y Y	N N N	Partition		e Format Des
/private/var/mobile/Library/SpringBoard/LockBackgroundThumbnail.jpg /private/var/mobile/Library/SpringBoard/LockBackgroundThumbnaildark.jpg /private/var/mobile/Library/SpringBoard/TodayViewArchive.plist /private/var/preferences/SystemConfiguration/com.apple.radios.plist	Wallpaper Wallpaper Today View and Widgets Airplane mode (on/off)	Y Y Y Y Y Y Y Y	N N N	System Userdata	NFORMATION /build.prop TXI /data/com.google.android.gms/databases/constellation.db SQ	Lite IMSI
/private/var/root/Library/Preferences/com.apple.preferences.network.plist  PASSWORD AND ACCOUNT INFORMATION /private/var/Keychains/	Airplane mode (on/off)/Wi-Fi (on/off)  iOS Keychain	Y Y	N N	Userdata Userdata Userdata	/data/com.google.android.gms/shared_prefs/Checkin.xml       XM         /data/com.google.android.gsf/databases/gservices.db       SQ         /property/persistent_properties       TXT	Lite Fitne T Time
/private/var/mobile/Library/Accounts/Accounts3.sqlite /private/var/mobile/Library/MedicalID/MedicalIDData.Archive /private/var/mobile/Library/Preferences/com.apple.corerecents.recentsd.plist /private/var/mobile/Library/Preferences/com.apple.homesharing.plist	Account information  Medical information (bloodtype, organ donor, name, DOB, etc.)  iCloud account ID and login information  iCloud account information	Y Y Y Y Y Y Y Y	N N N	Userdata Userdata Userdata	/system/netpolicy.xml XM	NL Pass Lite Lock NL Time
/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	iCloud account information, Find My iPhone settings and history of iOS versions Profiles and restrictions Account information	Y Y Y Y Y Y	N N N	Userdata Userdata Userdata	/system/users/ <usernumber>/settings_global.xml AB: /system/users/<usernumber>/settings_secure.xml AB: /system/users/<usernumber>/settings_system.xml AB:</usernumber></usernumber></usernumber>	X Glob X Secu
/private/var/wireless/Library/preferences/com.apple.commcenter.callservices.plist  INSTALLED APPLICATIONS /private/installd/Library/Logs/MobileInstallation/mobile_installation.log.* /private/var/containers/Bundle/Application/	Last iCloud account  Mobile Applications Installation Logs Bundle Folders	Y N	Y N	SYSTEM Userdata Userdata	SETTINGS /data/com.google.android.gms/shared_prefs/* /data/com.google.android.gsf/databases/googlesettings.db SQ	rious Pref Lite Goo
/private/var/mobile/Containers/Data/Application/ /private/var/mobile/Containers/Shared/AppGroup/ /private/var/mobile/Library/Caches/com.apple.appstored/StoreUser.db	Application Data folder Application Shared folder iCloud User App Library	Y Y Y Y N N	N N N N	Userdata Userdata Userdata Userdata	/data/com.google.android.gsf/databases/gservices.db       SQ         /system/notification_policy.xml       AB;         /system/users/ <usernumber>/settings_global.xml       AB;         /system/users/<usernumber>/settings_secure.xml       AB;</usernumber></usernumber>	Lite Fitne X Noti X Glob
/private/var/mobile/Library/FrontBoard/applicationState.db /private/var/mobile/Library/TCC/TCC.db /private/var/root/Library/MobileContainerManager/containers.sqlite3	Installed applications Applications permissions Installed Applications	Y Y Y Y Y Y N	N Y N	Userdata PASSWO Userdata	/system/users/ <usernumber>/settings_system.xml AB:  RDS AND ACCOUNT INFORMATION /data/com.android.providers.contacts/databases/contacts2.db SQ</usernumber>	X Syst
NATIVE APPS /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/WebKit/NetworkCache/</apple></apple></apple>	Safari Cache files Safari Cache database Safari WebKit Cache	N N N N N N N	N N N	Userdata Userdata Userdata Userdata	/data/com.android.vending/shared_prefs/lastaccount.xml     XM       /data/com.google.android.gms/databases/google_account_history.db     SQ       /data/com.google.android.gms/shared_prefs/BackupAccount.xml     XM       /data/com.google.android.gsf/databases/gservices.db     SQ	IL Last Lite Goo IL Back Lite Fitne
/private/var/mobile/Containers/Data/Application/ <apple guid="" safari="">/Library/Cookies/Cookies.binarycookies /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/Image Cache/Favicons/ /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/Preferences/com.apple.mobilesafari.plist /private/var/mobile/Containers/Data/Application/<apple guid="" safari="">/Library/Safari/Downloads/Downloads.plist</apple></apple></apple></apple>	Safari Cookies Safari Website favicons Safari Configuration Safari Download History	N Y N N N Y	N N N	Userdata Userdata Userdata	/system/sync/accounts.xml AB; /system/sync/accounts.xml AB; /system/users/ <usernumber>.xml AB;</usernumber>	X Acco X Syno
/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/Containers/Shared/AppGroup/<apple_files_guid>/smartfolders.db</apple_files_guid></apple></apple>	Safari Tabs Screenshots (PNG or KTX format) Safari WebKit Localstorage Apple Files	N Y Y Y N Y	N N N	Userdata INSTALLI Userdata	/system_de/ <usernumber>/accounts_de.db SQ ED APPLICATIONS /app/* API</usernumber>	Lite Acco
