SANS The most trusted source for cybersecurity training, certifications, degrees, and research

The Most Relevant Evidence per Gigabyte

for585.com/poster

$25.00
DFPS_FOR585_v3.2_0121

DIGITAL FORENSICS & INCIDENT RESPONSE

Operating System & Device In-Depth

FOR308 Digital Forensics Essentials

FOR498 Battlefield Forensics & Data Acquisition
GBFA

FOR500 Windows Forensic Analysis
GCFE

FOR518 Mac and iOS Forensic Analysis and Incident Response

FOR585 Smartphone Forensic Analysis In-Depth
GASF

Incident Response & Threat Hunting

FOR508 Advanced Incident Response, Threat Hunting, and Digital Forensics
GCFA

FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
GNFA

FOR578 Cyber Threat Intelligence
GCTI

FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GREM

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling
GCIH

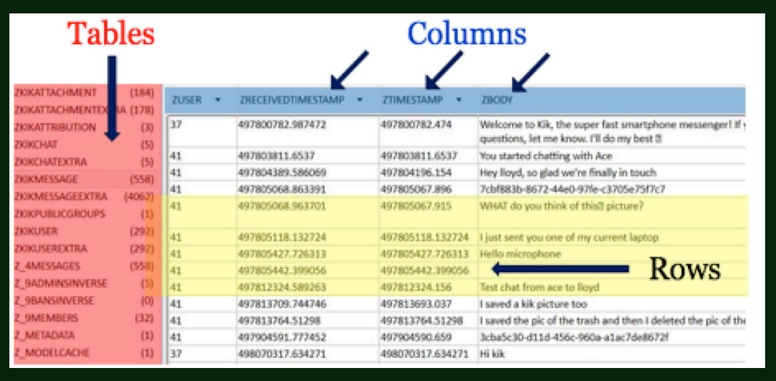
SANS DFIR

@sansforensics sansforensics dfir.to/MAIL-LIST

SQLite

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 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 the number by 1,000,000:

- `SELECT datetime(TS_COLUMN/1000000 + (strftime('%s','1601-01-01')),'UNIXEPOCH');`

Table Joins

Taking data from two (or more!) tables that have a column in common and joining them into one table. Identify tables of interest that contain unique values.

LEFT JOIN – Resulting rows are returned from the **LEFT** table even if there are no matches in the right. Using the **LEFT JOIN** returns all the text messages, including those with and without attachments.

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

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

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;`

Useful Stuff

Column Renaming:
A_TABLE.ZAWKWARDCOLUMNNAME AS "Chat Messages"

Counting:
`SELECT COUNT(*) FROM A_TABLE;`

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

Sorting with ORDER BY:
`SELECT * FROM CHAT ORDER BY A_TIMESTAMP ASC`
ASC = Ascending DESC = Descending

Searching with WHERE and LIKE:
`SELECT CONTACT, MESSAGE FROM CHAT WHERE CONTACT LIKE '%Hank%'`

Our Favorite Mobile Forensic Resources

Practitioners/Researchers

Sarah Edwards	https://www.mac4n6.com
Heather Mahalik	https://smarterforensics.com
Mattia Epifani	http://mattiaep.blogspot.com
Adrian Leong	http://cheeky4n6monkey.blogspot.com
Alexis Brignoni	https://abrignoni.blogspot.com
Jon B	https://www.ciofecaforensics.com
Mari DeGrazia	http://az4n6.blogspot.com
Andrew Hoog	https://www.hack42labs.com
Ian Whiffin	http://doubleblak.com/blogs.php
Josh Hickman	https://thebinaryhick.blog

Vendors

Oxygen Forensics	https://blog.oxygen-forensic.com
Magnet Forensics	https://www.magnetforensics.com/blog
Cellebrite	https://www.cellebrite.com/en/blog
BlackBag Technologies	https://www.blackbagtech.com/blog
Sanderson Forensics	https://sqliteforensictoolkit.com/support-articles
Elcomsoft	https://blog.elcomsoft.com

Additional Resources

DFRWS	https://dfrws.org/
iOS Jailbreaks	https://www.theiphonewiki.com/wiki/Jailbreak
FOR585 Google Group	*access granted to all 585 Alumni
DFIR mailing list	DFIR@lists.sans.org

Mobile Malware and Spyware

Key Artifacts: Static Analysis

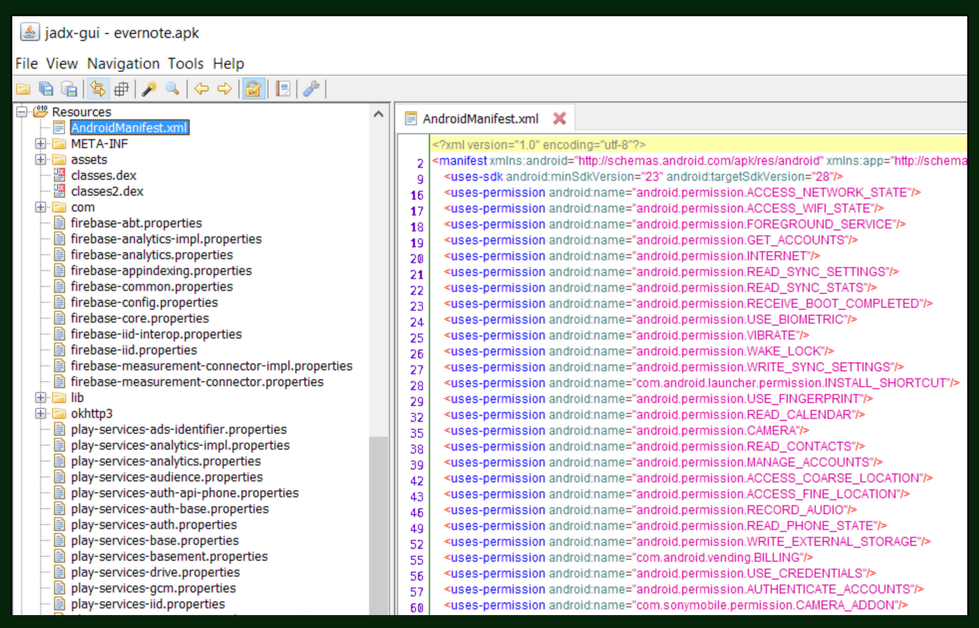
Requested Permissions: Granted to an application by the user (1) during installation or (2) upon execution/runtime. Found in the AndroidManifest.xml file.

