SANS

iOS Third-Party Apps Forensics

REFERENCE GUIDE

The aim of this poster is to provide a list of the most interesting files and folders in the "Data" and "Shared" folders for the most commonly used third-party apps.

DFPS_iOS-APPS-v1.3_04-24
This poster was created by Mattia Epifani (@mattiaep) with support of the SANS DFIR Faculty. ©2024 Mattia Epifani. All Rights Reserved.

iOS third-party apps can be installed from the Apple App Store, where they are organized based on categories (e.g., Social Networking, Business/Productivity, Navigation & Travel, and so on).

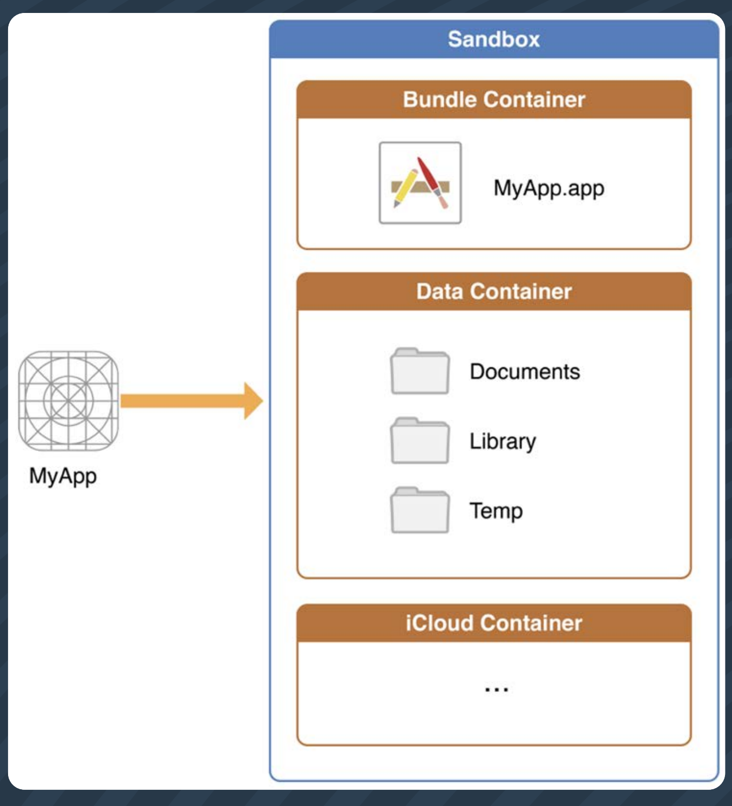
Once an app is installed on an iOS device:

- App Bundle is installed in a subfolder in the **/private/var/containers/Bundle** folder
- App Data is stored in a subfolder in the **/private/var/mobile/Containers/Data/Application/** folder (App Sandbox)

The easiest way to track down an iOS application's Data folder is to analyze the **/private/var/mobile/Library/FrontBoard/applicationstate.db** database, as described in a blog post by Alexis Brignoni[2].

Some Apps can also store data in other subfolders like the **/private/var/mobile/Containers/Share/AppGroup/** folder. Two good ways to locate the Sandbox folder for the AppGroup are mentioned in blog posts by Scott Vance[3] and Yogesh Khatri[4].

The internal structure of an App folder can be determined by the developer, but Apple provides some guidelines in its *File System Programming Guide*[5].



1

[1] Image is extracted from: https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html
[2] https://abrignoni.blogspot.com/2018/12/identifying-installed-and-uninstalled.html
[3] https://blog.d204n6.com/2020/09/ios-tracking-bundle-ids-for-containers.html
[4] https://www.swiftforensics.com/2021/01/ios-application-groups-shared-data.html
[5] https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html

Business/Productivity

Doodle

APPSTORE URL: **https://apps.apple.com/us/app/doodle-easy-scheduling/id938182547**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	doodle.yapdb	SQLite
/Library/Caches/com.doodle.Doodle-App/fsCachedData/	*	Various
/Library/Preferences/	com.doodle.Doodle-App.plist	Plist

Dropbox

APPSTORE URL: **https://apps.apple.com/us/app/dropbox-backup-sync-share/id327630330**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	spotlight.db	SQLite
/Documents/Users/<User_ID>/	Dropbox.sqlite	SQLite
/Documents/Users/<User_ID>/	metadata.db	SQLite
/Documents/Users/<User_ID>/	offline.db	SQLite
/Documents/Users/<User_ID>/	recent_actions_local.db	SQLite
/Documents/Users/<User_ID>/	recent_actions_server.db	SQLite
/Documents/Users/<User_ID>/	starred_infos_local.db	SQLite
/Library/Cache/Users/<User_ID>/FileCache/Loaded/	*	Various
/Library/Preferences/	com.getdropbox.Dropbox.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/File Provider Storage/<User-ID>/local-storage/	*	Various
/Library/Preferences/	group.com.getdropbox.Dropbox.plist	Plist
/Users/<User_ID>/	Dropbox.sqlite	SQLite
/Users/<User_ID>/	file_provider_metadata_with_assistant.db	SQLite
/Users/<User_ID>/	upload_queue_v2.db	SQLite
/Users/<User_ID>/FileCache/	*	Various

REFERENCES:
https://abrignoni.blogspot.com/2018/12/profiling-user-activity-in-dropbox-for.html
https://www.marshall.edu/forensics/files/Treleven-Dropbox-Paper-FINAL.pdf
https://arxiv.org/ftp/arxiv/papers/1709/1709.10395.pdf
https://link.springer.com/article/10.1007/s11227-020-03255-5
https://www.tandfonline.com/doi/abs/10.1080/00450618.2015.1110620?scroll=top&needAccess=true&journalCode=tajf20

Dust

APPSTORE URL: **https://apps.apple.com/us/app/dust-a-safer-place-to-text/id690158616**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	<User_ID>	Realm
/Documents/	contacts.json	JSON
/Documents/	default.realm	Realm
/Library/Preferences/	com.mentionmobile.cyberdust.plist	Plist
/SplashBoard/Snapshots/	*	KTX

REFERENCES:
https://www.nw3c.org/docs/research/dust.pdf

Eventbrite

APPSTORE URL: **https://apps.apple.com/us/app/eventbrite/id487922291**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	default.realm	Realm
/Library/Caches/com.eventbrite.attendee/com.alamofire.imagedownloader/fsCachedData/	*	JPG
/Library/Preferences/	com.eventbrite.attendee.plist	Plist

Gmail

APPSTORE URL: **https://apps.apple.com/us/app/gmail-email-by-google/id422689480**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	com.google.Gmail.plist	
/Library/Caches/com.google.commmon.SSO/<User_ID>/	Profile.plist	Plist
/Library/Caches/	Contacts_15_<User_ID>.db	SQLite
/Documents/drivekit/users/<User_ID>/gdx-cello/	cello.db	SQLite
/Library/Application Support/data/<Email_Address>/	sqlitedb	SQLite