/private/var/mobile/Containers/Shared/AppGroup/ <apple_notes_guid>/NoteStore.sqlite /private/var/mobile/Library/AddressBook/AddressBook.sqlitedb /private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb /private/var/mobile/Library/Application Support/CloudDocs/session/db/client.db</apple_notes_guid>	iCloud Notes Contacts Contact Images Apple Files	N Y N Y N N N	N N N N	Userdata Usredata Userdata Userdata	/dalvik-cache Var /data/ <application_sandbox> Var /data/com.android.vending/databases/auto_update.db SQ /data/com.android.vending/databases/frosting.db SQ</application_sandbox>	rious .dex rious App Lite Pack Lite Trac
/private/var/mobile/Library/Application Support/CloudDocs/session/db/server.db /private/var/mobile/Library/Application Support/FileProvider/backup/backup_manifest.db /private/var/mobile/Library/Calendar/Calendar.sqlitedb /private/var/mobile/Library/Calendar/Extras.db	Apple Files iCloud Documents details Calendar Extras for Calendar	N N N N N N Y Y	N N N	Userdata Userdata	/data/com.android.vending/databases/install_queue.db SQ /data/com.android.vending/databases/library.db SQ	Lite Iraci Lite Insta Lite Cont Lite Trac
/private/var/mobile/Library/Calendar/Notifications.Calendar.Protected /private/var/mobile/Library/CallHistoryDB/CallHistory.storedata /private/var/mobile/Library/CallHistoryDB/CallHistoryTemp.storedata	Calendar entries Call History Call History Temporary storage (Before First Unlock)	Y N N Y Y N	N N N	Userdata Userdata	/data/com.android.vending/databases/verify_apps.db SQ /data/com.android.vending/databases/xternal_referrer_status.db SQ	(no OLite Keyv OLite Insta OLite Insta
/private/var/mobile/Library/CallHistoryTransactions/ <guid>.log /private/var/mobile/Library/com.apple.siri.inference/siriremembers.sqlite3 /private/var/mobile/Library/DuetExpertCenter/ /private/var/mobile/Library/Health/ActivitySharing/contacts2.dat</guid>	Call log traces Siri Remembers User Notifications Apple Health Fitness Friends	N N N N N N N N	N N N N	Userdata	/data/com.google.android.gms/databases/gass.db SQ /misc_de/ <usernumber>/apexdata/com.android.permission/roles.xml XM /misc_de/<usernumber>/apexdata/com.android.permission/runtime-permissions.xml XM</usernumber></usernumber>	IL Dan
/private/var/mobile/Library/Health/healtdb.sqlite /private/var/mobile/Library/Health/healtdb_secure.sqlite /private/var/mobile/Library/Keyboard/ <language>-dynamic.lm/dynamic.dat /private/var/mobile/Library/Keyboard/<language>-dynamic.lm/dynamic-lexicon.dat</language></language>	Apple Health Apple Health Auto correction/Predictive text Auto correction/Predictive text	N Y N Y N N	N N N	Userdata Userdata	/system/packages.list TXI /system/packages.xml AB: /system/packages-cstats.list TXI	(fo T Inst X Inst
/private/var/mobile/Library/Reyboard/UserDictionary.sqlite /private/var/mobile/Library/Mail/ /private/var/mobile/Library/Mail/Envelope Index /private/var/mobile/Library/Mail/Protected Index	User created auto-correct Mail and settings Mail database Mail database	N N N N N N N N N N N N N N N N N N N	N N N	NATIVE A	APPS /data/com.android.providers.calendar/databases/calendar.db SQ	ev Lite Cale
/private/var/mobile/Library/Notes/notes.sqlite /private/var/mobile/Library/Passes/Cards/ /private/var/mobile/Library/Passes/passes23.sqlite	Notes Apple Pay Credit Cards Apple Passes	N Y N N N N Y	N N N	Userdata Userdata Userdata Userdata	/data/com.android.providers.contacts/databases/calllog.db       SQ         /data/com.android.providers.contacts/databases/contacts2.db       SQ         /data/com.android.providers.downloads/databases/downloads.db       SQ         /data/com.android.providers.telephony/databases/mmssms.db       SQ	Lite Call Lite Cont Lite Dow Lite SMS
/private/var/mobile/Library/Preferences/com.apple.cmfsyncagent.plist /private/var/mobile/Library/Preferences/com.apple.identityservices.idstatuscache.plist /private/var/mobile/Library/Preferences/com.apple.madrid.plist /private/var/mobile/Library/Preferences/com.apple.mobilenotes.plist	Blocked Dialers iCloud sync, Email, FaceTime, Email, more SMS, iMessage and FaceTime Notes	Y Y Y Y Y Y Y Y Y	N N N	Userdata Userdata Userdata Userdata	/data/com.android.providers.userdictionary/databases/user_dict.db     SQ       /data/com.google.android.gms/databases/android_pay     SQ       /data/com.google.android.gms/databases/icing_contacts.db     SQ       /data/com.google.android.gms/databases/icing_mmssms.db     SQ	Lite User Lite And Lite Conf Lite SMS
/private/var/mobile/Library/Preferences/com.apple.mobilephone.* /private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist /private/var/mobile/Library/Recents/Recents /private/var/mobile/Library/Reminders/	List of contacts added to the phone application's favorites list SMS, iMessage and FaceTime Recents communications Reminders	N Y Y Y N Y	N N N	Userdata Userdata GOOGLE	/data/com.sec.android.provider.logsprovider/databases/logs.db SQ /data/user_de/ <usernumber>/com.android.providers.telephony/app_parts Var APPS</usernumber>	Lite Call rious MMS