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.

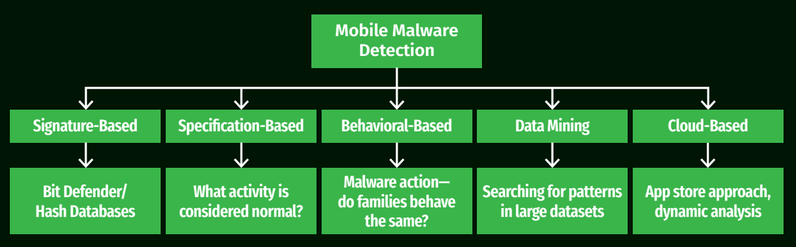
Content Providers: Refers to how information is stored within an application and shared between multiple applications. Example: a contact database often used by many native and third-party applications. The code would call the ContentResolver (the global instance that provides access to the content)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



Common Signs and Symptoms

- **Android devices are most at risk 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**
- **Unexpected device behaviors**
  - Unplanned reboots
  - Apps that close or open on their own
  - Unexplained settings changes
- **High-risk user behavior**
  - Risky downloads, browsing or link-clicking
- **Spyware: Device was out of owner's control**
  - Spyware installation requires possession of the device

Mobile Malware Detection



Online Mobile Malware Sandboxes

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

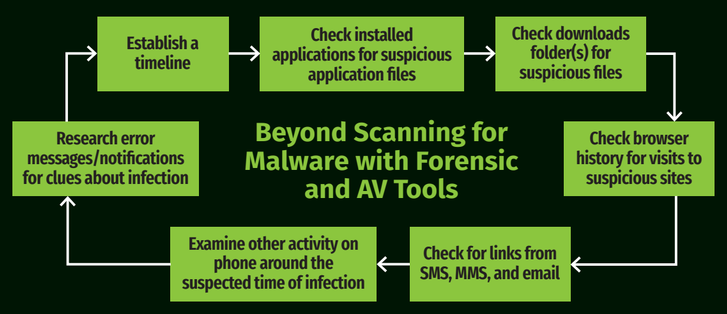
- https://www.joesandbox.com/
- https://amaaas.com/
- https://github.com/pjlantz/droidbox

Local Static Malware Analysis

Tools installed on the local machine for mobile malware analysis:

- Android SDK
- Dex2Jar
- Dexter
- JD-GUI

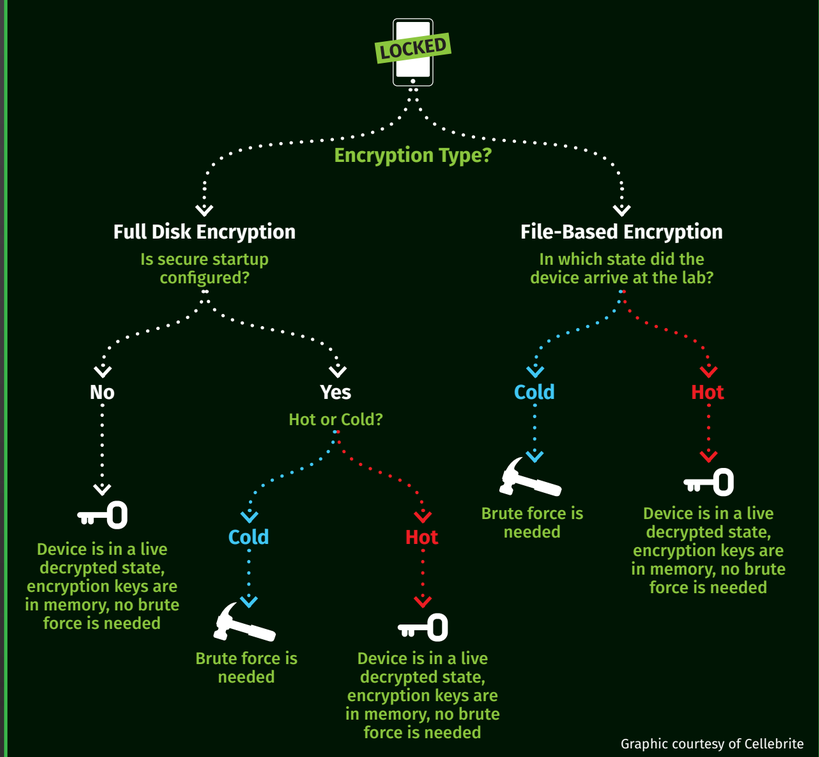
*Virtual machine environments for mobile malware analysis: Santoku



Free Scripts and Helpful Utilities

	Utility	Description	Repository
iOS	APOLLO	Apple Pattern of Life Lazy Output'er	https://github.com/mac4n6/APOLLO
	iLEAPP	iOS Logs, Events, And Properties Parser	https://github.com/abrignoni/iLEAPP
	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/ahoog42/ios-triage
	fplist	Converts plist files to json, dot notation or csv	https://www.hack42labs.com/tools/fplist/details/
	iOS_sysdiagnose_forensic_scripts	Scripts for parsing various iOS sysdiagnose logs	https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts
Android	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
	ftree	Identifies, hashes and destructures all files recursively from any file system	https://www.hack42labs.com/tools/ftree/details/
	FAPK	Extracts apk files from an Android device	https://www.hack42labs.com/tools/fapk/
Third-Party Applications/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
	SQLite-Deleted-Records-Parser	Recovers deleted entries from SQLite databases	https://github.com/mdegrazia/SQLite-Deleted-Records-Parser
	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

Android Extraction



Graphic courtesy of Cellebrite

Poster Authors

Heather Mahalik
hmahalik@gmail.com
@heathermahalik

Domenica "Lee" Crognale
domenica.crognale@gmail.com
@domenicacrognal

Mattia Epifani
mattia.epifani@realitynet.it
@mattiaep

©2021 Heather Mahalik, Domenica "Lee" Crognale, and Mattia Epifani. All Rights Reserved.