Google Drive

APPSTORE URL: **https://apps.apple.com/us/app/google-drive/id507874739**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/<User_ID>/	comments_snapshot_<User_ID>.db	SQLite
/Documents/drivekit/users/<User_ID>/cello/	cello.db	SQLite
/Documents/drivekit/users/<User_ID>/files/	*	Various
/Documents/drivekit/users/<User_ID>/logs/	*	TXT
/Documents/drivekit/users/<User_ID>/thumbnails/	*	Various
/Library/Caches/drivekit/users/<User_ID>/image-fetcher-cache/main-cache/	cacheV0.db	SQLite
/Library/Preferences/	com.google.Drive.plist	Plist

LinkedIn

APPSTORE URL: **https://apps.apple.com/us/app/linkedin-network-job-finder/id288429040**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	Messenger.sqlite	SQLite
/Documents/	msg_database.sqlite	SQLite
/Documents/LIImageCache/	*	Various
/Documents/LIMediaAVPlaybackDiskCache/	*	Various
/Library/Caches/WebKit/NetworkCache/	*	Various
/Library/Preferences/	com.linkedin.LinkedIn.plist	Plist

REFERENCES:
https://www.tandfonline.com/doi/abs/10.1080/00450618.2015.1066854?src=recsys&journalCode=tajf20
https://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?article=1017&context=electricalcomputerengineering-facpubs
https://it.scribd.com/document/57611870/Shmoocon-2011-Inside-the-App-All-Your-Data-are-Belong-to-Me

Mega

APPSTORE URL: **https://apps.apple.com/it/app/mega/id706857885**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/	karere-<Uder_ID>.db	SQLite
/Library/Application Support/	Megaclient_statecache13_<User_ID>.db	SQLite
/Library/Application Support/Uploads/	*	Various
/Library/Caches/com.hackemist.SDImageCache/ Various		*
/Library/Caches/mega.ios/	Cache.db	SQLite

REFERENCES:
https://abrignoni.blogspot.com/2018/12/profiling-user-activity-in-dropbox-for.html
https://www.marshall.edu/forensics/files/Treleven-Dropbox-Paper-FINAL.pdf
https://arxiv.org/ftp/arxiv/papers/1709/1709.10395.pdf
https://link.springer.com/article/10.1007/s11227-020-03255-5
https://www.tandfonline.com/doi/abs/10.1080/00450618.2015.1110620?scroll=top&needAccess=true&journalCode=tajf20

LogMeIn

APPSTORE URL: **https://apps.apple.com/us/app/logmein/id479229407**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/LogMeInConfig/	com.logmein.ignition.xml	XML
/Library/LogMeInConfig/	sessiondata.xml	XML
/Library/Preferences/	com.logmein.logmein.plist	Plist

Microsoft OneDrive

APPSTORE URL: **https://apps.apple.com/us/app/microsoft-onedrive/id477537958**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Database/	moddatabase.db	SQLite
/Library/Preferences/	com.microsoft.skydrive.plist	Plist
/SplashBoard/Snapshots/	*	KTX

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	group.com.microsoft.onedrive.plist	Plist
/OneDrive/DatabaseQT/	QTMetadata.db	SQLite
/OneDrive/StramCacheQT/	*	Various

REFERENCES:
https://digital-forensics.sans.org/summit-archives/Prague_Summit/Cloud_Storage_Forensics_Mattia_Eppifani.pdf

Microsoft Teams

APPSTORE URL: **https://apps.apple.com/us/app/microsoft-teams/id1113153706**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/.IntuneMAM/	Config.plist	Plist
/Library/Shiftr/	Shiftr.sqlite	SQLite
/Library/Preferences/	com.microsoft.skype.teams.plist	Plist
/SplashBoard/Snapshots/	*	KTX

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	group.com.microsoft.skype.teams.plist	Plist
/SkypeSpacesDogfood/<Team_ID>/	SkypeSpacesDogfood-<GUID>.sqlite	SQLite
/SkypeSpacesDogfood/Downloads/<Team_ID>/	*	Various

Proton Mail

APPSTORE URL: **https://apps.apple.com/us/app/protonmail-encrypted-email/id979659905**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/SentryCras/ProtonMail/Data/	CrashState.json	JSON
/Library/Preferences/	ch.protonmail.protonmail.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/	ProtonMail.sqlite	SQLite
/Library/Preferences/	group.ch.protonmail.protonmail.plist	Plist

REFERENCES:
https://xperylab.medium.com/protonmail-forensic-decryption-of-ios-app-8e9ae9f50953

Silent Phone

APPSTORE URL: **https://apps.apple.com/us/app/silent-phone/id554269204**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/ com.silentcircle.SilentPhone/Chat/	ChatMessages_cipher.db	SQLite
/Library/Application Support/com.silentcircle.SilentPhone/tivi/	axo_<User-ID>_secure_sql.db	SQLite
/Library/Application Support/com.silentcircle.SilentPhone/tivi/	zids_sqlite.db	SQLite
/Library/Preferences/	com.silentcircle.SilentPhone.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/com.silentcircle.SilentPhone/Chat/	*	JPG
/com.silentcircle.SilentPhone/Preferences/	preferences.plist	Plist

Slack

APPSTORE URL: **https://apps.apple.com/us/app/slack/id618783545**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/Slack/<Workspace_id>/Database/	main_db	SQLite
/Library/Caches/com.tinyspeck.chatlyio/fsCachedData/	*	JPG
/Library/Caches/default/com.hackemist.SDWebImageCache.default/	*	JPG
/Library/Preferences/	com.tinyspeck.chatlyio.plist	Plist

REFERENCES:
https://abrignoni.blogspot.com/2018/10/finding-slack-app-messages-in-ios.html

Tutanota

APPSTORE URL: **https://apps.apple.com/us/app/tutanota/id922429609**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	de.tutao.tutanota.plist	Plist
/Library/WebKit/WebsiteData/IndexedDB/v1/file__0/	IndexedDB.sqlite3	SQLite
/Library/WebKit/WebsiteData/LocalStorage/	file__0.localstorage	SQLite
/SplashBoard/Snapshots/	*	KTX

Wire

APPSTORE URL: **https://apps.apple.com/us/app/wire-secure-messenger/id930944768**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	com.wearezeta.zclient.ios.plist	Plist
/SplashBoard/Snapshots/	*	KTX

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/AccountData/<GUID>/store/	store.wiredatabase	SQLite
/Accounts/	*	JSON
/Library/Caches/	*	Various
/Library/Preferences/	group.com.wearezeta.zclient.ios.plist	Plist

REFERENCES:
https://www.x41-dsec.de/reports/X41-Kudelski-Wire-Security-Review-iOS.pdf
https://blog.oxygen-forensic.com/wire-app-extraction
https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf

Zoom

APPSTORE URL: **https://apps.apple.com/us/app/zoom-cloud-meetings/id546505307**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/data/	*	JPG
/Documents/data/	zoommeeting.db	SQLite
/Documents/data/	zoomus.db	SQLite
/Documents/data/	zoomus.tmp.db	SQLite
/Documents/data/<User_ID>/	<User_ID>@xmpp.zoom.us.asyn.db	SQLite
/Documents/data/<User_ID>/	<User_ID>@xmpp.zoom.us.db	SQLite
/Documents/data/<User_ID>/	<User_ID>@xmpp.zoom.us.idx.db	SQLite
/Documents/data/<User_ID>/	<User_ID>@xmpp.zoom.us.sync.db	SQLite
/Library/Preferences/	us.zoom.videomeetings.plist	Plist

REFERENCES:
https://www.hecfblog.com/2020/04/daily-blog-684-solution-saturday-42520.html

Navigation & Travel

Booking

APPSTORE URL: **https://apps.apple.com/us/app/booking-com-hotels-travel/id367003839**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/	BookingClouds	Plist
/Library/Application Support/	KeyValueStorageAccountDomain	Plist
/Library/Application Support/	KeyValueStorageRecentsDomain	Plist
/Library/Application Support/	KeyValueStorageSharedDomain	Plist
/Library/Caches/	location_cache_V2.db	SQLite
/Library/Caches/com.booking.BookingApp/com. alamofire.imagedownloader/fsCachedData/	*	JPG
/Library/Caches/com.booking.BookingApp/fsCachedData/	*	JSON
/Library/Preferences/	com.booking.BookingApp.plist	Plist

Foursquare Swarn

APPSTORE URL: **https://apps.apple.com/us/app/foursquare-swarm-check-in-app/id870161082**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/	foursquare.sqlite	SQLite
/Library/Preferences/	com.foursquare.robin.plist	Plist

Google Maps

APPSTORE URL: **https://apps.apple.com/us/app/google-maps-transit-food/id585027354**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/GMSCacheStorage-AZSpotlightStorageModel/GMSCacheStorage-AZSpotlightStorageModel/	AZSpotlightStorageModel.sqlite	SQLite
/Library/Application Support/	com.google.gscors.account.AllAccountsFile	Plist
/Library/Application Support/CachedRoutes/	*	Plist
/Library/Application Support/GMSCacheStorage-MyMaps/	MyMaps.sqlite	SQLite
/Library/Application Support/GMSCacheStorage-SavedUserEvent3/	SavedUserEvent3.sqlite	SQLite
/Library/Application Support/GMSCacheStorage-Tiles/	Tiles.sqlite	SQLite
/Library/Caches/ImageCache	*	JPG
/Library/Caches/com.google.commmon.SSO/<User_ID>/	Profile.plist	Plist
/Library/Preferences/	com.google.Maps.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	CurrentDirections	Plist
/Library/Preferences/	group.com.google.Maps.plist	Plist

REFERENCES:
https://commons.erau.edu/cgi/viewcontent.cgi?article=1414&context=jdfsl
https://www.ijrte.org/wp-content/uploads/papers/v8i4/D4374118419.pdf

KLM

APPSTORE URL: **https://apps.apple.com/us/app/klm/id391732065**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	CoreAppRedesign_iPhone.sqlite	SQLite
/Library/Caches/com.klm.mobile.iphone.klmmobile/fsCachedData/	*	Various
/Library/Preferences/	com.klm.mobile.iphone.klmmobile.plist	Plist

Lufthansa

APPSTORE URL: **https://apps.apple.com/us/app/lufthansa/id299219152**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	*	HTML
/Library/Application Support/	Database.sqlite	SQLite
/Library/Caches/com.lufthansa.launcher/fsCachedData/	*	XML
/Library/Preferences/	com.lufthansa.launcher.plist	Plist

Skyscanner

APPSTORE URL: **https://apps.apple.com/us/app/skyscanner-travel-deals/id415458524**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	MiniEvents.sqlite	SQLite
/Documents/WatchedFlights/	WatchedFlights.json	JSON
/Library/Caches/com.hackemist.SDImageCache/default/	*	JPG
/Library/Caches/net.skyscanner.iphone/netcache/	Cache.db	SQLite
/Library/Caches/net.skyscanner.iphone/netcache/fsCachedData/	*	JSON
/Library/Preferences/	net.skyscanner.iphone.plist	Plist

Tripadvisor

APPSTORE URL: **https://apps.apple.com/us/app/tripadvisor-hotels-vacation/id284876795**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	FSQPVisitStoreLocations.archive	Plist
/Documents/	geo_recents	Plist
/Documents/	logged_in_user_info	Plist
/Documents/	shortlist	Plist
/Documents/	ta-journal.sqlite	SQLite
/Documents/	TripAdvisor-Preferences.plist	Plist
/Documents/	typeahead_recents	Plist
/Documents/inbox/	db	SQLite
/Library/Caches/com.tripadvisor.LocalPicks/fsCachedData/	*	JSON
/Library/Caches/TIPImagePipeline/	*	JPEG
/Library/Preferences/	com.tripadvisor.LocalPicks.plist	Plist

Uber

APPSTORE URL: **https://apps.apple.com/us/app/uber/id368677368**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	database.db	SQLite
/Library/Application Support/com.ubercab.UberClient/	*	Various
/Library/Application Support/Persistent Storage/BootstrapStore/RealtimeRider.StreamModelKey/	client	JSON
/Library/Application Support/Persistent Storage/Store/PaymentFoundation.PaymentStreamModeKey/	eyeball	JSON
/Library/Application Support/Persistent Storage/BootstrapStore/RealtimeRider.StreamModelKey/	profiles	JSON
/Library/Caches/com.ubercab.UberClient/com.uber.images/fsCachedData/	*	Various
/Library/Preferences/	com.ubercab.UberClient.plist	Plist

REFERENCES:
https://www.researchgate.net/publication/323759986_A_Dynamic_and_Static_Analysis_of_the_Uber_Mobile_Application_from_a_Privacy_Perspective

Waze

APPSTORE URL: **https://apps.apple.com/us/app/waze-navigation-live-traffic/id323229106**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Document/	user	TXT
/Document/	session	TXT
/Document/	preferences	TXT
/Document/	user.db	SQLite
/Library/Preferences/	com.waze.iphone.plist	Plist

Utilities

Brave Browser

APPSTORE URL: **https://apps.apple.com/us/app/brave-private-browser-vpn/id1052879175**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/Downloads/	*	Various
/Library/Application Support/	Brave.sqlite	SQLite
/Library/Preferences/	com.brave.ios.browser.plist	Plist

