Android 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" folder for the most commonly used third-party apps.

DFPS ANDROID-APPS-v1.1 04-21 ©2021 Mattia Epifani. All Rights Reserved. Android apps can be installed from the Google Play Store, from other App stores, and also directly on the device via the ADB or SD Card. Apps are organized based on categories (e.g., Communications, Social Networking, Business/ Productivity, and so on).

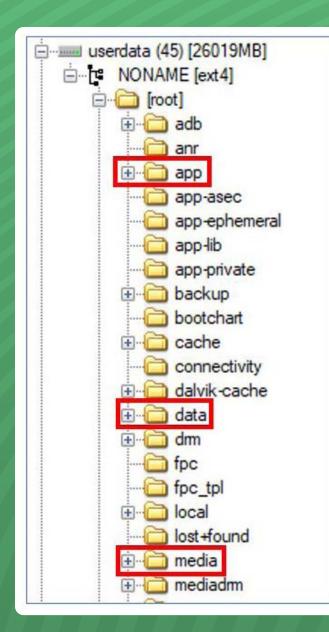
Once an app is installed on an Android device:

- App APK is stored in the USERDATA partition in a subfolder of the "/app" folder
- App Data is stored in the USERDATA partition in a subfolder of the "/data" folder (app Sandbox)

The App Data folder uses the package name (e.g., "com.whatsapp," "com.facebook.katana," "org.telegram.messenger").

The "/data/com.android.vending/database/localappstate.db" file contains information about installed packages.

Once installed, an app can request permissions to read and write data in the "/media" folder in the USERDATA partition.



Entertainment/Photo & Video



/da	ata/com.apple.android.music/	
Internal App Path	File Name	File Typ
/databases/	accounts.sqlitedb	SQLite
/databases/	bookkeeper.db	SQLite
/databases/	MediaLibrary.sglitedb	SQLite



Gallery Vault

Google

/databases/

/databases/

/.galleryvalut_DoNotDelete_<User_ID>/

/cache/image_manager_disk_cache/

https://www.mdpi.com/2079-9292/9/8/1215/pdf

/shared_prefs/

Internal App Path

/cache/<User ID>/

/cache/glide-cache/

/databases/

/databases/

/databases/

/databases/

/shared_prefs/

Internal App Pati

/.MvSecuritvData/dont_remove/ dom0o7b1i1le/dont_remove/

/files/Media/

/databases/

/shared_prefs/

/app_chrome/Default/

/app_tabs/

/shared_prefs/

https://core.ac.uk/download/pdf/214330118.pdf

	PLAY STORE URL: https://play.g	oogle.com/store/apps/details?id=com.d	elphicoder.flud
	Internal App Path	/data/com.delphicoder.flud/ File Name	File Type
	/databases/	suggestions.db	SQLite
	/databases/	torrents_db	SQLite
Flud – Torrent Downloader		m/2018/04/torrent-applications-in-andre	

PLAY STORE URL: https://plav.google.com/store/apps/details?id=com.thinkyeah.galleryvault

/data/com.thinkyeah.galleryvault/

/media/

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.google.android.apps.tachyon

/data/com.google.android.apps.tachyon/

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.google.android.apps.photos

/data/com.google.android.apps.maps/

File Name

gphotos0.db

gphotos-1.db

local_trash.db

accounts.xml

https://deagler4n6blog.blogspot.com/2021/01/dumpster-diving-in-google-photos-android-app.html

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.domobile.applock.in

/data/com.domobile.applock/

<User_ID>

File Name

domobile_elock.db

com.domobile.applock_preferences.xml XML

https://digitalforensicforest.com/2016/01/28/android-backup-file-ab-analysis

media_store_extras

TopNContactsGrpc*.dat

com.google.android.apps.tachyon_ preferences.xml

file_action_log.db

galleryvault.db



Internal App Path	File Name	File Type
/cache/image_manager_disk_cache/	*	Various
/cache/okhttpcache/	*	Various
/cache/videoplayer/	*	Various
/databases/	imgur.db	SQLite
/shared_prefs/	com.imgur.mobile_preferences.xml	XML
PLAY STORE URL: https://play.google.co	m/store/apps/details?id=com.netflix.me	diaclient