https://t.me/learningnets

iOS Cheatsheet

DEVICE INFORMATION

Path	Description	BFU	Backup	Sysdiagnose
/private/var/installd/Library/MobileInstallation/LastBuildInfo.plist	Operating system version	Y	Y	N
/private/var/mobile/Library/CoreDuet/coreduetd.db	Lock/Device Passcode Info (0=unlocked, 1=locked) (Up to iOS 9)	N	N	N
/private/var/mobile/Library/Logs/mobileactivationd/	MobileActivation Logs	Y	N	Y
/private/var/mobile/Library/Preferences/com.apple.AdLib.plist	May show older iOS versions used	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.aggregated.plist	Last BootTime	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.mmcs.plist	IMSIs	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.mobilegestalt.plist	Device name	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.preferences.datetime.plist	Time settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.preferences.network.plist	Airplane mode (on/off)	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.Preferences.plist	Disk usage	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist	Language, Country info, Device IDs	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.timed.plist	Auto Time and Auto Time Zone settings	Y	Y	N
/private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist	Network IP, WiFi, Cellular Information	Y	Y	N
/private/var/preferences/SystemConfiguration/com.apple.radios.plist	Airplane mode (on/off)	Y	Y	N
/private/var/preferences/SystemConfiguration/NetworkInterfaces.plist	Wi-Fi Mac Addresses	Y	N	Y
/private/var/preferences/SystemConfiguration/preferences.plist	Network and VPN information	Y	Y	N
/private/var/root/Library/Lockdown/escrow_records/	Computer Trust/Pair certificates	Y	N	N
/private/var/root/Library/Lockdown/pair_records/	Computer Trust/Pair certificates	Y	N	N
/private/var/root/Library/Preferences/com.apple.preferences.network.plist	Airplane mode (on/off)	Y	Y	N
/private/var/wireless/Library/Preferences/com.apple.commcenter.plist	Device Info (IMEI, Phone Number, Network Carrier, ICCIDs, IMSIs, etc.)	Y	Y	N

PASSWORDS AND ACCOUNT INFORMATION

Path	Description	BFU	Backup	Sysdiagnose
/private/var/mobile/Library/Accounts/Accounts3.sqlite	Account information	Y	Y	N
/private/var/mobile/Library/DataAccess/	Account information used to set up apps (Email, #, etc)	Y	Y	N
/private/var/mobile/Library/DataAccess/AccountInformation.plist	Email sync data	Y	Y	N
/private/var/mobile/Library/DataAccess/iCloud-[iCloud email account name]/.mboxCache.plist	iCloud Email account information	Y	Y	N
/private/var/mobile/Library/Health/healthdb.sqlite	Health data, personal data, iOS version info, etc.	N	Y	N
/private/var/mobile/Library/Health/healthdb_secure.sqlite	Health data, personal data, iOS version info, etc.	N	Y	N
/private/var/mobile/Library/MedicalID/MedicalIDData.Archive	Medical Information (bloodtype, organ donor, name, DOB, etc.)	N	Y	N
/private/var/mobile/Library/Preferences/com.apple.accountsettings.plist	Email accounts pushed to device	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.cmfsyncagent.plist	Blocked Dialers	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.commcenter.shared.plist	Phone number	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.conference.plist	Facetime phone number in use, SMS phone number, user accounts	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.contacts.donation-agent.plist	Last Metrics Attempts (usage information)	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.contextstored.plist	Activity throttling	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.coreduetd.plist	Activity throttling	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.corerecents.recentsd.plist	iCloud login information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.FeedbackAssistant.plist	Last successful email address used to login to cloud	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.homesharing.plist	iCloud account information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.icloud.findmydeviced.FMIPAccounts.plist	Find My iPhone settings	Y	Y	N
/private/var/mobile/Library/UserConfigurationProfiles/	Profiles and restrictions	Y	Y	N
/private/var/preferences/SystemConfiguration/com.apple.accounts.exists.plist	Account information	Y	Y	N
/private/var/root/Library/Lockdown/data_ark.plist	Last backup computer, iCloud Backup Settings, Device info	Y	N	N
/private/var/wireless/Library/preferences/com.apple.commcenter.callservices.plist	Last iCloud account	Y	N	N

SETTINGS – SYSTEM CONTROLLED – KEYBOARDS, DICTIONARY, LOGS, BT ADDRESS, ETC.

Path	Description	BFU	Backup	Sysdiagnose
/private/installd/Library/Logs/MobileInstallation/mobile_installation.log*	Mobile Applications Installation Logs	Y	N	Y
/private/var/mobile/Containers/	Application Folders	Y	Y	N
/private/var/mobile/Library/BulletinBoard/ClearedSections.plist	Logs of cleared notifications	Y	Y	N
/private/var/mobile/Library/Keyboard/<language>-dynamic.lm/dynamic-lexicon.dat	Auto correction / Predictive text	N	N	N
/private/var/mobile/Library/Preferences/	Examine plists for more information	Y	Y	N
/private/var/preferences/SystemConfiguration/NetworkInterfaces.plist	Wi-Fi Mac Addresses	Y	N	Y

SETTINGS – USER CONTROLLED – SYNC SETTINGS, SPRINGBOARD, ETC.