Burner

APPSTORE URL: **https://apps.apple.com/us/app/burner-private-phone-line/id505800761**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/com.adhoclabs.burner/	Cache.db	SQLite
/Library/Caches/com.adhoclabs.burner/fsCachedData/	*	Various
/Library/Preferences/	com.adhoclabs.burner.plist	Plist
/SplashBoard/Snapshots/	*	KTX

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/	Phoenix.sqlite	SQLite

REFERENCES:
https://digitalforensicstips.com/2013/07/forensic-artifact-analysis-of-the-burner-app-for-the-iphone

DuckDuckGo Browser

APPSTORE URL: **https://apps.apple.com/us/app/duckduckgo-privacy-browser/id663592361**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	com.duckduckgo.mobile.ios.plist	Plist
/Library/Caches/WebKit/NetworkCache/Version 16/Records/	*	Various

Firefox

APPSTORE URL: **https://apps.apple.com/us/app/firefox-private-safe-browser/id989804926**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/WebKit/NetworkCache/	*	Various
/Library/Preferences/	org.mozilla.ios.Firefox.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/profile.profile/	browser.db	SQLite
/profile.profile/	logins.db	SQLite
/profile.profile/	places.db	SQLite
/profile.profile/	tabState.archive	Plist
/Library/Preferences/	group.org.mozilla.ios.Firefox.plist	Plist

Firefox Focus

APPSTORE URL: **https://apps.apple.com/us/app/firefox-focus-privacy-browser/id1055677337**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	org.mozilla.ios.Focus.plist	Plist
/Library/Caches/KSCrash/Firefox Focus/Data/	CrashState.json	JSON

Google Chrome

APPSTORE URL: **https://apps.apple.com/us/app/google-chrome/id535886823**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/Google/Chrome/Default/	*	Various
/Library/Caches/com.google.commmon.SSO/<User_ID>/	Profile.plist	Plist
/Library/Preferences/	com.google.chrome.ios.plist	Plist

Microsoft Edge

APPSTORE URL: **https://apps.apple.com/us/app/microsoft-edge-web-browser/id1288723196**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	OfflineCache.sqlite	SQLite
/Documents/CitrixLogs/Diagnostics/	*	CSV
/Documents/TabScreenshot/	*	JPG
/Library/Application Support/ChromeSync/	*	Various
/Library/Caches/com.microsoft.msedge/fsCachedData/	*	Various
/Library/Preferences/	com.microsoft.msedge.plist	Plist

Onion Browser

APPSTORE URL: **https://apps.apple.com/us/app/onion-browser/id519296448**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	bookmarks.plist	Plist
/Library/Caches/com.miketigas.OnionBrowser/	Cache.db	SQLite
/Library/Caches/tor/	state	TXT
/Library/Preferences/	com.miketigas.OnionBrowser.plist	Plist

REFERENCES:
https://roselabs.nl/files/audit_reports/Cure53_-_Onion_Browser.pdf

Finance

Paypal

APPSTORE URL: **https://apps.apple.com/us/app/paypal/id283646709**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	com.yourcompany.PPClient.plist	Plist

Venmo

APPSTORE URL: **https://apps.apple.com/us/app/venmo/id351727428**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	Model.sqlite	SQLite
/Documents/	mParticle28.db	SQLite
/Library/Caches/com.hackemist.SDImageCache/default/	*	Various
/Library/Preferences/	net.kortina.labs.Venmo.plist	Plist
/SplashBoard/Snapshots/	*	KTX

REFERENCES: **https://thebinaryhick.blog/2019/11/07/venmo-the-app-for-virtual-ballers**

Social Networking

BeReal

APPSTORE URL: **https://apps.apple.com/us/app/bereal-your-friends-for-real/id1459645446**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/disk-bereal-ProfileRepository/	*	JSON
/Library/Caches/disk-bereal-RelationshipContactsManager-contact/	*	JSON
/Library/Caches/AlexisBarreyat.BeReal/	Cache.db	SQLite
/Library/Caches/AlexisBarreyat.BeReal/fsCachedData/	*	Various
/Library/Caches/com.hackemist.SDImageCache/default/	*	Various

Discord

APPSTORE URL: **https://apps.apple.com/us/app/discord-talk-chat-hang-out/id985746746**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/mmkv/	mmkv.default	JSON
/Documents/RCTAsyncLocalStorage_V1/	<GUID>	JSON
/Documents/RCTAsyncLocalStorage_V1/	manifest.json	JSON
/Library/Caches/com.hackemist.SDImageCache/	*	PNG
/Library/Caches/com.hammerandchisel.discord/	Cache.db	SQLite
/Library/Caches/com.hammerandchisel.discord/fsCachedData/	*	JSON
/Library/Preferences/	com.hammerandchisel.discord.plist	Plist

REFERENCES:

https://abrignoni.blogspot.com/2018/08/finding-discord-chats-in-ios.html

https://abrignoni.blogspot.com/2020/08/update-on-discord-forensic-artifacts.html

https://www.nw3c.org/docs/research/discord.pdf

https://bluecrewforensics.com/2023/10/30/connecting-discord-attachments-threads-sdwebimage-library

Facebook

APPSTORE URL: **https://apps.apple.com/us/app/facebook/id284882215**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	time_in_app_<User_ID>.db	SQLite
/Documents/cask/<User_ID>/FBMessagingMailboxCaskStore/1	fb-msys-<User_ID>.db	SQLite
/Library/Caches/com.facebook.Facebook.MosaicIGImageDiskCache/	*	Various
/Library/Caches/com.facebook.Facebook/fsCachedData	*	Various
/Library/Caches/graphStoreDB/	GraphStore_<User_ID>.sqlite3	SQLite
/Library/Caches/messenger_contacts.<GUID>/	fbsyncstore.db	SQLite
/Library/Caches/search_bootstrap.<GUID>/search/	graph_search_entity_bootstrap.data	File
/Library/Caches/video_cache.<GUID>/storage/	*	Plist
/Library/Preferences/	com.facebook.Facebook.plist	Plist

REFERENCES:

https://www.academia.edu/10726810/Social_Media_Forensics_on_Mobile_Devices

https://www.tandfonline.com/doi/abs/10.1080/00450618.2015.1066854?src=recsys&journalCode=tajf20

https://www.fbiic.gov/public/2011/jul/Facebook_Forensics-Finalized.pdf

https://www.researchgate.net/publication/224221519_Third_Party_Application_Forensics_on_Apple_Mobile_Devices

https://www.diva-portal.org/smash/get/diva2:651693/fulltext01.pdf

Facebook Messenger

APPSTORE URL: **https://apps.apple.com/us/app/messenger/id454638411**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/com.facebook.Messenger.preferences/	<User_ID>.session	Plist
/Documents/messenger_secure_messages.sessionless.1/	<User_ID>_threadStateStore.db	SQLite
/Documents/messenger_secure_messages.sessionless.1/	<User_ID>_v1464784789_tincan.db	SQLite
/Library/Caches/graphStoreDB/	GraphStore_<User_ID>.sqlite3	SQLite
/Library/Preferences/	com.facebook.Messenger.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/lightspeed-userDatabase/	<User_ID>.db	SQLite
/_store_<GUID>/messenger_contacts.v1/	fbomnistore.db	SQLite
/shared_messenger_contacts.<GUID>/	fbomnistore.db	SQLite
/shared_messenger_messages.<GUID>/	orca2.db	SQLite
/lightspeed-imageCache/	*	Various