/private/var/mobile/Library/Safari/Bookmarks.db /private/var/mobile/Library/Safari/BrowserState.db /private/var/mobile/Library/Safari/CloudTabs.db	Safari Bookmarks Safari Suspended State Tab Safari Cloud Tabs	N Y N Y N N	N N N	Userdata Userdata Userdata	/data/com.google.android.apps.docs/databases/DocList.db SQ /data/com.google.android.apps.dynamite/dynamite.db SQ /data/com.google.android.apps.messaging/databases/annotaded_call_log.db SQ	Lite Goo Lite Goo Lite Goo Lite Pho
/private/var/mobile/Library/Safari/History.db /private/var/mobile/Library/Safari/SafariTabs.db /private/var/mobile/Library/SMS/Attachments/ /private/var/mobile/Library/SMS/Drafts/	Safari History Safari Tabs MMS File SMS/MMS Drafts	N Y N Y N Y N Y	N N N N	Userdata Userdata Userdata	/data/com.google.android.apps.messaging/databases/bugle_db SQ /data/com.google.android.apps.messaging/databases/phone_lookup_history.db SQ /data/com.google.android.apps.nbu.files/databases/files_master_database SQ	Lite Goo Lite Pho Lite Files Lite Goo
/private/var/mobile/Library/SMS/sms.db /private/var/mobile/Library/SMS/sms-temp.db /private/var/mobile/Library/UserNotifications/ /private/var/mobile/Library/Voicemail/voicemail.db	SMS/MMS messages SMS Temporary storage (Before First Unlock) User Notifications Voicemail	N Y Y N Y Y Y Y	N N N	Userdata Userdata Userdata	/data/com.google.android.apps.tachyon/databases/tachyon.dbSQ/data/com.google.android.calendar/databases/cal_v2aSQ/data/com.google.android.dialer/databases/dialer.dbSQ	Lite Goo Lite Goo Lite Pho Lite Goo
APPLICATION USAGE  *.ktx /Library/LaunchAgents/	Application Snapshots Launch Agents	N N N	N N	Userdata Userdata Userdata	/data/com.google.android.googlequicksearchbox/app_session Var /data/com.google.android.googlequicksearchbox/files/recently Var /data/com.google.android.inputmethod.latin/databases/trainingcachev3.db SQ	rious Goo rious Goo Lite Gbo Lite Goo
/Library/LaunchDaemons/ /private/var/containers/Shared/SystemGroup/ <guid>/Library/BatteryLife/CurrentPowerLog.PLSQL /private/var/db/biome/ /private/var/mobile/Library/AggregatedDictionary/ADDataStore.sqlitedb</guid>	Launch Daemons Battery life tracker Biome (Suggestions) Aggregated Dictionary	N N N N N N Y N	N Y N N	APPLICA Userdata Userdata	TION USAGE /data/com.android.vending/databases/data_usage.db SQ /data/com.android.vending/databases/notification_cache SQ	Lite App Lite App
/private/var/mobile/Library/Application Support/com.apple.remotemanagmentd/RMAdminStore-Cloud.sqlite /private/var/mobile/Library/Application Support/com.apple.remotemanagmentd/RMAdminStore-Local.sqlite /private/var/mobile/Library/Assistant/knowledgeC.db /private/var/mobile/Library/Biome/	Screen time Screen time Application traces Biome (Suggestions)	N N N N N N	N N N	Userdata Userdata Userdata	/data/com.google.android.apps.turbo/databases/battery_health.db     SQ       /data/com.google.android.apps.turbo/databases/turbo.db     SQ       /data/com.google.android.apps.turbo/sahred_prefs/app_usage_stats.xml     XM	Lite Chai Lite Batt
/private/var/mobile/Library/BulletinBoard/ClearedSections.plist /private/var/mobile/Library/Caches/com.apple.Pasteboard/ /private/var/mobile/Library/com.apple.itunesstored/itunesstored2.sqlitedb	Logs of cleared notifications Pasteboard Application traces	Y Y Y N N Y Y	N N N	Userdata Userdata Userdata	/data/com.google.android.as/databases/cell_dbSQ/data/com.google.android.as/databases/echo_dbSQ/data/com.google.android.as/databases/nasa_ps.dbSQ	Lite App Lite App Lite App Lite App
/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/Keyboard/app_usage_database.plist	Installed Applications Application traces Application traces Keyboard Application Usage	N N N Y N N	N N N N	Userdata Userdata Userdata	/data/com.google.android.as/databases/SimpleStorage     SQ       /data/com.google.android.as/databases/smartselect_db     SQ       /data/com.google.android.gms/databases/ns.db     SQ	Lite And Lite App Lite App
/private/var/mobile/Library/Keyboard/langlikelihood.dat /private/var/mobile/Library/Logs/CrashReporter/*.ips /private/var/mobile/Library/Preferences/com.apple.corespotlightui.plist /private/var/mobile/Library/Preferences/com.apple.mt.lastLaunch.plist	Application traces Crash Logs Application traces Application Execution Traces	Y Y Y N Y Y N Y Y Y Y Y Y Y Y Y Y Y Y Y	N Y N	Userdata Userdata Userdata	/data/com.google.android.gms/files/fcm_queued_messages.ldb Lev /data/com.google.android.settings.intelligence/databases/battery-usage-db-v <number> SQ /data/com.samsung.android.forest/databases/dwbCommon.db SQ</number>	Lite App velDB Firel Lite Batt Lite Digit
/private/var/networkd/netusage.sqlite /private/var/wireless/Library/Databases/DataUsage.sqlite  MULTIMEDIA	Network data usage per App Application traces	N N Y Y	N N	Userdata Userdata Userdata Userdata	/data/com.samsung.android.providers.context/databases/ContextLog_0.db     SQ       /data/com.sec.android.app.launcher/databases/launcher.db     SQ       /data/semclipboard     /system/appops.xml	Lite App Lite App Clipl X App