Path	Description	BFU	Backup	Sysdiagnose
/private/var/containers/Shared/SystemGroup/systemgroup.com.apple.configurationprofiles/Library/ConfigurationProfilesCloudConfigurationDetails.plist	Cloud configurations	N	N	N
/private/var/mobile/Library/DoNotDisturb/DB/Settings.json	Do not disturb settings	Y	Y	N
/private/var/mobile/Library/Keyboard/UserDictionary.sqlite	User created auto-correct	N	N	N
/private/var/mobile/Library/Mail/	Mail and settings	N	N	N
/private/var/mobile/Library/Preferences/com.apple.assistant*	Siri	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.assistant.backedup.plist	Cloud sync settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.camera.plist	Camera settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.celestial.plist	Camera, CarPlay, Volumes and other settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.cloudphotod.plist	Cloud photo sync information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.CoreDuet.plist	Cloud sync settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.imservice*	SMS, iMessage and FaceTime	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist	Time to keep messages	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.preferences.network.plist	Airplane Mode Settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.springboard.plist	User created restrictions/Remote wipe settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.weather.plist	Weather (including current city)	Y	Y	N
/private/var/mobile/Library/SpringBoard/HomeBackground.cpbitmap	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/HomeBackgroundThumbnail.jpg	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/IconState.plist	Homescreen icon layout	Y	Y	N
/private/var/mobile/Library/SpringBoard/LockBackground.cpbitmap	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/LockBackgroundThumbnail.jpg	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/LockBackgroundThumbnaildark.jpg	Wallpaper	Y	Y	N
/private/var/mobile/Library/SpringBoard/PushStore/	Notifications	N	N	N
/private/var/mobile/Library/UserConfigurationProfiles/UserSettings.plist	User created restrictions	Y	Y	N
/private/var/mobile/Library/UserNotifications/	User Notifications	Y	Y	N
/private/var/root/Library/Lockdown/data_ark.plist	Last backup computer, iCloud Backup Settings, Device info	Y	N	N
/private/var/root/Library/Preferences/com.apple.preferences.network.plist	Airplane Mode Settings	Y	Y	N

COMMUNICATIONS – SMS, CALLS, EMAIL

Path	Description	BFU	Backup	Sysdiagnose
/private/var/mobile/Library/CallHistory/call_history.db	Call log (Up to iOS 7)	N	Y	N
/private/var/mobile/Library/CallHistoryDB/CallHistory.storedata	Call log (From iOS 8)	N	Y	N
/private/var/mobile/Library/CallHistoryDB/CallHistoryTemp.storedata	Call History Temporary storage (Before First Unlock)	Y	N	N
/private/var/mobile/Library/Mail/	Mail and settings	N	N	N
/private/var/mobile/Library/Preferences/com.apple.madrid.plist	SMS, iMessage and FaceTime	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.mobilephone.*	List of contacts added to the phone application's favorites list	N	Y	N
/private/var/mobile/Library/Preferences/com.apple.MobileSMS.plist	SMS, iMessage and FaceTime	Y	Y	N
/private/var/mobile/Library/Recents/	Recents communications	N	N	N
/private/var/mobile/Library/SMS/Attachments/*	MMS File	N	Y	N
/private/var/mobile/Library/SMS/Drafts/*	SMS/MMS Drafts	N	Y	N
/private/var/mobile/Library/SMS/sms.db	SMS/MMS messages	N	Y	N
/private/var/mobile/Library/SMS/sms-temp.db	SMS Temporary storage (Before First Unlock)	Y	N	N
/private/var/mobile/Library/Suggestions/query_predictions.db	Contains iMessage/SMS traces	N	N	N
/private/var/mobile/Library/Voicemail/voicemail.db	Voicemail	Y	N	N
/private/var/mobile/Media/Recordings/*	Voice Memos	N	Y	N

BROWSER ACTIVITY

Path	Description	BFU	Backup	Sysdiagnose
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Caches/com.apple.mobilesafari/	Safari Cache files	N	N	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Caches/com.apple.mobilesafari/Cache.db	Safari Cache database	N	N	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Caches/com.apple.WebAppCache/ApplicationCache.db	Safari Website cache	N	N	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Cookies/Cookies.binarycookies	Safari Cookies	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Favicons/Favicons/	Safari Website favicons	N	N	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Preferences/com.apple.mobilesafari.plist	Safari Configuration	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Safari/Downloads/Downloads.plist	Safari Download History	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Safari/Thumbnails/	Safari Tabs Screenshots (PNG or KTX format)	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/WebKit/WebsiteData/LocalStorage/*	Safari WebKit Localstorage	Y	Y	N
/private/var/mobile/Library/Assistant/knowledgeC.db	Safari History information	N	N	N
/private/var/mobile/Library/Safari/Bookmarks.db	Safari Bookmarks	N	Y	N
/private/var/mobile/Library/Safari/BrowserState.db	Safari Suspended State Tab	N	N	N
/private/var/mobile/Library/Safari/CloudTabs.db	Safari Cloud Tabs	N	N	N
/private/var/mobile/Library/Safari/History.db	Safari History	N	N	N

MULTIMEDIA

Path	Description	BFU	Backup	Sysdiagnose
*.ktx	Application Snapshots	N	N	N
/private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb	Contacts pictures	N	Y	N
/private/var/mobile/Library/Preferences/com.apple.mobileslideshow.plist	Photos	Y	Y	N
/private/var/mobile/Library/SMS/Attachments/	MMS File	N	Y	N
/private/var/mobile/Media/DCIM/1*APPLE	User Created/Saved Photos	N	Y	N
/private/var/mobile/Media/iTunes_Control/iTunes/MediaLibrary.sqlitedb	iTunes Media Library	Y	Y	N
/private/var/mobile/Media/PhotoData/*.ithmb	Thumbnails databases	N	Y	N
/private/var/mobile/Media/PhotoData/AlbumsMetadata/	Photo Albums Metadata	N	Y	N
/private/var/mobile/Media/PhotoData/CPL/	Cloud Photo Library	N	Y	N
/private/var/mobile/Media/PhotoData/Photos.sqlite	Photos/Videos Database	N	Y	N
/private/var/mobile/Media/PhotoData/V2/	Photos saved from Live Video and SMS photo capture	N	Y	N