REFERENCES:

https://www.academia.edu/10726810/Social_Media_Forensics_on_Mobile_Devices

https://boncaldoforensics.wordpress.com/2018/07/28/facebook-messenger-windows-app-store-forensics

https://www.champlain.edu/Documents/LCDI/iPhone%20Artifacts.pdf

https://sqliteforensictoolkit.com/forensic-browser-for-sqlite-structured-storage-manager

Google Chat

APPSTORE URL: **https://apps.apple.com/it/app/google-chat/id1163852619**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/user_account/<User_ID>/	dynamite.db	SQLite
/Library/Caches/ImageFetcherCache/	cacheV0.db	SQLite
/Library/Preferences/	com.google.Dynamite.plist	Plist

Google Meet

APPSTORE URL: **https://apps.apple.com/us/app/google-duo/id1096918571**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/logs/	*	TXT
/Library/Application Support/	DataStore	SQLite
/Library/Caches/com.google.commmon.SSO/<User_ID>/	Profile.plist	Plist
/Library/Preferences/	com.google.Tachyon.plist	Plist

imo

APPSTORE URL: **https://apps.apple.com/us/app/imo-video-calls-and-chat-hd/id1400579543**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	imo_acc	Plist
/Documents/	imo_last_ts_log_appAlive	Plist
/Documents/	imo_save_media_local_setting_1	Plist
/Documents/	imo_stories	Plist
/Library/Caches/default/com.hackemist.SDWebImageCache.default/	*	Various
/Library/Caches/videos/	*	Various
/Library/Preferences/	co.babypenguin.imo.plist	Plist
/SplashBoard/Snapshots/	*	KTX

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/	IMODb2.sqlite	SQLite
/	IMOShareDb.sqlite	SQLite
/Library/Preferences/	group.co.babypenguin.plist	Plist

REFERENCES:

https://www.sciencedirect.com/science/article/abs/pii/S1742287618300094

http://prr.hec.gov.pk/jspui/bitstream/123456789/13429/1/Muhammad%20Asad%20Khan%20Sudozai%20electrical%20engg%202019%20NUST%20isb%20prr.pdf

Kik Messenger

APPSTORE URL: **https://apps.apple.com/us/app/kik/id357218860**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/com.hackemist.SDImageCache/default/	*	Various
/Library/Caches/com.kik.chat/fsCachedData/	*	Various
/Library/Preferences/	com.kik.chat.plist	Plist
/SplashBoard/Snapshots/	*	KTX

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/cores/private/<User-ID>/	kik.sqlite	SQLite
/cores/private/<User-ID>/app-lock/	app-lock-settings	JSON
/cores/private/<User-ID>/attachments/	*	Various
/cores/private/<User-ID>/defaults/	kik.defaults	Plist
/cores/private/<User-ID>/globalDefaults/	kik.defaults	Plist
/cores/private/<User-ID>/suggested-chats/	suggested	JSON
/cores/private/<User-ID>/urlData/	*	PNG
/globalDefaults/	kik.defaults	Plist
/Library/Preferences/	group.com.kik.chat.plist	Plist

REFERENCES:

https://www.sciencedirect.com/science/article/pii/B9781597496599000067

https://researchonline.gcu.ac.uk/files/24282895/K.Ovens_revisedKMOvensManuscript3_2.pdf

https://www.scribd.com/doc/145278610/Artefacts-of-Kik-Messenger-on-iOS

https://blog.oxygen-forensic.com/kickin-kik

https://dfir.pubpub.org/pub/z29xp2bu/release/1

MeWe

APPSTORE URL: **https://apps.apple.com/us/app/mewe-network/id918464474**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	Sgroupledb.sqlite	SQLite
/Library/Caches/com.mewe/fsCachedData/	*	Various
/Library/Caches/com.hackemist.SDImageCache/	*	Various
/Library/Preferences/	com.mewe.plist	Plist

LINE

APPSTORE URL: **https://apps.apple.com/us/app/line/id443904275**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/PrivateStore/	*	Various
/Library/Caches/jp.naver.line/fsCachedData/	*	Various
/Library/Preferences/	jp.naver.line.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/KeepFileProvider/	Keep.sqlite	SQLite
/Library/Application Support/PrivateStore/<User-ID>/Messages/	ChetExt.sqlite	SQLite
/Library/Application Support/PrivateStore/<User-ID>/Messages/	E2EEData.sqlite	SQLite
/Library/Application Support/PrivateStore/<User-ID>/Messages/	Line.sqlite	SQLite
/Library/Preferences/	group.com.linecorp.line.plist	Plist

REFERENCES:

https://prezi.com/mloxlacowypf/iphone-forensic-line/

https://reincubate.com/support/how-to/recover-iphone-hike-line-wechat-messages/

https://pdfs.semanticscholar.org/fe66/52f6fe64ce1af44dd7d433ecf5a00b57ca0a.pdf

Signal

APPSTORE URL: **https://apps.apple.com/us/app/signal-private-messenger/id874139669**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/	*	JPG
/Library/Logs/	*.log	TXT
/Library/Preferences/	org.whispersystems.signal.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/Attachments/	*	Various
/grdb/	signal.sqlite	SQLite
/Library/Preferences/	group.org.whispersystems.signal.group.plist	Plist
/ProfileAvatars/	*	JPG

REFERENCES:

https://github.com/Magpol/HowTo-decrypt-Signal.sqlite-for-iOS

https://support.magnetforensics.com/s/article/Decrypt-app-data-using-the-iOS-Keychain-and-GrayKey

https://pdfs.semanticscholar.org/fe66/52f6fe64ce1af44dd7d433ecf5a00b57ca0a.pdf

https://isc.sans.edu/forums/diary/Looking+for+the+insider+Forensic+Artifacts+on+iOS+Messaging+App/21363

http://www.ijits-bg.com/contents/IJITS-No4-2019/2019-N4-07.pdf

https://www.sciencedirect.com/science/article/pii/S2666281722000166

https://blog.elcomsoft.com/2019/08/how-to-extract-and-decrypt-signal-conversation-history-from-the-iphone