/private/var/mobile/Library/Preferences/com.apple.mobileslideshow.plist /private/var/mobile/Media/DCIM/1*APPLE /private/var/mobile/Media/iTunes_Control/iTunes/MediaLibrary.sqlitedb /private/var/mobile/Media/MediaAnalysis/mediaanalysis.db	Photos (Download and Keep Originals) User Created/Saved Photos iTunes Media Library Media analysis and classification	Y Y Y Y Y Y N Y	N N N	Userdata Userdata Userdata Userdata	/system/appops/discrete AB/ /system/appops_accesses.xml AB/ /system/battery-history/ /system/batterystats.bin	X Priva X App Batt Batt
/private/var/mobile/Media/PhotoData/AlbumsMetadata/ /private/var/mobile/Media/PhotoData/CPL/ /private/var/mobile/Media/PhotoData/CPL/syncstatus.plist	Photo Albums Metadata Cloud Photo Library iCloud Photo Library Exists	N Y N Y N Y	N N N	Userdata Userdata Userdata	/system/batterystats-checkin.bin /system/batterystats-daily.xml AB/ /system/battery-usage-stats/	Batt
/private/var/mobile/Media/PhotoData/Mutuations/ /private/var/mobile/Media/PhotoData/Photos.sqlite /private/var/mobile/Media/PhotoData/private/com.apple.accountsd/cloudServiceEnableLog.plist /private/var/mobile/Media/PhotoData/Thumbnails/*.ithmb	Photo mutuations Photos/Videos Database iCloud Photos and Shared Albums Enabled Thumbnails databases	N Y N Y N Y N Y	N N N N	Userdata Userdata Userdata	/system/graphicsstats/ /system/job/jobs_ <uid>.xml AB/ /system/notification_log.db SQ</uid>	Grap X App Lite App
/private/var/mobile/Media/PhotoData/Thumbnails/V2/ /private/var/mobile/Media/Recordings/ LOCATION ARTIFACTS	Photos saved from Live Video and SMS photo capture Voice Memos	N Y Y	N N	Userdata Userdata Userdata	/system/procstats /system/shutdown-checkpoints TXI /system/users/ <local_user_number>/app_idle_stats.xml XM</local_user_number>	NL App
/private/var/mobile/Containers/Data/Application/ <apple_maps_guid>/Library/Maps/Pins.metadata /private/var/mobile/Containers/Data/Application/<apple_maps_guid>/Library/Preferences/com.apple.Maps.plist /private/var/mobile/Containers/Shared/AppGroup/<apple_maps_guid>/Maps/MapsSync_0.0.1 /private/var/mobile/Library/Caches/com.apple.geod/AP.db</apple_maps_guid></apple_maps_guid></apple_maps_guid>	Pinned locations Last latitude and longitude, map search history Apple Maps history Geolocation Report (Application)	N N Y Y N N N	N N N	Userdata Userdata Userdata Userdata	/system_ce/ <usernumber>/notifcation_history/history /system_ce/<usernumber>/recent_images/*.png /system_ce/<usernumber>/recent_tasks/*.xml /system_ce/<usernumber>/shortcut_service/bitmaps/ PN</usernumber></usernumber></usernumber></usernumber>	otobuf Noti IG App NL Rece IG App
/private/var/mobile/Library/Caches/com.apple.geod/MapTiles/MapTiles.sqlitedb /private/var/mobile/Library/Caches/com.apple.geod/PDPlaceCache.db /private/var/mobile/Library/Caches/com.apple.routined/Cache.sqlite	Map Tiles Cache PD Place Cache Cached locations Significant Location	N N N N N N N N N N N N N N N N N N N	N N N	Userdata Userdata Userdata	/system_ce/ <usernumber>/shortcut_service/packages/ /system_ce/<usernumber>/snapshots/*.jpg /system_ce/<usernumber>/usagestats/</usernumber></usernumber></usernumber>	X App
/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	Significant Location Personalization Portrait "Location Services" setting (Enabled = 1; Disabled = 0)	N N N N Y Y Y	N N N	Userdata Userdata Userdata	/data/com.google.android.gms/databases/herrevad SQ /data/com.google.android.gms/databases/personalsafety_db SQ	Lite Cast Lite Wire Lite And
/private/var/mobile/Media/PhotoData/Caches/GraphService/CLSPublicEventCache.sqlite /private/var/mobile/Media/PhotoData/Caches/GraphService/PhotosGraph/photosgraph.kgdb /private/var/mobile/Media/PhotoData/Photos.sqlite /private/var/root/Library/Caches/locationd/cache_encryptedB.db	Queried events Photo Analytics Photos/Videos Database Cell Towers/Wi-Fi Locations	N Y Y N Y N N N	N N N	Userdata Userdata Userdata Userdata	/data/com.google.android.gms/shared_prefs/nearbysharing:service:state.xml XM /log/wifi/iwc/iwc_dump.txt TXI /misc/adb/adb_keys TXI /misc/apexdata/com.android.wifi/WiFiConfigStore.xml XM	NL Nea T Wire T Com
/private/var/root/Library/Caches/locationd/cache_encryptedC.db /private/var/root/Library/Caches/locationd/clients.plist /private/var/root/Library/Caches/locationd/consolidated.db	Motion State History/Step Count Application using location services Application Traces and GeoFence information	N N Y Y Y Y	N N N	Userdata Userdata	/misc/apexdata/com.android.wifi/WiFiConfigStoreSoftAp.xml XM /misc/apexdata/com.android.wifi/WiFiConfigStoreSoftAp.xml XM /misc/bluedroid/bt_config.conf TXI /misc/bluedroiddump/mainBuffer.log TXI	NL Info T Info Bl
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 /private/var/containers/Shared/SystemGroup/<guid>/Library/Preferences/com.apple.MobileBluetooth.devices.plist</guid></guid></guid>	Seen Bluetooth devices Paired Bluetooth devices Paired Bluetooth devices	N Y Y Y N Y	N N N	Userdata Userdata <b>MULTIME</b>	/misc/wifi/WifiConfigStore.xml XM /system/wifigeofence.db SQ EDIA	NL Wire Lite Wi-I