NETWORK CONNECTIONS

Path	Description	BFU	Backup	Sysdiagnose
/private/var/db/dhcpclient/leases/	DHCP Lease	Y	N	N
/private/var/mobile/Library/Preferences/com.apple.preferences.network.plist	Airplane mode ON/OFF	Y	Y	N
/private/var/networkd/netusage.sqlite	Network data usage per App	N	N	N
/private/var/preferences/com.apple.networkextension.plist	Network Extension	Y	Y	N
/private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist	Network IP, Wi-Fi, Cellular	Y	Y	N
/private/var/preferences/SystemConfiguration/com.apple.wifi.plist	Wi-Fi	Y	Y	Y
/private/var/preferences/SystemConfiguration/NetworkInterfaces.plist	Wi-Fi Mac Addresses	Y	N	Y
/private/var/preferences/SystemConfiguration/preferences.plist	Wi-Fi, VPN, Certs and more	Y	Y	N
/private/var/root/Library/Preferences/com.apple.preferences.network.plist	Wi-Fi ON/OFF	Y	Y	N
/private/var/wireless/Library/Databases/CellularUsage.db	SIMs used in device, including most recent	Y	Y	N
/private/var/wireless/Library/Preferences/com.apple.CommCenter.counts.plist	Data and Cellular network statistics	Y	Y	N
/private/var/wireless/Library/Preferences/com.apple.commcenter.device_specific_nobackup.plist	Device IMEI	Y	Y	N
/private/var/wireless/Library/Preferences/com.apple.commcenter.plist	SIM Card ICCID	Y	Y	N

SYNCING ARTIFACTS

Path	Description	BFU	Backup	Sysdiagnose
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Database/com.apple.MobileBluetooth.ledevices.other.db	Seen Bluetooth devices	N	Y	N
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db	Paired Bluetooth devices	Y	Y	N
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Preferences/com.apple.MobileBluetooth.devices.plist	Paired Bluetooth devices	N	Y	N
/private/var/mobile/Library/DataAccess/iCloud-[iCloud email account name]/.OfflineCache/[number]	iClould offline cache	Y	Y	N
/private/var/mobile/Library/DeviceRegistry.state/activeStateMachine.plist	Apple Watch pairing information	Y	Y	N
/private/var/mobile/Library/DeviceRegistry.state/historySecureProperties.plist	Apple Watch information (also previously paired Apple Watch)	N	Y	N
/private/var/mobile/Library/DeviceRegistry.state/stateMachine-<GUID>.plist	Apple Watch pairing information (also previously paired Apple Watch)	N	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/	Apple Watch data	Y	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/NanoAppRegistry/Applications/	Apple Watch Applications	Y	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/NanoMail/registry.sqlite	Apple Watch Mail application	Y	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/NanoPasses/nanopasses.sqlite3	Apple Watch Wallet Passes	N	Y	N
/private/var/mobile/Library/DeviceRegistry/<GUID>/NanoPreferencesSync/Backup/Files/	Apple Watch Faces	Y	Y	N
/private/var/mobile/Library/Health/NanoSync/com.apple.private.alloy.health.sync.db	AppleWatch Health data sync	N	Y	N
/private/var/mobile/Library/homed/datastore.sqlite	Apple HomeKit Devices	N	Y	N
/private/var/mobile/Library/MobileBluetooth/com.apple.MobileBluetooth.ledevices.plist	Seen Bluetooth devices	Y	Y	N
/private/var/mobile/Library/NanoBackup/	Apple Watch information	Y	Y	N
/private/var/mobile/Library/NanoMusicSync/	Apple Watch information	Y	N	N
/private/var/mobile/Library/NanoPreferencesSync/	Apple Watch information	Y	N	N
/private/var/mobile/Library/NanoTimeKit/	Apple Watch information	Y	N	N
/private/var/mobile/Library/Preferences/com.apple.carplay.plist	Apple CarPlay configuration	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.cloud.quota.plist	iCloud quota information	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.CoreDuet.QueuedDenials.plist	Cloud Sync denials and dates	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.coreduetd.plist	sync devices	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.identityservices.idstatuscache.plist	iCloud sync, Email, FaceTime, Email, more	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.mobile.ldbackup.plist	Last iTunes and last iCloud backup date and timezone.	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.nano*.plist	Apple Watch preferences	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.sharingd.plist	Device AirDrop ID	Y	Y	N
/private/var/mobile/Library/Springboard/<GUID>-CarDisplay[Desired]IconState.plist	Apple CarPlay per car App Icon configuration	Y	Y	N
/private/var/mobile/Media/iTunesControl/iTunes/iTunesPrefs	List of computer where the device was connected to	Y	Y	N
/private/var/root/Library/Lockdown/data_ark.plist	Last backup computer, iCloud Backup Settings, Device info	Y	N	N
/private/var/wireless/Library/Databases/DataUsage-watch.sqlite	Watch Application Usage	N	N	N

LOCATION ARTIFACTS

Path	Description	BFU	Backup	Sysdiagnose
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Database/com.apple.MobileBluetooth.ledevices.other.db	Seen Bluetooth devices	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple_Maps_GUID>/Library/Maps/GeoHistory.mapsdata	Apple Maps history	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple_Maps_GUID>/Library/Maps/History.mapsdata	Apple Maps history	N	Y	N
/private/var/mobile/Containers/Data/Application/<Apple_Maps_GUID>/Library/Preferences/com.apple.Maps.plist	Last latitude and longitude, map search history	Y	Y	N
/private/var/mobile/Containers/Data/Application/<Apple_Maps_GUID>/Library/SyncedPreferences/com.apple.Maps-com.apple.Maps.recents.plist	Apple Maps recents	Y	N	N
/private/var/mobile/Containers/Data/Application/<Apple_Maps_GUID>/Library/SyncedPreferences/com.apple.Maps-com.apple.MapsSupport.bookmarks.plist	Apple Maps bookmarks	Y	N	N
/private/var/mobile/Containers/Data/Application/<Apple_Maps_GUID>/Library/SyncedPreferences/com.apple.Maps-com.apple.MapsSupport.history.plist	Apple Maps history	Y	N	N
/private/var/mobile/Containers/Shared/AppGroup/<Apple_MAPS_GUID>/Library/Preferences/group.com.apple.Maps.plist	Last latitude and longitude, map search history	Y	Y	N
/private/var/mobile/Library/Caches/com.apple.routined/Cache.sqlite	Location information	N	N	N
/private/var/mobile/Library/Caches/com.apple.routined/Local.sqlite	Location information	N	N	N
/private/var/mobile/Library/Preferences/com.apple.locationd.plist	"Location Services" setting (Enabled = 1; Disabled = 0)	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.preferences.datetime.plist	Time settings	Y	Y	N
/private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist	Language, Country info, Device IDs	Y	Y	N
/private/var/preferences/SystemConfiguration/com.apple.networkidentification.plist	Network IP, WiFi, Cellular	Y	Y	N
/private/var/preferences/SystemConfiguration/preferences.plist	Network and VPN information	Y	Y	N
/private/var/root/Library/Caches/locationd/Cache.sqlite	Location information	N	N	N
/private/var/root/Library/Caches/locationd/cache_encryptedA.db	Location information	N	N	N
/private/var/root/Library/Caches/locationd/cache_encryptedB.db	Location information	N	N	N
/private/var/root/Library/Caches/locationd/cache_encryptedC.db	Location information	N	N	N
/private/var/root/Library/Caches/locationd/consolidated.db	Application Traces and GeoFence information	Y	Y	N
/private/var/root/Library/Caches/locationd/significant.plist	Significant Location	N	Y	N
/private/var/root/Library/Caches/locationd/significantVisitAuth.plist	Significant Location	Y	Y	N
/private/var/root/Library/Caches/locationd/significantVisitInterest.plist	Significant Location	Y	Y	N