Skout

APPSTORE URL: **https://apps.apple.com/us/app/skout-meet-new-people/id302324249**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/SKOUT/	SKCache.sqlite	SQLite
/Library/Caches/default/com.hackemist.SDWebImageCache.default/	*	Various
/Library/Preferences/	com.skout.SKOUT.plist	Plist
/SplashBoard/Snapshots/	*	KTX

Skype

APPSTORE URL: **https://apps.apple.com/us/app/skype-for-iphone/id304878510**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/RCTAsyncLocalStorage_V1/	manifest.json	JSON
/Library/Application Support/Skype4LifeSlimCore/<Skype_Username>/	main.db	SQLite
/Library/Caches/Logs/	com.skype.*.log	TXT
/Library/LocalDatabase/	s4l-<Skype_Username>.db	SQLite
/Library/Preferences/	com.skype.skype.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/	s4l-<Skype_Username>.db	SQLite

REFERENCES:

https://bebinary4n6.blogspot.com/2019/07

https://pdfs.semanticscholar.org/fe66/52f6fe64ce1af44dd7d433ecf5a00b57ca0a.pdf

Telegram

APPSTORE URL: **https://apps.apple.com/us/app/telegram-messenger/id686449807**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	ph.telegra.Telegraph.plist	Plist
/Library/Caches/ph.telegra.Telegraph/fsCachedData/	*	Various

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/telegram-data/account-<Account_ID>/postbox/db/	db_sqlite	SQLite
/telegram-data/account-<Account_ID>/postbox/media/	*	Various
/telegram-data/logs/	*	TXT
/telegram-data/share-logs/	*	TXT

REFERENCES:

https://www.forensicfocus.com/news/telegram-messenger-data-extraction-in-oxygen-forensic-detective

TextNow

APPSTORE URL: **https://apps.apple.com/us/app/textnow-call-text-unlimited/id314716233**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	<User-ID>	SQLite
/Documents/com.hackemist.SDWebImageCache.default/	*	JPG
/Library/Application Support/	eventHistory.db	SQLite
/Library/Caches/Logs/sip/	*.log	TXT
/Library/Caches/media/	*	JPG
/Library/Preferences/	com.tinginteractive.usms.plist	Plist

Tinder

APPSTORE URL: **https://apps.apple.com/us/app/tinder-dating-new-people/id547702041**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/	Tinder2.sqlite	SQLite
/Library/Preferences/	com.cardify.tinder.plist	Plist

Threema

APPSTORE URL: **https://apps.apple.com/us/app/threema-the-secure-messenger/id578665578**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	ProfilePicture.out	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Preferences/	group.ch.threema.plist	Plist
/Library/	ThreemaData.sqlite	SQlite

REFERENCES:

https://www.sciencedirect.com/science/article/pii/S2666281722000166

Viber Messenger

APPSTORE URL: **https://apps.apple.com/us/app/viber-messenger-chats-calls/id382617920**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/Attachments/	*	Various
/Documents/ChatExIcons/	*	Various
/Documents/UserEngagement/	*	Various
/Library/Caches/com.viber/fsCachedData/	*	Various
/Library/Preferences/	com.viber.plist	Plist
/SplashBoard/Snapshots/	*	KTX

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/com.viber/AttachmentsPreview/	*	Various
/com.viber/ContactIcons/	*	JPG
/com.viber/database/	Contacts.data	SQLite
/com.viber/settings/	Settings.data	SQLite

REFERENCES:

https://pdfs.semanticscholar.org/fe66/52f6fe64ce1af44dd7d433ecf5a00b57ca0a.pdf

https://blog.oxygen-forensic.com/viber-messenger-forensics

https://blog.digital-forensics.it/2019/12/checkra1n-era-ep-4-analyzing.html

WeChat

APPSTORE URL: **https://apps.apple.com/us/app/wechat/id414478124**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/<User_ID>/	mmsetting.archive	Plist
/Documents/<User_ID>/	wc005_008.db	SQLite
/Documents/<User_ID>/DB/	MM.sqlite	SQLite
/Documents/<User_ID>/DB/	WCDB_Contact.sqlite	SQLite
/Library/Preferences/	com.tencent.xin.plist	Plist

REFERENCES:

https://www.researchgate.net/publication/261016959_Forensic_Analysis_of_Social_Networking_Application_on_iOS_devices

https://www.ictsecuritymagazine.com/articoli/wechat-forensics-parte-i

WhatsApp Messenger

APPSTORE URL: **https://apps.apple.com/us/app/whatsapp-messenger/id310633997**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	Blockedcontacts.dat	Plist
/Documents/	calls.backup.log	Plist
/Documents/	StatusMessages.plist	Plist
/Library/Caches/ChatMedia/	*	Various
/Library/Caches/GalleryMedia/	*	Various
/Library/Caches/net.whatsapp.WhatsApp/fsCachedData/	*	Various
/Library/Caches/spotlight-profile-v2/	*	PNG
/Library/Logs/	whatsapp-*.log	TXT
/Library/Preferences/	net.whatsapp.WhatsApp.plist	Plist
/SplashBoard/Snapshots/	*	KTX

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/	calls.log	Plist
/	CallHistory.sqlite	SQLite
/	ChatStorage.sqlite	SQLite
/	ContactsV2.sqlite	SQLite
/	current_wallpaper.jpg	JPG
/	Location.sqlite	SQLite
/Biz/	Biz.sqlite	SQLite
/fts/	ChatSearch*.sqlite	SQLite
/Library/Preferences/	group.net.whatsapp.WhatsApp.shared.plist	Plist
/Media/Profile/	*	Various
/Message/Media/	*	Various
/stickers/	*	Various

REFERENCES:

https://www.group-ib.com/blog/whatsapp_forensic_artifacts

https://pdfs.semanticscholar.org/fe66/52f6fe64ce1af44dd7d433ecf5a00b57ca0a.pdf

https://sudonull.com/post/30099-WhatsApp-in-the-palm-of-your-hand-where-and-how-can-you-detect-forensic-artifacts-Group-IB-Blog

https://www.ijesm.co.in/uploads/68/5543_pdf.pdf

http://www.securitybydefault.com/2011/06/what-whatsapp-doesnt-tell-you.html

Wickr

APPSTORE URL: **https://apps.apple.com/us/app/aws-wickr/id1200926568**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/KSCrashReports/Wickr Me/	*	JSON
/Library/Caches/Sessions/Wickr Me/	*	JSON
/Library/Preferences/	com.mywickr.wickr.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/	wickrLocal.sqlite	SQLite

REFERENCES:

https://thebinaryhick.blog/2019/08/23/wickr-alright-well-call-it-a-draw

https://blog.oxygen-forensic.com/wickr-some-forensics-up

https://support.magnetforensics.com/s/article/Decrypt-app-data-using-the-iOS-Keychain-and-GrayKey

https://www.sciencedirect.com/science/article/pii/S2666281722000166

Entertainment/Photo & Video

Amazon Prime Video

APPSTORE URL: **https://apps.apple.com/us/app/amazon-prime-video/id545519333**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/<ID>/	store	JSON
/Library/Application Support/com.amazon.AIVWebImageCache/	*	Various
/Library/Caches/com.amazon.AIVAdvertCache/	*	Various
/Library/Preferences/	com.amazon.aiv.AIVApp.plist	Plist