/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	Cloud Documents details iClould offline cache Apple Watch pairing information Apple Watch information (also previously paired Apple Watch)	N N Y Y Y Y	N N N	Userdata Userdata Userdata Userdata	/data/com.google.android.apps.maps/databases/ugc_photos_location_data.db     SQ       /data/com.google.android.apps.photos/databases/gphotos <number>.db     SQ       /data/com.google.android.providers.media.module/databases/external.db     SQ       /data/com.samsung.android.providers.media/databases/media.db     SQ</number>	Lite Pho Lite Goo Lite Trac Lite Med
/private/var/mobile/Library/DeviceRegistry.state/stateMachine- <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) Apple Watch data Apple Watch Applications	N Y Y Y Y Y	N N N	Userdata Userdata Userdata	/data/com.samsung.cmh/databases/cmh.db     SQ       /data/com.samsung.storyservice/databases/dme.db     SQ	Lite Cam Lite Sam Lite Cam
/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</guid></guid></guid>	Apple Watch Mail application Apple Watch Wallet Passes Apple Watch Faces Apple Watch Health data sync	Y Y Y Y Y Y Y N Y	N N N	LOCATIO Userdata Userdata	NATIFACTS /data/com.google.android.apps.maps/app_tts-temp/tts-%UNIXEPOCH% /data/com.google.android.apps.maps/databases/gmm myplaces.db SO	
/private/var/mobile/Library/homed/datastore.sqlite /private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.plist /private/var/mobile/Library/NanoBackup/ /private/var/mobile/Library/NanoMusicSync/	Apple HomeKit Devices Seen Bluetooth devices Apple Watch information Apple Watch information	N Y Y Y Y Y Y Y N	N N N	Userdata Userdata Userdata Userdata	/data/com.google.android.apps.maps/databases/gmm_storage.db SQ /data/com.google.android.apps.maps/databases/gmm_sync.db SQ /data/com.google.android.apps.maps/files/new_recent_history_cache_searches.cs /data/com.google.android.apps.turbo/databases/turbo.db SQ	Lite Sear Lite Favo otobuf Goo Lite Time
/private/var/mobile/Library/NanoPreferencesSync/ /private/var/mobile/Library/NanoTimeKit/ /private/var/mobile/Library/Preferences/com.apple.carplay.plist	Apple Watch information Apple Watch information Apple CarPlay configuration	Y N Y N Y Y	N N N	Userdata Userdata Userdata	/data/com.sec.android.daemonapp/db/weatherClock SQ /log/wifi/iwc/iwc_dump.txt TXT /Media/0/DCIM/Camera *	Lite Whe T Wire EXIF
/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.coreduetd.plist /private/var/mobile/Library/Preferences/com.apple.identityservices.idstatuscache.plist	iCloud quota information Cloud Sync denials and dates sync devices iCloud sync, Email, FaceTime, Email, more	Y Y Y Y Y Y Y Y Y	N N N	<b>DEVICE V</b> Userdata	VIPING/SETUP /data/com.android.providers.media/databases/internal.db SQ	Lite Wi-F Lite Inte Lite Digit
/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</guid>	Last iTunes and last iCloud backup date and timezone. Apple Watch preferences Device AirDrop ID Apple CarPlay per car App Icon configuration	Y Y Y Y Y Y Y Y Y	N N N	Userdata Userdata Userdata	/data/com.samsung.android.forest/databases/dwbCommon.db SQ /data/data/com.google.android.settings.intelligence/shared_prefs/setup_wizard_info.xml XM /data/data/com.google.android.settings.intelligence/shared_prefs/suggestions.xml XM	Lite Digit IL Setu IL Setu
/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 /private/var/wireless/Library/Databases/DataUsage-watch.sqlite</guid>	Apple CarPlay per car App Icon configuration List of computer where the device was connected to Last backup computer, iCloud Backup Settings, Device info Watch Application Usage	Y Y Y N N	N N N	Userdata Userdata	/misc/bootstat/factory_reset /misc/bootstat/last_boot_time_utc /property/persistent_properties /system/user/service/data/eRR.p	Cheo Cheo T Rebo Sam

Path Description	BFU	Backup	Sysdiagnose
NETWORKS AND CONNECTIONS			
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Database/com.apple.MobileBluetooth.ledevices.other.db Seen Bluetooth devices</guid>	N	Υ	N
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db Paired Bluetooth devices</guid>	Y	Ϋ́	N
/private/var/containers/Shared/SystemGroup/ <guid>/Library/Preferences/com.apple.MobileBluetooth.devices.plist Paired Bluetooth devices</guid>	Ň	Ÿ	N
/private/var/db/dhcpclient/leases/	Υ	N	N
/private/var/db/dhcpd_leases DCHP Deamons Lease	N	N	N
/private/var/mobile/Library/Biome/sync/sync.db Synced devices	N	N	N
/private/var/mobile/Library/Caches/com.apple.findmy.fmipcore/Devices.data FindMy Devices	N	N	N
/private/var/mobile/Library/Caches/com.apple.findmy.fmipcore/FamilyMembers.data FindMy Family Members	N	N	N
/private/var/mobile/Library/Caches/com.apple.findmy.fmipcore/Items.data FindMy Items (AirTags)	N	N	N
/private/var/mobile/Library/Caches/com.apple.findmy.fmipcore/Owner.data FindMy Owner	N	N	N
/private/var/mobile/Library/DeviceRegistry.state/historySecureProperties.plist Apple Watch information	N	Υ	N
(also previously paired Apple Watch)			
/private/var/mobile/Library/DeviceRegistry/ <guid>/ Apple Watch data</guid>	Υ	Υ	N