/data/com.imgur.mobile/

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.imgur.mobile



Imgur

	data/com.netflix.mediaclient/	F11 - T
Internal App Path	File Name	File Type
/databases/	OfflineDb	SQLite
/files/	offline.realm	Realm
/files/	falkor.realm	Realm
/shared prefs/	nfxpref.xml	XML

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.lenovo.anyshare.gps



SQLite

SQLite

SOLite

SQLite

File Type

ISON

Various

SQLite

SQLite

SQLite

Otilities

File Type

SQLite

SQLite

File Name	File Type
download.db	SQLite
history.db	SQLite
sharead.db	SQLite
Settings.xml	XML
/media/	
File Name	File Type
*	Various
	download.db history.db sharead.db Settings.xml /media/ File Name



Internal App Path	/data/com.spotify.music/ File Name	File Type
/files/settings/	prefs	TXT
/files/settings/Users/	*	Various
/shared_prefs/	spotify_preferences.xml	XML
/shared_prefs/	user- <user_id>.xml</user_id>	XML





PLAY STORE URL: https://play.google.com/store/apps/details?id=com.google.android.youtube		
- Ida	:a/com.google.android.youtube/	
/data/com.googte.android.youtube/		
Internal App Path	File Name	File Type
/cache/	*.cache	Various
/databases/	identity.db	SQLite

 ${\tt PLAY\ STORE\ URL: } {\bf https://play.google.com/store/apps/details?id=com.google.android.apps.}$

/data/com.google.android.apps.chromecast.app/

File Name

growthkit.db

account.notifications.db

app_preferences.xml

com.google.android.apps.chromecast. XML

com.google.android.apps.chromecast. XML

app_preferences_no_backup.xml

SOLite

Business/Productivity



Internal App Path	File Name	File Type
/databases/	<user_id>-db.db</user_id>	SQLite
/databases/	<user_id>-prefs.db</user_id>	SQLite
/databases/	db.db	SQLite
/databases/	prefs.db	SQLite
/shared_prefs/	DropboxAccountPrefs.xml	XML
/shared_prefs/	DropboxPersistentPrefs.xml	XML

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.dropbox.android

https://www.researchgate.net/publication/267027268_Acquisition_and_Analysis_of_Digital Evidence_in_Android_Smartphones $https://www.researchgate.net/publication/337419373_Digital_Forensics_Study_of_a_Cloud_transfer for the control of the contro$ Storage_Client_A_Dropbox_Artifact_Analysis

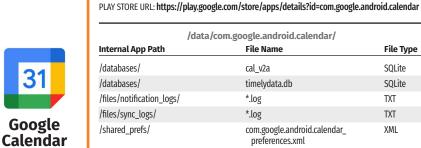
PLAY STORE URL: https://play.google.com/store/apps/details?id=com.google.android.gm

/data/com.google.android.gm/



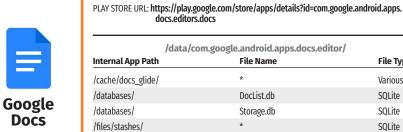
Google

Internal App Path	File Name	File T
/cache/ <user_id>/</user_id>	TopNContactsGrpc*.dat	JSON
/cache/org.chromium.android_webview/	*	Variou
/cache/	<name>.attachment</name>	Variou
/databases/	<email_address>.db</email_address>	SQLite
/databases/	bigTopDataDB <user_id></user_id>	SQLite
/databases/	EmailProvider.db	SQLite
/databases/	metadata <user_id></user_id>	SQLite
/files/downloads/	*	Variou
/shared_prefs/	Gmail.xml	XML
/shared prefs/	MailAppProvider.xml	XML



https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07s07.html





Internal App Path	/data/com.google.android.apps.docs/ File Name	File Type
PLAY STORE URL: https://	play.google.com/store/apps/details?id=com.google.an	droid.apps.docs
/silaleu_piels/	dooglebriveSitaledFleteTelletences.Allit	AML
/shared prefs/	GoogleDriveSharedPreferences.xml	XML
/files/stashes/	*	SQLite
/databases/	Storage.db	SQLite
/ualabases/	DUCLISCUD	JULILE