Google Photos

APPSTORE URL: **https://apps.apple.com/us/app/google-photos/id962194608**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/com.google.commmon.SSO/<User_ID>/	Profile.plist	Plist
/Library/Application Support/store/	collections-<User_ID>	SQLite
/Library/Application Support/store/	photos-<User_ID>	SQLite
/Library/Caches/com.google.photos/ImageFetcherCache/	cacheV0.db	SQLite
/Library/Caches/com.google.photos/ImageFetcherCache_proxy/	cacheV0.db	SQLite
/Library/Preferences/	com.google.photos.plist	Plist

Imgur

APPSTORE URL: **https://apps.apple.com/us/app/imgur-funny-meme-gif-maker/id639881495**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	default.realm	Realm
/Library/Caches/com.hackemist.SDImageCache/default/	*	Various
/Library/Caches/Logs/	*.log	TXT
/Library/Preferences/	imgurmobile.plist	Plist

REFERENCES:

https://abrignoni.blogspot.com/2019/12/ios-imgur-app-realm-database-example.html

Instagram

APPSTORE URL: **https://apps.apple.com/us/app/instagram/id389801252**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	time_in_app_<User_ID>.db	SQLite
/Library/Caches/<User_ID>/	*	Various
/Library/Caches/com.burbn.instagram.IGImageCache/	*	Images
/Library/Caches/com.burbn.instagram.IGSparseVideoCache/	*	Videos
/Library/Caches/com.burbn.instagram.IGSparseVideoPrefetchCacheForNewCacheKey/	*	Videos
/Library/Caches/Items/	lastentries.<User_ID>.1.coded	Plist
/Library/Caches/Items/	lastentries-quickCache.<User_ID>.1.coded	Plist
/Library/Caches/Items/	lastentries-fullCache.<User_ID>.1.coded	Plist
/Library/Application Support/<User_ID>/	pending-requests.plist	Plist
/Library/Application Support/DirectSQLiteDatabase/	<User_ID>.db	SQLite
/Library/Preferences/	com.burbn.instagram.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/<User_ID>/user_bootstrap/	shared_bootstraps.plist	SQLite
/Library/Preferences/	group.com.burbn.instagram.plist	Plist

REFERENCES:

https://salt4n6.com/2018/05/15/a-few-interesting-ios-forensic-artefacts

http://xml.jips-k.org/full-text/view?doi=10.3745/JIPS.03.0097

https://www.forensicfocus.com/articles/forensic-analysis-of-third-party-application-instagram

Netflix

APPSTORE URL: **https://apps.apple.com/us/app/netflix/id363590051**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	store.sqlite	SQLite
/Library/assetCache/	*	JPG
/Library/Caches/br/ch/	*	Various
/Library/Caches/com.netflix.Netflix/	Cache.db	SQLite
/Library/Caches/com.netflix.Netflix/fsCachedData/	*	Various
/Library/Preferences/	com.netflix.Netflix.plist	Plist

Pinterest

APPSTORE URL: **https://apps.apple.com/us/app/pinterest/id429047995**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	activeUser	Plist
/Documents/	activeUser<User_ID>	Plist
/Library/Caches/com.pinterest.PINDiskCache.PINRemoteImageManagerCache/	*	Various
/Library/Caches/com.pinterest.PINDiskCache.PINRemoteModelCache/	*	Various
/Library/Preferences/	pinterest.plist	Plist

Private Photo Vault

APPSTORE URL: **https://apps.apple.com/us/app/private-photo-vault-pic-safe/id417571834**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/	PPVCoreData.sqlite	SQLite
/Library/PPV_Pics/	*	Various
/Library/Preferences/	com.enchantedcloud.photovault.plist	Plist

REFERENCES:

https://cdn.ymaws.com/www.oshean.org/resource/resmgr/Email/ruledtheword.pdf

Snapchat

APPSTORE URL: **https://apps.apple.com/us/app/snapchat/id447188370**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	user.plist	Plist
/Documents/	chatConversationStore.plist	Plist
/Documents/	friendsForAsyncDecode.plist	Plist
/Documents/	stories.plist	Plist
/Documents/gallery_data_object/1/<User_ID>/	scdb-27.sqlite3	SQLite
/Documents/global_scoped/Gallery/	*	Various
/Documents/user_scoped/<User_ID>/arroyo/	arroyo.db	SQLite
/Documents/user_scoped/<User_ID>/databases/	memories_asset_repository.sqite	SQLite
/Documents/user_scoped/<User_ID>/DocObjects/	primary.docobjects	SQLite
/Documents/user_scoped/<User_ID>/TIV/	tiv.db	SQLite
/Documents/user_scoped/<User_ID>/userPreferences/	pref.docobjects	SQLite
/Library/Caches/com.snap.file_manager_<Number>_SCContent_<GUID>/	*	Various
/Library/Caches/SCCache/	*	Various
/Library/Preferences/	com.toyopagroup.picaboo.plist	Plist

REFERENCES:

https://www.researchgate.net/profile/Imam_Riadi/publication/320467249_The_digital_forensic_analysis_of_snapchat_application_using_XML_records/links/59e73e87a6fdcc0e882d82e7/The-digital-forensic-analysis-of-snapchat-application-using-XML-records.pdf

https://www.marshall.edu/forensics/files/Cindy-Q.-Wu-Forensic-Analysis-of-Data-Transience-PPT.pdf

https://resources.infosecinstitute.com/ios-application-security-part-10-ios-filesystem-and-forensics/#gref

https://doubleblak.com/blogPosts.php?id=5

http://www.carpeindicium.com/blog/gone_10-seconds

Spotify

APPSTORE URL: **https://apps.apple.com/us/app/spotify-music-and-podcasts/id324684580**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/PersistentCache/	mercury.db	SQLite
/Library/Application Support/PersistentCache/Storage/	*	JPG
/Library/Application Support/Users/<User_ID>-user/	*	Various
/Library/Caches/com.spotify.client/nsurlcache/fsCachedData/	*	JPG
/Library/Preferences/	com.spotify.client.plist	Plist