/private/var/mobile/Library/DeviceRegistry/ <guid>/NanoAppRegistry/Applications/ Apple Watch Applications</guid>	Υ	Υ	N
/private/var/mobile/Library/DeviceRegistry/ <guid>/NanoMail/registry.sqlite Apple Watch Mail application</guid>	Υ	Υ	N
/private/var/mobile/Library/DeviceRegistry/ <guid>/NanoPasses/nanopasses.sqlite3 Apple Watch Wallet Passes</guid>	N	Υ	N
/private/var/mobile/Library/DeviceRegistry/ <guid>/NanoPreferencesSync/Backup/Files/ Apple Watch Faces</guid>	Υ	Υ	N
/private/var/mobile/Library/Health/NanoSync/com.apple.private.alloy.health.sync.db Apple Watch Health data sync	N	Υ	N
/private/var/mobile/Library/homed/datastore.sqlite Apple Home information and devices	N	Υ	N
/private/var/mobile/Library/NanoBackup/ Apple Watch information	Υ	Υ	N
/private/var/mobile/Library/NanoPreferencesSync/ Apple Watch information	Υ	N	N
/private/var/mobile/Library/NanoTimeKit/ Apple Watch information	Υ	N	N
/private/var/mobile/Library/Preferences/com.apple.carplay.plist Apple CarPlay configuration	Υ	Υ	N
/private/var/mobile/Library/Preferences/com.apple.CarPlayApp.plist Apple CarPlay configuration	Υ	Υ	N
/private/var/mobile/Library/Springboard/ <guid>-CarDisplay[Desired]IconState.plist Apple CarPlay per car App Icon configuration</guid>	Υ	Υ	N
/private/var/mobile/Media/iTunesControl/iTunes/iTunesPrefs List of computer where the device was connected by the connected by th		Υ	N
/private/var/networkd/netusage.sqlite Network data usage per App	N	N	N
/private/var/preferences/com.apple.networkextension.plist Network Extension	Υ	Υ	N
/private/var/preferences/com.apple.wifi.known-networks.plist Wi-Fi Network List	N	N	Y
/private/var/preferences/SystemConfiguration/com.apple.wifi.plist Wi-Fi Network List (old format)	Y	Υ	Y
/private/var/preferences/SystemConfiguration/com.apple.wifi-private-mac-networks.plist Wi-Fi Network List	Y	Υ	Y
/private/var/preferences/SystemConfiguration/preferences.plist Wi-Fi, VPN, Certs and more	Y	Υ	N
/private/var/root/Library/Application Support/com.apple.wifianalyticsd/DeviceAnalyticsModel.sqlite Wi-Fi information	N	N	N
/private/var/root/Library/Application Support/WiFiNetworkStoreModel.sqlite Wi-Fi information	N	N	N
/private/var/root/Library/Caches/com.apple.wifid/ThreeBars.sqlite Wi-Fi information	N	N	N
/private/var/root/Library/Preferences/com.apple.preferences.network.plist Wi-Fi ON/OFF	Y	Υ	N
/private/var/wireless/Library/Databases/DataUsage.sqlite Network data usage per App	N	Υ	N
/private/var/wireless/Library/Preferences/com.apple.CommCenter.counts.plist Data and Cellular network statistics	Υ	Υ	N

Partition I		File Format	Description
System Userdata	NFORMATION	TXT SQLite SQLite XML SQLite TXT N/A XML SQLite XML SQLite XML SQLite XML ABX ABX ABX SQLite Various SQLite	Device information (version, patches, etc.) IMSI of last used SIM Card Sim card information Activity on device related to installed SIM (ICCID and Google Account included) Fitness settings, network settings, other settings Timezone and local language Files needed for password cracking Passcode requirements and policies. Syncing info may exist Lock settings information Timezone Global settings Secure settings System settings System settings Sim card information  Preference files Google preferences – location, maps, wallet, etc1=true
Userdata Userdata Userdata Userdata Userdata Userdata	/data/com.google.android.gsf/databases/gservices.db /system/notification_policy.xml /system/users/ <usernumber>/settings_global.xml /system/users/<usernumber>/settings_secure.xml /system/users/<usernumber>/settings_system.xml  RDS AND ACCOUNT INFORMATION /data/com.android.providers.contacts/databases/contacts2.db</usernumber></usernumber></usernumber>	SQLite ABX ABX ABX ABX SQLite	Fitness settings, network settings, other settings Notifications settings Global settings Secure Settings System Settings Login info
Userdata	/data/com.android.vending/shared_prefs/lastaccount.xml /data/com.google.android.gms/databases/google_account_history.db /data/com.google.android.gms/shared_prefs/BackupAccount.xml /data/com.google.android.gsf/databases/gservices.db /system/sync/accounts.xml /system/sync/accounts.xml /system/users/ <usernumber>.xml /system_ce/<usernumber>/accounts_ce.db /system_de/<usernumber>/accounts_de.db</usernumber></usernumber></usernumber>	XML SQLite XML SQLite ABX ABX ABX SQLite SQLite	Last account used on Google PlayStore Google account history Backup account email address Fitness settings, network settings, other settings Account sync information Syncing information Local user information and Last loggedin timestamp Accounts with credentials Accounts with creation timestamps