File Type

Various

SQLite JSON Various

SQLite

Internal App Path	File Name
/app_cello/ <user_email>/</user_email>	cello.db
/cache/ <user_id>/</user_id>	TopNContactsGrpc*.dat
/cache/docs_glide/	*
/databases/	DocList.db
/shared_prefs/	GoogleDriveSharedPreferences.xml
/shared_prefs/	webview.xml



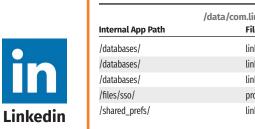
https://www.researchgate.net/publication/257687927_Digital_Forensic_Investigation_of_

PLAY STORE URL: https://play.google.cor	n/store/apps/details?id=com.google.andro	oid.keep
/data/cor	n.google.android.keep/ File Name	File Ty
/cache/image_manager_disk_cache/	*	Variou
/databases/	keep.db	SQLite
Inhamad musfal		VAAL

Cloud_Storage_Services

com.google.android.keep_preferences.xml XML /shared_prefs/ https://link.springer.com/article/10.1007/s11042-016-3718-2 https://www.oreillv.com/libra 071a51a4-563f-4232-b5df-8

	PLAY STORE URL: https://	play.google.com/store/apps/details?id=com.micro	soft.skyd
	Internal App Path	/data/com.microsoft.skydrive/ File Name	F
	/databases/	metadata	S
Microsoft	/databases/	AriaStorage.db	S
OneDrive	/files/aria/	*	V



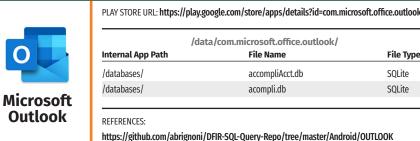
Internal App Path	/data/com.linkedin.android/ File Name	File Type
/databases/	linkedin_messenger.db	SQLite
/databases/	linkedin.db	SQLite
/databases/	linkedin_search.db	SQLite
/files/sso/	profile_pic.png	PNG
/shared_prefs/	linkedInPrefsName.xml	XML

File Type

File Type

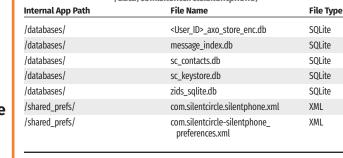
SQLite

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.linkedin.android

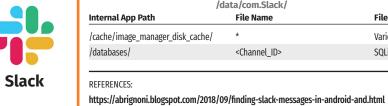


/data/com.pinterest/			
Internal App Path	File Name	File Type	
/databases/	<user_id>-AttachmentMetadata Database.db</user_id>	SQLite	
/databases/	<user_id>-ContactsDatabase.db</user_id>	SQLite	
/databases/	<user_id>-MessagesDatabase.db</user_id>	SQLite	
/databases/	<user_id>-NotificationsDatabase.db</user_id>	SQLite	
/databases/	<pre><user_id>-PendingActionsDatabase.db</user_id></pre>	SQLite	
/datahases/	clicar ID>-UnroadCountercDatabace dh	COLita	





Internal App Path	/data/com.Slack/ File Name
PLAY STORE URL: https://pla	y.google.com/store/apps/details?id=com.Sla
https://eprint.iacr.org/2016/	703.pdf



REFERENCES:

ogle.com/store/apps/details?id=com	.wire
/data/com.wire/ File Name	File Type
<user_id></user_id>	SQLite
	/data/com.wire/ File Name

https://github.com/abrignoni/DFIR-SQL-Query-Repo/tree/master/Android/SLACK

	Internal App Path	File Name	File Type
	/databases/	<user_id></user_id>	SQLite
n ı	/files/assets/	*	JPG
W)	/shared_prefs/	com.wire.preferences.xml	XML
Wire	REFERENCES: https://wire-docs.wire.com/do	wnload/Wire+Security+Whitepaper.pdf	

https://www.x41-dsec.de/reports/X41-Kudelski-Wire-Security-Review-Android.pdf https://repository.canterbury.ac.uk/download/cca0400883a9c164da4db892fd2442a51cd 5f5b87c73116de6fbab8e7d3291d8/1542565/IARIA-journal-ephemeral-Camera-ReadyV4.pdf https://blog.oxygen-forensic.com/wire-app-extraction/
PLAY STORE URL: https://play.google.com/store/apps/details?id=us.zoom.videomeetings
the transfer of the