REFERENCES:

https://arstechnica.com/information-technology/2016/11/for-five-months-spotify-has-badlyabused-users-storage-drives

https://thinkdfir.com/2019/01/11/what-did-i-listen-to-on-spotify-for-ios

TikTok

APPSTORE URL: **https://apps.apple.com/us/app/tiktok/id835599320**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	AwemeIM.db	SQLite
/Documents/drafts/	*	Various
/Library/Application Support/ChatFiles/<User-ID>/	db.sqlite	SQLite
/Library/AWEStorage/	UnifyStorage.sqlite	SQLite
/Library/AWEVideoCache/FileCache/	*	M4V
/Library/Caches/com.ibireme.yykit/images/data/	*	Various
/Library/Caches/TTPlayerCache/	*	M4V
/Library/Heimdallr/	heimdallr.db	SQLite
/Library/Preferences/	com.zhiliaoapp.musically.plist	Plist

REFERENCES:

https://abrignoni.blogspot.com/2018/11/finding-tiktok-messages-in-ios.html

https://www.systoolsgroup.com/updates/retrieve-messages-from-tiktok

https://blog.oxygen-forensic.com/whos-knocking-tiktok

https://dfir.pubpub.org/pub/h6vyh33u/release/1

YouTube

APPSTORE URL: **https://apps.apple.com/us/app/youtube-watch-listen-stream/id544007664**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/com.google.commmon.SSO/<User_ID>/	Profile.plist	Plist
/Library/Caches/com.pinterest.PINDiskCache.com.youtube.innertube.imageservice.cache/	*	Various
/Library/Preferences/	com.google.ios.youtube.plist	Plist

News

Reddit

APPSTORE URL: **https://apps.apple.com/us/app/reddit/id1064216828**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/release02/accounts/	*	Plist
/Documents/release02/accountData/	*	Plist
/Library/Caches/com.reddit.Reddit/com.alamofire.imageDownloader/	*	Images
/Library/Caches/com.reddit.Reddit/com.github.kean.Nuke.Cache/	*	Images
/Library/Caches/com.reddit.Reddit/fsCachedData/	*	Various
/Library/Caches/com.reddit.Reddit/imagedownload/fsCachedData/	*	Various
/Library/Preferences/	com.reddit.Reddit.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/accounts	*	Plist

X (Twitter)

APPSTORE URL: **https://apps.apple.com/us/app/x/id333903271**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/com.atebits.tweetie.application-important-state/	*	Various
/Documents/com.atebits.tweetie.application-state/	app.acct.<Twitter_Username>	Plist
/Documents/com.atebits.tweetie.compose.attachments/	*	JPG
/Documents/com.atebits.tweetie.direct-message.attachments/	*	Various
/Library/Caches/com.atebits.Tweetie2/fsCachedData/	*	Various
/Library/Caches/com.atebits.tweetie.direct-message.cache/	<User_ID>-<User_Number>	Plist
/Library/Caches/com.twitter.simple.disk.caches/	*	MP4
/Library/Caches/TIPImagePipeline/	*	PNG
/Library/Preferences/	com.atebits.Tweetie2.plist	Plist

/private/var/mobile/Containers/Shared/AppGroup/<APP_GUID>

Internal App Path	File Name	File Type
/com.atebits.tweetie.scribe/	Scribe.2.sqlite-sqlite	SQLite
/Library/Preferences/	group.com.atebits.Tweetie2.plist	Plist
/TFSModelCache.1/<User_ID>/database/	modelCache.sqlite3	SQLite

REFERENCES:

http://cs.lewisu.edu/mathcs/msisprojects/papers/kevinswartz.pdf

https://www.academia.edu/10726810/Social_Media_Forensics_on_Mobile_Devices

https://www.tandfonline.com/doi/abs/10.1080/00450618.2015.1066854?src=recsys&journalCode=tajf20

Reference

Google Translate

APPSTORE URL: **https://apps.apple.com/us/app/google-translate/id414706506**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	translate.db	SQLite
/Library/Preferences/	com.google.Translate.plist	Plist

Health & Fitness

Fitbit

APPSTORE URL: **https://apps.apple.com/us/app/fitbit-health-fitness/id462638897**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/	fitbit.sqlite	SQLite
/Library/Application Support/Fitbit/Defaults/	UserInfo.plist	Plist
/Library/Caches/com.fitbit.FitbitMobile/fsCachedData/	*	JSON
/Library/Preferences/	com.fitbit.FitbitMobile.plist	Plist

Runtastic

APPSTORE URL: **https://apps.apple.com/us/app/adidas-running-app-runtastic/id336599882**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Documents/raw_traces/<User_ID>/	*	CSV
/Library/Application Support/runtastic/	RTCoreDataAdditionalSessionInfo.sqlite	SQLite
/Library/Application Support/runtastic/	RTCoreDataGeoImageInfo.sqlite	SQLite
/Library/Application Support/runtastic/	RTCoreDataHeartRateInfo.sqlite	SQLite
/Library/Application Support/runtastic/	RTCoreDataLiveTrackingInfo.sqlite	SQLite
/Library/Application Support/runtastic/	RTCoreDataLocationInfo.sqlite	SQLite
/Library/Application Support/runtastic/	RTCoreDataRoute.sqlite	SQLite
/Library/Application Support/runtastic/	RTCoreDataSession.sqlite	SQLite
/Library/Application Support/runtastic/	RTCoreDataSpeedInfo.sqlite	SQLite
/Library/Application Support/runtastic/	RTCoreDataUser.sqlite	SQLite
/Library/Application Support/runtastic/	RTDatabaseEventTrace.sqlite	SQLite
/Library/Application Support/runtastic/	RTDatabaseGoalInfo.sqlite	SQLite
/Library/Application Support/runtastic/	RTDatabaseStepInfo.sqlite	SQLite
/Library/Application Support/runtastic/	RTDatabaseWorkout.sqlite	SQLite
/Library/Preferences/	at.runtastic.gpssportapp.plist	Plist

Strava

APPSTORE URL: **https://apps.apple.com/us/app/strava-run-ride-swim/id426826309**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Application Support/	Strava.sqlite	SQLite
/Library/Application Support/	Strava.sqlite.error	SQLite
/Library/Application Support/	record-release.db	SQLite
/Library/Preferences/	com.strava.stravaride.plist	Plist

REFERENCES:

https://deepsec.net/docs/Slides/2019/Still_Secure_We_Empower_What_We_Harden_Because_We_Can_Conceal_-_Yury_Chemerkin.pdf

Shopping

Amazon Shopping

APPSTORE URL: **https://apps.apple.com/us/app/amazon-shopping/id297606951**

/private/var/mobile/Containers/Data/Application/<APP_GUID>

Internal App Path	File Name	File Type
/Library/Caches/com.amazon.Amazon/	Cache.db	SQLite
/Library/Caches/com.amazon.Amazon/fsCachedData/	*	Various
/Library/Caches/WebKit/NetworkCache/Version 14/	*	Various
/Library/Preferences/	com.amazon.Amazon.plist	Plist
/Library/WebKit/WebsiteData/LocalStorage/	https_www.amazon.com_0.localstorage	SQLite

SANS DFIR @SANSForensics | dfir.to/DFIRCast | dfir.to/LinkedIn