Userdata	/app/* /data/ <application_sandbox> /data/com.android.vending/databases/auto_update.db /data/com.android.vending/databases/frosting.db /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/suggestions.db /data/com.android.vending/databases/verify_apps.db /data/com.android.vending/databases/xternal_referrer_status.db /data/com.google.android.gms/databases/gass.db /misc_de/<usernumber>/apexdata/com.android.permission/roles.xml /misc_de/<usernumber>/apexdata/com.android.permission/runtime-permissions.xml /system/packages.list /system/packages.cstats.list</usernumber></usernumber></application_sandbox>	APK Various Various SQLite XML XML TXT ABX TXT	APK files for installed applications .dex/.oat/.art files for installed applications Application Data Files* Packages set to auto update Tracks the installation and update of applications regardless of how they were installed Installed packages Contains the library of applications for the Google user in use on the device. Tracks applications installed on the device via the Google Play Store (not apps installed by other means) Keywords searched on the Google Play Store Installed packages Installed applications. The information is not removed when an app is uninstalled Tracks applications installed on the device, no matter how they were installed. It stores SHA-256 hash of the last APK. List of applications set by default for certain functions in Android Dangerous permissions information (for each package and each permission, granted true/false) Installed packages (package name, package UID, installer) Installed packages (package manager compiler (it contains references to an application, even after it has been uninstalled)
Userdata	/data/com.android.providers.calendar/databases/calendar.db /data/com.android.providers.contacts/databases/calllog.db /data/com.android.providers.contacts/databases/contacts2.db /data/com.android.providers.downloads/databases/downloads.db /data/com.android.providers.telephony/databases/mmssms.db /data/com.android.providers.userdictionary/databases/user_dict.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.sec.android.provider.logsprovider/databases/logs.db /data/user_de/ <usernumber>/com.android.providers.telephony/app_parts</usernumber>	SQLite Various	Calendar Call logs Contacts Downloads SMS/MMS User dictionary Android Pay Contacts SMS/MMS [Up to Android 11] Call logs [Up to Android 9] MMS Attachments
Userdata	/data/com.google.android.apps.docs.editors.docs/app_cello/email_address>/cello.db /data/com.google.android.apps.docs/databases/DocList.db /data/com.google.android.apps.dynamite/dynamite.db /data/com.google.android.apps.messaging/databases/annotaded_call_log.db /data/com.google.android.apps.messaging/databases/bugle_db /data/com.google.android.apps.messaging/databases/phone_lookup_history.db /data/com.google.android.apps.nbu.files/databases/files_master_database /data/com.google.android.apps.photos/databases/files_master_database /data/com.google.android.apps.photos/databases/gphotos <n>.db /data/com.google.android.calendar/databases/tachyon.db /data/com.google.android.dialer/databases/dialer.db /data/com.google.android.gm/databases/bigTopDataDB.<user-id> /data/com.google.android.googlequicksearchbox/app_session /data/com.google.android.googlequicksearchbox/files/recently /data/com.google.android.inputmethod.latin/databases/trainingcachev3.db /data/com.google.android.keep/databases/keep.db</user-id></n>	SQLite Various Various SQLite SQLite	Google Docs Google Docs Google Chat (formerly Hangouts) Phone by Google Google Android Messaging (including RCS) Phone by Google Files by Google Google Photos Google Photos Google Calendar Phone by Google Google Calendar Phone by Google Google Mail Google Quicksearch – Searches and personal assistant Google Quicksearch – Recent Searches Gboard – Google Keyboard Google Keep
APPLICAT Userdata	TION USAGE  /data/com.android.vending/databases/data_usage.db /data/com.android.vending/databases/notification_cache /data/com.google.android.apps.turbo/databases/battery_health.db /data/com.google.android.apps.turbo/databases/turbo.db /data/com.google.android.apps.turbo/sahred_prefs/app_usage_stats.xml /data/com.google.android.asps.wellbeing/databases/app_usage /data/com.google.android.as/databases/cell_db /data/com.google.android.as/databases/cell_db /data/com.google.android.as/databases/people_search /data/com.google.android.as/databases/simpleStorage /data/com.google.android.as/databases/simpleStorage /data/com.google.android.as/databases/smartselect_db /data/com.google.android.gms/databases/reminders.db /data/com.google.android.gms/files/fcm_queued_messages.ldb /data/com.google.android.settings.intelligence/databases/battery-usage-db-v <number> /data/com.samsung.android.forest/databases/dwbCommon.db /data/com.samsung.android.providers.context/databases/ContextLog_0.db /data/com.sec.android.app.launcher/databases/launcher.db /data/semclipboard</number>	SQLite SQLite SQLite SQLite XML SQLite	Application usage traces Application usage traces Charging sessions, including start timestamp and duration Battery Level Application execution timestamps Digital Wellbeing (Google) Application usage traces Application, User and Location traces Application, User and Location traces Firebase Cloud Messaging Battery Usage [From Android 12] Digital Wellbeing (Samsung devices only) Application traces (only Samsung devices) [Up to Android 10] Application artifacts (even after deleted) Clipboard content (only Samsung devices)