/data/us.zoom.videomeetings/			
Internal App Path	File Name	File Type	
/data/ <user_id>@xmpp.zoom.us/</user_id>	<pre><user_id>@xmpp.zoom.us.asyn.db</user_id></pre>	SQLite	
/data/ <user_id>@xmpp.zoom.us/</user_id>	<pre><user_id>@xmpp.zoom.us.db</user_id></pre>	SQLite	
/data/ <user_id>@xmpp.zoom.us/</user_id>	<pre><user_id>@xmpp.zoom.us.idx.db</user_id></pre>	SQLite	
/data/ <user_id>@xmpp.zoom.us/</user_id>	<pre><user_id>@xmpp.zoom.us.sync.db</user_id></pre>	SQLite	
/data/	zoommeeting.db	SQLite	
/data/	zoomus.db	SQLite	
• "	cience/article/pii/S2666281721000019		
forensic analysis of the Zoom	ıblication/348715321_Zooming_into_the_pande	emic_A_	

brary/view/learning-android-forensics/97817891310 -8b981a57c4df.xhtml	17/	Zoom	data/	zoomus.db	SQLite
ay.google.com/store/apps/details?id=com.microsoft.skydrive		h	•	m/science/article/pii/S2666281721000019	
/data/com.microsoft.skydrive/ File Name	File Type		ttps://www.researchgate.net forensic_analysis_of_the_Zo	t/publication/348715321_Zooming_into_th om_Application	ıe_pandemic_A_
metadata	SQLite				
AriaStorage.db	SQLite				
*	Various				

File Type



burners.db

PLAY STORE URL: https://play.google.com/store/apps/details?id=org.mozilla.firefox

GeneralPreferences.xml



Google

/databases

/databases/

/shared prefs/

/shared_prefs/

/cache/Cache/

I	data/com.isharing.isharing/	
Internal App Path	File Name	File Type
/databases/	com.hypertrack.common.device logs.db	SQLite
/databases/	Isharing_talk	SQLite
/shared_prefs/	ISHARING PREFS.xml	XML

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.microsoft.emmx

https://openrepository.aut.ac.nz/bitstream/handle/10292/13208/VargasS.pdf

Google Keep

Drive

/6	data/com.microsoft.skydrive/	
Internal App Path	File Name	File Typ
/databases/	metadata	SQLite
/databases/	AriaStorage.db	SQLite
/files/aria/	*	Various

Firefox

Internal App Path	File Name	File Type
/cache/ <id>.default/cache2/entries/</id>	*	Various
/cache/mozac_browser_icons/icons/	*	JPG
/cache/mozac_browser_thumbnails/ thumbnails/	*	JPG
/databases/	logins.sqlite	SQLite
/databases/	top_sites	SQLite
/files/mozilla/ <id>.default/</id>	*	Various
/files/	places.sqlite	SQLite

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.android.chrome

https://www.sciencedirect.com/science/article/abs/pii/S0167739X18308070

/data/com.android.chrome/

File Name

https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07s08.html

com.android.chrome_preferences.xml XML



Various

Various

ı	/databases/	BingSearchHistory.db	SQLite
	/shared_prefs/	com.microsoft.emmx_preferences.xml	XML
	PLAY STORE URL: https://play.g	oogle.com/store/apps/details?id=com.opera.brows	er
ı		/data/com.opera.browser/	
ı		/ data/comoperationoci/	
	Internal App Path	File Name	File Type
	Internal App Path /app_opera/		File Type Various
	l —	File Name	