TRACES OF DESTRUCTION – WIPING, ETC.

Path	Description	BFU	Backup	Sysdiagnose
/private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist	Language, Country info, Device IDs	Y	Y	Y
/private/var/root/.obliterated	Creation time stamp -> Device reset time	Y	N	N
/private/var/root/Library/Preferences/com.apple.MobileBackup.plist	Restore information (timestamp, local vs. iCloud)	Y	Y	Y

APPLICATION USAGE

Path	Description	BFU	Backup	Sysdiagnose
/private/var/installd/Library/Logs/MobileInstallation/mobile_installation.log*	Mobile Applications Installation Logs	Y	N	Y
/private/var/containers/Shared/SystemGroup/<GUID>/Library/BatteryLife/CurrentPowerLog.PLSQL	Battery life tracker	N	N	Y
/private/var/mobile/Library/AggregatedDictionary/ADDataStore.sqlitedb	Application traces	Y	N	N
/private/var/mobile/Library/AppConduit/AvailableApps.plist	Installed Apps and Apps Path	Y	N	N
/private/var/mobile/Library/AppConduit/AvailableCompanionApps.plist	Installed Apps and Apps Path	Y	N	N
/private/var/mobile/Library/Application Support/com.apple.remotemanagmentd/RMAdminStore-Local.sqlite	Screen time	N	N	N
/private/var/mobile/Library/ApplicationSync/AssetSortOrder.plist	Application order on the SpringBoard	Y	N	N
/private/var/mobile/Library/Assistant/knowledgeC.db	Application traces	N	N	N
/private/var/mobile/Library/com.apple.itunesstored/itunesstored2.sqlitedb	Application traces	Y	Y	N
/private/var/mobile/Library/com.apple.itunesstored/kvs.sqlitedb	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
/private/var/mobile/Library/Logs/AppConduit/	Installed Apps and Apps Path	Y	N	Y
/private/var/mobile/Library/Logs/mobile_installation_helper.log*	Application traces	N	Y	N
/private/var/mobile/Library/Preferences/addaily.plist	Application traces	Y	Y	N
/private/var/containers/Shared/SystemGroup/<GUID>/Library/Logs/mobile_installation_helper.log*	Application traces	N	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
/private/var/mobile/Library/Preferences/com.apple.corespotlightui.plist	Application traces	Y	Y	N
/private/var/mobile/Library/TCC/TCC.db	Applications permissions	Y	Y	N
/private/var/networkd/netusage.sqlite	Network data usage per App	N	N	N
/private/var/root/Library/Caches/locationd/clients.plist	Application traces	Y	Y	N
/private/var/root/Library/Logs/MobileContainerManager	MobileContainerManager logs	Y	N	Y
/private/var/root/Library/MobileContainerManager/containers.sqlite3	Installed Applications	Y	N	N
/private/var/wireless/Library/Databases/DataUsage.sqlite	Application traces	Y	N	N

Android Cheatsheet

DEVICE INFORMATION

Partition	Path	Tables of Interest	Description
System	/build.prop	N/A	Device information (version, patches, etc.)
Userdata	/data/com.android.providers.calendar/databases/calendar.db	*	Calendar Items and Timezone information
Userdata	/data/com.android.providers.settings/databases/settings.db	*	Lock settings information
Userdata	/data/com.android.providers.settings/databases/settings.db-WAL	*	Lock settings information
Userdata	/data/com.android.providers.settings/databases/locksettings.db	*	Lock settings information
Userdata	/data/com.android.providers.settings/databases/locksettings.db-WAL	*	Lock settings information
Userdata	/data/com.google.android.gms/shared_prefs/Checkin.xml	N/A	Activity on device related to installed SIM (ICCID and Google Account included)
Userdata	/data/com.google.android.gsf/databases/gservices.db	*	Fitness settings, network settings, other settings
Userdata	/misc/	N/A	Bluetooth, VPN, Wi-Fi and more
Userdata	/Property/persist.sys.timezone	N/A	Timezone (Up to Android 8)
Userdata	/Property/persistent_properties	N/A	Timezone (From Android 9)
Userdata	/system/*.key	N/A	Files needed for password cracking
Userdata	/system/device_policies.xml	N/A	Passcode requirements and policies. Syncing info may exist
Userdata	/system/locksettings.db	*	Lock settings information
Userdata	/system/locksettings.db-WAL	*	Lock settings information
Userdata	/system/netpolicy.xml	N/A	Timezone
Userdata	/system/SimCard.dat	N/A	Sim card and phone number information
Userdata	/system/users/0/settings_global.xml	N/A	Global settings
Userdata	/system/users/0/settings_secure.xml	N/A	Secure settings
Userdata	/system/users/0/settings_system.xml	N/A	System settings