Userdata	/system/appops.xml /system/appops_accesses.xml /system/battery-history/ /system/batterystats.bin /system/batterystats-daily.xml /system/battery-tasge-stats/ /system/dmappmgr.db /system/graphicsstats/ /system/job/jobs_ <uid>.xml /system/ontification_log.db /system/procstats /system/procstats /system/procstats /system/system/shutdown-checkpoints /system/users/<local_user_number>/app_idle_stats.xml /system_ce/<usernumber>/recent_images/*.png</usernumber></local_user_number></uid>	ABX ABX ABX  ABX  SQLite  ABX SQLite SQLite  TXT XML Protobuf PNG	Application permissions usage Privacy dashboard – Dangerous permissions usage [From Android 12] Application permissions usage Battery Usage Stats – Contains Application Usage information Application Usage (only Samsung devices) Graphic Stats Application Usage Application notifications [Up to Android 10] Application execution (only Samsung devices) Application usage traces Shutdown Checkpoints Application Usage Notification history Application snapshots
Userdata	/system_ce/ <usernumber>/recent_tasks/*.xml /system_ce/<usernumber>/shortcut_service/bitmaps/ /system_ce/<usernumber>/shortcut_service/packages/ /system_ce/<usernumber>/snapshots/*.jpg /system_ce/<usernumber>/usagestats/  KS AND CONNECTIONS /data/com.google.android.gms/databases/cast.db /data/com.google.android.gms/databases/herrevad /data/com.google.android.gms/databases/personalsafety_db /data/com.google.android.gms/shared_prefs/nearbysharing:service:state.xml /log/wifi/iwc/iwc_dump.txt /misc/adb/adb_keys /misc/apexdata/com.android.wifi/WiFiConfigStore.xml</usernumber></usernumber></usernumber></usernumber></usernumber>	XML PNG ABX JPG Protobuf  SQLite SQLite SQLite SQLite XML TXT TXT XML	Recent Tasks Application usage traces Application usage traces Application snapshots Application Usage Stats  Cast devices Wireless network and MAC addresses [Up to Android 9] Android Airtag Scans Nearby Share Wireless network connections log (Samsung device only) Computers connected via ADB Wireless network [From Android 11]
Userdata	/misc/apexdata/com.android.wifi/WiFiConfigStoreSoftAp.xml /misc/bluedroid/bt_config.conf  /misc/bluedroiddump/mainBuffer.log /misc/wifi/WifiConfigStore.xml /system/wifigeofence.db  EDIA /data/com.google.android.apps.maps/databases/ugc_photos_location_data.db /data/com.google.android.apps.photos/databases/gphotos <number>.db /data/com.google.android.providers.media.module/databases/external.db /data/com.samsung.android.providers.media/databases/media.db /data/com.samsung.cmh/databases/cmh.db</number>	XML TXT  TXT XML SQLite SQLite SQLite SQLite SQLite SQLite SQLite	Information about the Wi-Fi hotspot of the device Information about the Bluetooth configuration of the device and the history of connected Bluetooth devices Bluetooth logs (only Samsung devices) Wireless network [Up to Android 10] Wi-Fi Geofence (only Samsung devices)  Photos and Videos metadata Google Photos Traces to SD card used in the device or emulated SD card Media file metadata (only Samsung devices) Camera Photo (only Samsung Devices)
Userdata	/data/com.samsung.storyservice/databases/dme.db /data/com.samsung.visionprovider/databases/visionprovider.db /media/  N ARTIFACTS /data/com.google.android.apps.maps/app_tts-temp/tts-%UNIXEPOCH% /data/com.google.android.apps.maps/databases/gmm_myplaces.db /data/com.google.android.apps.maps/databases/gmm_storage.db /data/com.google.android.apps.maps/databases/gmm_sync.db /data/com.google.android.apps.maps/files/new_recent_history_cache_searches.cs /data/com.google.android.apps.turbo/databases/turbo.db /data/com.sec.android.daemonapp/db/weatherClock /log/wifi/iwc/iwc_dump.txt /Media/0/DCIM/Camera /system/wifigeofence.db	SQLite SQLite N/A  WAV SQLite SQLite SQLite Protobuf SQLite SQLite TXT * SQLite	Samsung Story Service (only Samsung Devices) Camera Photo (only Samsung Devices) Emulated SD Card  Google Maps turn-by-turn directions Home address/Work address/Labeled addresses Search history Maps Favorites Google Maps searches Timezone Wheather app (Samsung devices only) Wireless network connections log (Samsung device only) EXIF data with location info Wi-Fi Geofence (Samsung devices only)
Userdata	VIPING/SETUP  /data/com.android.providers.media/databases/internal.db  /data/com.google.android.apps.wellbeing/databases/app_usage  /data/com.google.android.forest/databases/dwbCommon.db  /data/data/com.google.android.settings.intelligence/shared_prefs/setup_wizard_info.xml  /data/data/com.google.android.settings.intelligence/shared_prefs/suggestions.xml  /misc/bootstat/factory_reset  /misc/bootstat/last_boot_time_utc  /property/persistent_properties  /system/user/service/data/eRR.p	SQLite SQLite SQLite XML XML	Internal system files timestamps Digital Wellbeing (Google) Digital Wellbeing (Samsung) Setup wizard timestamp Setup wizard timestamp Check modified timestamp Check modified timestamp Reboot, Factory Reset Samsung devices only