Microsoft

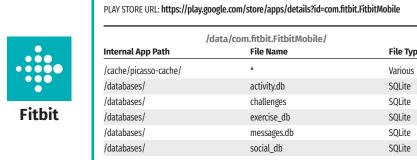
Edge

	File Name	Internal App Path
Vari	*	/app_opera/
Vari	*	/cache/cache/
XML	recent_searches.xml	/shared_prefs/
	recent_searches.xml	/shared_prefs/
-		REFERENCES:



AY STORE URL: https://play.google.com/	store/apps/details?id=org.torpro	ject.torbrowser
	prproject.torbrowser/	
ternal App Path	File Name	File Type
pp_torservice/.tor/	state	TXT
les/mozilla/ <id>.default/</id>	browser.db	SQLite
	/media/	
ternal App Path	File Name	File Type
ndroid/data/org.torproject.torbrowser/	*	Various

Health & Fitness



	PLAY STORE URL: https://play.go	ogle.com/store/apps/details?id=com.m	yfitnesspal.andro
*	/dat	ta/com.myfitnesspal.android/ File Name	File
	/databases/	myfitnesspal.db	SQLi
	/cache/picasso-cache/	*	Vario
FitnessPal			
	RFFFRFNCFS.		

https://core.ac.uk/download/pdf/301365837.pdf

NRC	
Nike Run Club	

	/data/com.nike.plusgps/	
Internal App Path	File Name	File Type
/databases/	com.nike.activitystore.database	SQLite

	om.fitnesskeeper.runkeeper.pro/	
Internal App Path	File Name	File Type
/databases/	RunKeeper.sqlite	SQLite
/databases/	PC.db	SQLite
/databases/	PC_PILL.db	SQLite
/cache/picasso-cache/	*	Various

/dat	a/com.myfitnesspal.android/	
nternal App Path	File Name	File Type
databases/	myfitnesspal.db	SQLite
cache/picasso-cache/	*	Various

Social Networking

Snapchat

/data/com/internal App Path	n.facebook.katana/ File Name	File Typ
/app_compactdisk/	*	Various
/app_light_prefs/	logged_in_ <user_id></user_id>	JSON
/cache/compactdisk/	*	Various
/cache/org.chromium.android_webview/	*	Various
/databases/	admined_pages_db	SQLite
/databases/	bookmarks_db2	SQLite
/databases/	contacts_db2	SQLite
/databases/	data_usage_db	SQLite
/databases/	events.db	SQLite
/databases/	fb.db	SQLite
/databases/	local_media_db	SQLite
/databases/	nearbytiles_db	SQLite
/databases/	newsfeed.db	SQLite
/databases/	omnistore_ <user_id>_v01.db</user_id>	SQLite
/databases/	prefs_db	SQLite
/databases/	search_bootstrap_db	SQLite
/databases/	threads_db2	SQLite
/databases/	time_in_app_ <user_id>.db</user_id>	SQLite
/databases/	uploadmanager.db	SQLite
/files/ExoPlayerCacheDir/	*	Various
/shared_prefs/	com.facebook.orca_preferences.xml	XML

Facebook

Internal App Path File Name File Type /DCIM/Facebook/ Various https://onlinelibrary.wiley.com/doi/abs/10.1111/1556-4029.13267

http://cheeky4n6monkey.blogspot.com/2014/01/facebook-facebook-messenger-android-app.html http://freeandroidforensics.blogspot.com/2015/02/facebook-for-android-artifacts.html https://www.academia.edu/10726810/Social_Media_Forensics_on_Mobile_Devices https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07s13.html https://www.tandfonline.com/doi/full/10.1080/00450618.2015.1066854

	PLAY STORE URL: https://play.google.co	m/store/apps/details?id=com.h	erzick.houseparty
	/data/co Internal App Path	m.herzick.houseparty/ File Name	File Type
	/cache/image_manager_disk_cache/	*	Various
	/databases/	instabug.db	SQLite
	/files/	default.realm	Realm
	/shared_prefs/	instabug.xml	XML
Houseparty	REFERENCES: https://www.researchgate.net/publicat AMONG TEENS - ARE FORENSIC TOO		GING_MOBILE_APPS_