PASSWORDS AND ACCOUNT INFORMATION

Partition	Path	Tables of Interest	Description
Userdata	/data/com.android.email/databases/EmailProvider.db	Account, Email AddressCache, Mailbox*	Email accounts, 3rd party app data, and messages associated with Email notifications, Email accounts, 3rd party app data, and messages associated with Email notifications
Userdata	/data/com.android.providers.contacts/databases/contacts2.db	accounts	Login info
Userdata	/data/com.android.providers.settings/*	N/A	Username and passwords
Userdata	/data/com.android.vending/shared_prefs/lastaccount.xml	N/A	Last account used on Google PlayStore (Android 9 and above)
Userdata	/data/com.google.android.gms/shared_prefs/BackupAccount.xml	N/A	Backup account email address
Userdata	/data/com.google.android.googlequicksearchbox/databases/app_icons.db	*	Google Account Information
Userdata	/data/com.google.android.googlequicksearchbox/databases/launcher.db	*	Google Account Information
Userdata	/data/com.google.android.googlequicksearchbox/databases/opa_history	*	Google Account Information
Userdata	/data/com.google.android.gsf/databases/gservices.db	*	Fitness settings, network settings, other settings
Userdata	/system_ce/0/accounts_ce.db	*	Additional accounts (could also be system_de or accounts_de)
Userdata	/system_de/0/accounts_de.db	*	Additional accounts (could also be system_de or accounts_de)
Userdata	/misc/wifi/softap.conf	N/A	Hotspot Passwords
Userdata	/misc/wifi/wpa_supplicant.conf	N/A	Wi-Fi Network Password
Userdata	/system/accounts*.db	*	User account information
Userdata	/system/sync/accounts.xml	N/A	User account information
Userdata	/system/users/0/0.xml	N/A	User information

SYSTEM SETTINGS

Partition	Path	Tables of Interest	Description
Userdata	/data/com.google.android.gms/shared_prefs/*	N/A	Preference files
Userdata	/data/com.google.android.gsf/databases/gservices.db	*	Fitness settings, network settings, other settings
Userdata	/system/recent_images/*.png	N/A	Application snapshots
Userdata	/system_ce/recent_images/*.png		Application snapshots
Userdata	/system/users/0/settings_global.xml	N/A	Global settings
Userdata	/system/users/0/settings_secure.xml	N/A	Secure Settings
Userdata	/system/users/0/settings_system.xml	N/A	System Settings

USER SETTINGS

Partition	Path	Tables of Interest	Description
Userdata	/data/com.android.providers.calendar/databases/calendar.db	*	Calendar Items and Timezone information
Userdata	/data/com.android.providers.userdictionary/databases/user_dict.db	*	Dictionary Files (Keylogging)
Userdata	/data/com.google.android.gms/databases/NetworkUsage.db	*	Application, User and Location traces
Userdata	/data/com.google.android.gms/databases/ns.db	*	Application, User and Location traces
Userdata	/data/com.google.android.gms/databases/reminders.db	*	Application, User and Location traces
Userdata	/data/com.google.android.gsf/databases/googlesettings.db	*	Google preferences – location, maps, wallet, etc --1=true
Userdata	/data/com.google.android.gsf/databases/gservices.db	*	Fitness settings, network settings, other settings
Userdata	/data/com.sec.android.inputmethod/Swiftkey/user/dynamic.lm	N/A	Dictionary Files (Keylogging) SwiftKey folder name may vary

COMMUNICATIONS – SMS, CALLS, EMAILS

Partition	Path	Tables of Interest	Description
Cache	*	*	Gmail attachments, Downloads and Browser data
Userdata	/data/com.android.providers.contacts/databases/calllog.db	calls	Call logs (From Android 7)
Userdata	/data/com.android.providers.contacts/databases/contacts2.db	calls	Call logs (Up to Android 6)
Userdata	/data/com.android.providers.telephony/databases/mmssms.db	sms and part	SMS/MMS
Userdata	/data/com.google.android.apps.messaging/databases/bugle_db	*	RCS/Android Messages (refer to notebook for query)
Userdata	/data/com.google.android.dialer/databases/dialer.db	*	Call logs
Userdata	/data/com.google.android.gm/databases/<mail-name>.db	conversations and messages	Gmail snippets
Userdata	/data/com.google.android.gm/databases/bigTopDataDB.<user-id>		Email information
Userdata	/data/com.google.android.gm/databases/EmailProvider.db		Email information
Userdata	/data/com.google.android.gms/databases/icing_mmssms.db	*	SMS/MMS
Userdata	/data/com.google.android.gms/databases/ipa_mmssms.db	*	SMS/MMS
Userdata	/data/com.sec.android.provider.logsprovider/databases/logs.db	logs	Call logs

MULTIMEDIA

Partition	Path	Tables of Interest	Description
Userdata	/data/com.android.providers.media/databases/external*.db	*	Traces to SD card used in the device. This is stored on the phone.
Userdata	/data/com.android.providers.media/databases/external*.db-WAL	*	Traces to SD card used in the device. This is stored on the phone.
Userdata	/data/com.google.android.apps.photos/databases/gphotos0.db	local_media	Camera Photos information
Userdata	/data/com.samsung.cmh/databases/cmh.db	files	Camera Photo - Samsung Devices
Userdata	/data/com.samsung.storyservice/databases/dme.db	info	Camera Photo - Samsung Devices
Userdata	/data/com.samsung.visionprovider/databases/visionprovider.db	files	Camera Photo - Samsung Devices
Userdata	/media/	N/A	Acts like SD card

BROWSER ACTIVITY

Partition	Path	Tables of Interest	Description
Cache	*	N/A	Gmail attachments, Downloads and Browser data
Userdata	/data/com.android.browser/app_databases/*	*	Internet History
Userdata	/data/com.android.browser/app_geolocation/GeolocationPermissions.db	*	Internet History
Userdata	/data/com.android.browser/databases/Browser.db		
Userdata	/data/com.android.browser/databases/browser2.db	*	Internet History
Userdata	/data/com.android.browser/databases/webview.db	*	Internet History
Userdata	/data/com.android.browser/databases/webviewCache.db	*	Internet History
Userdata	/data/com.android.email/webviewCache.db	*	Internet History