/data/data/dinternal App Path	com.instagram.android/ File Name	File Type
/cache/	ManifestFeed- <user_id>.json</user_id>	JSON
/cache/	tmp_photo_*.jpg	JPG
/cache/images/	*	JPG
/cache/original_images/	*	Various
/databases/	contacts_db2	SQLite
/databases/	direct.db	SQLite
/databases/	fileregistry.db	SQLite
/databases/	time_in_app_ <user_id>.db</user_id>	SQLite
/databases/	transactions.db	SQLite
/files/music/	*	Various
/files/pending_media_images/	*	Various
/files/rendered_videos/	*	Various
/shared_prefs/	<user_id>.xml</user_id>	XML
/shared_prefs/	<pre><user_id>_USER_PREFERENCES.xml</user_id></pre>	XML
/shared_prefs/	User_ID>_usersBootstrapService.xml	XML
/shared_prefs/	com.instagram.android_preferences.xml	XML
Internal App Path	/media/ File Name	File Type
/Movies/Instagram/	*	Various

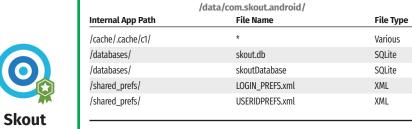
https://iopscience.iop.org/article/10.1088/1757-899X/1007/1/012116/pdf https://www.techscience.com/csse/v37n2/41447/pdf https://www.researchgate.net/publication/347441116_Investigation_on_Instagram_ Android-based_using_Digital_Forensics_Research_Workshop_Framework
PLAY STORE URL: https://play.google.com/store/apps/details?id=com.mewe
ldata Isom movo l

/Pictures/Instagram/

REFERENCES:

	PLAY STORE URL: https://play.google.cor	n/store/apps/details?id=com.mewe	
MeWe	/d Internal App Path	ata/com.mewe/ File Name	File Type
	/cache/image_manager_disk_cache/	*	Various
MeWe	/databases/	app_database	SQLite
	/shared_prefs/	SGSession.xml	XML
	PLAY STORE URL: https://play.google.cor	n/store/apps/details?id=com.pinterest	

Internal App Path	/data/com.pinterest/ File Name	File Type
/cache/picasso-cache/	*	Various
/cache/video/	*	Various
/databases/	pinterest-db <number></number>	SQLite
/shared_prefs/	pinterest.invite_preferences_manager.xml	XML
/shared_prefs/	pinterest.xml	XML



	/databases/	skoutDatabase	SQLite
	/shared_prefs/	LOGIN_PREFS.xml	XML
X	/shared_prefs/	USERIDPREFS.xml	XML
ıt	REFERENCES:	om/doi/abs/10.1111/1556-4029.13267	
	1	ot.com/2020/05/app-skout-on-android.html	ļ
	https://media.kasperskycon	tenthub.com/wp-content/uploads/sites/58/	2017/10/2118094

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.skout.android

/data/com.snapchat.android/			
Internal App Path	File Name	File Type	
/databases/	arroyo.db	SQLite	
/databases/	gallery_database.db	SQLite	
/databases/	journal.db	SQLite	
/databases/	main.db	SQLite	
/databases/	memories.db	SQLite	
/databases/	tcspahn.db	SQLite	
/files/file_manager/	*	Various	
/shared_prefs/	com.snapchat.android_preferences.xml	XML	
/shared_prefs/	user_session_shared_pref.xml	XML	
	/media/		
Internal App Path	File Name	File Type	

REFERENCES:
https://onlinelibrary.wiley.com/doi/abs/10.1111/1556-4029.13267
https://www.sciencedirect.com/science/article/pii/S1877050917311006/pdf
https://thebinaryhick.blog/2019/06/01/two-snaps-and-a-twist-an-in-depth-and-updated- look-at-snapchat-on-android
https://www.researchgate.net/publication/317549540_Snapchat_Analysis_to_Discover_Digital_ Forensic_Artifacts_on_Android_Smartphone

https://courses.csail.mit.edu/6.857/2016/files/11.pdf https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07s16.html
PLAY STORE URL: https://play.google.com/store/apps/details?id=com.zhiliaoapp.musically
/data/com zhiliaoann musically/

/data/	com.zhiliaoapp.musically/	
Internal App Path	File Name	File Type
/databases/	<user_id>_im.db</user_id>	SQLite
/databases/	aweme.db	SQLite
/databases/	downloader.db	SQLite
/databases/	db_im_xx	SQLite
/databases/	TIKTOK.db	SQLite
/databases/	video.db	SQLite
/files/	*	Various
/shared_prefs/	aweme_user.xml	XML
	/media/	
Internal App Path	File Name	File Typ
/Android/data/com.zhiliaoapp. musically/cache/	*	Various
/Android/data/com.zhiliaoapp.	*	Various

REFERENCES:
https://abrignoni.blogspot.com/2018/11/finding-tiktok-messages-in-android.html
https://github.com/abrignoni/DFIR-SQL-Query-Repo/tree/master/Android/TIKTOK
https://www.researchgate.net/publication/343856173_Post-mortem_digital_forensic_artifacts_ of_TikTok_Android_App

Internal App Path	/data/com.tinder/ File Name	File Type
/cache/picasso-cache/	*	Various
/databases/	tinder.db	SQLite
/shared prefs/	SP.xml	XML

	/data/sh.whisper/	
Internal App Path	File Name	File Typ
/databases/	c.db	SQLite
/databases/	w.db	SQLite
/shared prefs/	sh.whisper preferences.xml	XML

https://www.nw3c.org/docs/research/whisper-application.pdf

Navigation & Travel

/data/com.go Internal App Path	ogle.android.apps.maps/ File Name	File Ty
/app_tts-cache/	*	Various
/cache/image_manager_disk_cache/	*	Various
/databases/	gmm_myplaces.db	SQLite
/databases/	gmm_storage.db	SQLite
/databases/	gmm_sync.db	SQLite
/shared_prefs/	settings_preference.xml	XML

PLAY STORE URL: https://play.goo	gle.com/store/apps/details?id=com.ub	ercab
Internal App Path	data/com.ubercab/ File Name	File
/files/base-key-value-store/	realtime-demo_KEY_CITY	JSON
/files/base-key-value-store/	realtime-demo_KEY_RIDER	JSON

	News
PLAY STORE URL:	nttps://play.google.com/store/apps/details?id=com.reddit.frontpage

/data/com.reddit.frontpage/				
Internal App Path	File Name	File Type		
/cache/image_manager_disk_cache/	*	Various		
/databases/	AndroidVideoCache.db	SQLite		
/databases/	reddit_db_ <user_id></user_id>	SQLite		
/databases/	wallet.db	SQLite		
/shared_prefs/	com.reddit.storage.account.xml	XML		
/shared_prefs/	com.reddit.user_settings.xml	XML		
	/media/			
Internal App Path	File Name	File Type		
/Pictures/Reddit/	*	Various		

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.twitter.android

Reddit

/data/d	com.twitter.android/	
Internal App Path	File Name	File Type
/databases/	<user_id>.db</user_id>	SQLite
/databases/	<user_id>-dm.db</user_id>	SQLite
/databases/	<user_id>-drafts.db</user_id>	SQLite
/databases/	<user_id>-NN.db</user_id>	SQLite
/databases/	<user_id>-scribe.db</user_id>	SQLite
/databases/	global.db	SQLite
/shared_prefs/	com.twitter.android_preferences.xml	XML
/shared_prefs/	PostActivity.xml	XML
/shared_prefs/	TimelineActivity.xml	XML
	/media/	
Internal App Path	File Name	File Type
/Android/data/com.twitter.android/cache/	*	Various
/Pictures/Twitter/	*	Various