NETWORK CONNECTIONS

Partition	Path	Tables of Interest	Description
Userdata	/data/com.android.connectivity.metrics/databases/events.db	completed_events_requests	USB, Bluetooth, NFC and other connects - Acquisition connection tracked here
Userdata	/data/com.google.android.gms/databases/herrevad	*	Wireless network and MAC addresses
Userdata	/data/com.google.android.locations/files/cache.cell	*	Cellular and WiFi
Userdata	/data/com.google.android.locations/files/cache.wifi	*	Cellular and WiFi
Userdata	/misc/wifi/WifiConfigStore.xml	N/A	Wireless network

SYNCING ARTIFACTS

Partition	Path	Tables of Interest	Description
Userdata	/data/com.google.android.apps.docs.editors.docs/databases/*	*	Google Docs
Userdata	/data/com.google.android.apps.docs.editors.sheets/databases/*	*	Google Docs
Userdata	/data/com.google.android.apps.docs.editors.slides/databases/*	*	Google Docs
Userdata	/data/com.google.android.apps.docs/databases/*	*	Google Docs
Userdata	/data/com.google.android.apps.genie.geniewidget/databases/newsweather.db	*	Sync activity
Userdata	/data/com.google.android.gms/databases/peoplelog.db	*	Sync activity - contacts
Userdata	/data/com.google.android.gms/shared_prefs/com.google.android.gms.auth.authzen.cryptauth.SyncManager.proximity_features.xml	N/A	Sync Activity
Userdata	/system/sync/accounts.xml		Synced Accounts

LOCATION ARTIFACTS

Partition	Path	Tables of Interest	Description
Userdata	/data/com.google.android.apps.maps/databases/da_destination_history	destination history	Maps
Userdata	/data/com.google.android.apps.maps/databases/gmm_storage.db	*	Search history Maps
Userdata	/data/com.google.android.apps.maps/databases/search_history.db	history & suggestions	Maps
Userdata	/data/com.google.android.apps.maps/databases/gmm_sync.db	*	Syncing
Userdata	/data/com.sec.android.daemonapp/db/weatherClock	*	Location artifacts
Userdata	/Media/0/DCIM/Camera	*	EXIF data with location info

APPLICATION USAGE

Partition	Path	Tables of Interest	Description
Userdata	/app/*	N/A	APK files for installed applications
Userdata	/dalvik-cache	N/A	.dex/.oat/.art files for installed applications
Userdata	/data/"Application Folder"	N/A	Application Data Files*
Userdata	/data/com.android.vending/databases/data_usage.db	app_data_usage	Application traces
Userdata	/data/com.android.vending/databases/frosting.db	frosting	Application traces
Userdata	/data/com.android.vending/databases/install_queue.db	install_requests	Application traces
Userdata	/data/com.android.vending/databases/library.db	ownership	Application traces
Userdata	/data/com.android.vending/databases/localappstate.db	appstate	Application traces
Userdata	/data/com.android.vending/databases/notification_cache	notifications	Application traces
Userdata	/data/com.android.vending/databases/package_verification.db	verification_cache	Application traces
Userdata	/data/com.android.vending/databases/suggestions.db	suggestions	Application traces
Userdata	/data/com.android.vending/databases/verify_apps.db	*	Application traces
Userdata	/data/com.google.android.gms/databases/config.db	main	Application traces
Userdata	/data/com.google.android.gms/databases/gass.db	app_info	Application traces
Userdata	/data/com.google.android.gms/databases/gcm_registrar.db	packages	Application traces
Userdata	/data/com.google.android.gms/databases/google_app_measurement.db	*	Application traces
Userdata	/data/com.google.android.gms/shared_prefs/batterystats.xml	N/A	Battery Usage Stats - Contains Application Usage information
Userdata	/data/com.google.android.googlequicksearchbox/*	N/A	Google App searches, installed applications and more
Userdata	/data/com.samsung.android.providers.context.databases.ContextLog_0.db	*	Application traces (Samsung devices)
Userdata	/data/com.sec.android.app.launcher/databases/launcher.db	N/A	Application artifacts (even after deleted)
Userdata	/data/data/com.google.android.gms/files/batterystatsdumpsystask.gz	N/A	Battery Usage Stats - Contains Application Usage information
Userdata	/system/appops.xml	N/A	Application permissions
Userdata	/system/batterystats.bin	N/A	Battery Usage Stats - Contains Application Usage information
Userdata	/system/batterystats-checkin.bin	N/A	Battery Usage Stats - Contains Application Usage information
Userdata	/system/batterystats-daily.xml	N/A	Battery Usage Stats - Contains Application Usage information
Userdata	/system/dmappmgr.db	N/A	Application Usage
Userdata	/system/job/jobs.xml	N/A	Application Usage
Userdata	/system/notification_log.db	N/A	Application notifications
Userdata	/system/packages.list	N/A	Application permissions and metadata
Userdata	/system/packages.xml	N/A	Application permissions
Userdata	/system/usagestats/0/*	N/A	Application Usage Stats
Userdata	/system/users/0/app_idle_stats.xml	N/A	Application Usage
Userdata	/system_ce/0/recent_images/*.png	N/A	Application snapshots
Userdata	/system_ce/0/recent_tasks/*.xml	N/A	Recent Tasks
Userdata	/log/sdp_log - valid and invalid lockscreen code attempts	N/A	Valid and invalid lockscreen code attempts

NATIVE APPLICATIONS

Partition	Path	Tables of Interest	Description
Userdata	/data/com.android.providers.calendar/databases/calendar.db	*	Calendar Items
Userdata	/data/com.android.providers.contacts/databases/contacts2.db	contacts & raw contacts	Contacts
Userdata	/data/com.android.providers.contacts/databases/contacts2.db	calls	Call Logs
Userdata	/data/com.android.providers.contacts/databases/calllog.db	calls	Call Logs
Userdata	/data/com.android.providers.downloads/databases/downloads.db	*	Downloads
Userdata	/data/com.google.android.gms/databases/icing_contacts.db	*	Contacts
Userdata	/data/com.google.android.gms/databases/icing_mmssms.db		MMS/SMS
Userdata	/data/com.google.android.gms/databases/ipa_mmssms.db	*	MMS/SMS
Userdata	/data/com.google.android.gms/databases/android_pay	wallet	Android Pay
Userdata	/data/com.google.android.gms/databases/pluscontacts.db	*	Google+ Contacts

https://t.me/learningnets