	/shared_prefs/	TimelineActivity.xml	X
ter	Internal App Path	/media/ File Name	F
	/Android/data/com.twitter.android/ cache/	*	V
	/Pictures/Twitter/	*	V
	REFERENCES:		
	https://onlinelibrary.wiley.com/doi/a	abs/10.1111/1556-4029.13267	
	https://www.tandfonline.com/doi/fu	ll/10.1080/00450618.2015.1066854	
	http://cs.lewisu.edu/mathcs/msispro	ojects/papers/kevinswartz.pdf	

SANS DFIR OPERATING SYSTEM & DEVICE IN-DEPTH

@sansforensics

sansforensics

dfir.to/MAIL-LIST

FOR308: Digital Forensics Essentials FOR498: Battlefield Forensics & Data Acquisition | GBFA

FOR500: Windows Forensics | 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

FOR509: Enterprise Cloud Forensics & Incident Response

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

and Incident Handling | всин

unications

Telegram

	PLAY STORE URL: https://play.google.co	om/store/apps/details?id=com.discord	
	/d Internal App Path	ata/com.discord/ File Name	File Type
		*	
	/cache/app_images_cache_small/		Various
	/shared_prefs/	com.discord_preferences.xml	XML
	/shared_prefs/	prefsSessionDurable.xml	XML
		/media/	
الم	Internal App Path	File Name	File Type
rd	/Pictures/Discord/	* 07/discord-app-forensic-artifacts-in.htr	Various
rd	/Pictures/Discord/ REFERENCES: https://abrignoni.blogspot.com/2017/uhttps://www.nw3c.org/docs/research/	* 07/discord-app-forensic-artifacts-in.htr	Various nl
d	/Pictures/Discord/ REFERENCES: https://abrignoni.blogspot.com/2017/uhttps://www.nw3c.org/docs/research/	* 07/discord-app-forensic-artifacts-in.htr /discord.pdf	Various nl
d	/Pictures/Discord/ REFERENCES: https://abrignoni.blogspot.com/2017/uhttps://www.nw3c.org/docs/research/	* 07/discord-app-forensic-artifacts-in.htr /discord.pdf om/store/apps/details?id=com.radicala	Various nl
rd	/Pictures/Discord/ REFERENCES: https://abrignoni.blogspot.com/2017/uhttps://www.nw3c.org/docs/research/	* 07/discord-app-forensic-artifacts-in.htr discord.pdf om/store/apps/details?id=com.radicala n.radicalapps.cyberdust/	Various nl pps.cyberdust
d	/Pictures/Discord/ REFERENCES: https://abrignoni.blogspot.com/2017/chttps://www.nw3c.org/docs/research/ PLAY STORE URL: https://play.google.co//data/cor/Internal App Path	* D7/discord-app-forensic-artifacts-in.htr discord.pdf pm/store/apps/details?id=com.radicala n.radicalapps.cyberdust/ File Name	Various nl pps.cyberdust File Type
	/Pictures/Discord/ REFERENCES: https://abrignoni.blogspot.com/2017/thttps://www.nw3c.org/docs/research/ PLAY STORE URL: https://play.google.co//data/cor/ Internal App Path /cache/image_manager_disk_cache/	* 27/discord-app-forensic-artifacts-in.htr /discord.pdf 20m/store/apps/details?id=com.radicala 20m.radicalapps.cyberdust/ 20m/store/apps/details?id=com.radicala	Various nl pps.cyberdust File Type Various
d	/Pictures/Discord/ REFERENCES: https://abrignoni.blogspot.com/2017/https://www.nw3c.org/docs/research/ PLAY STORE URL: https://play.google.co //data/cor/ Internal App Path /cache/image_manager_disk_cache/ //databases/	* 27/discord-app-forensic-artifacts-in.htr /discord.pdf 20m/store/apps/details?id=com.radicala n.radicalapps.cyberdust/ File Name * room-db	Various nl pps.cyberdust File Type Various SQLite

e Name ged_in_ <user_id> L_logs_db ntacts_db2 nnistore_<user_id>_v01.db</user_id></user_id>	JSON Various Various Various SQLite SQLite
l_logs_db ntacts_db2 nnistore_ <user_id>_v01.db</user_id>	Various Various Various SQLite SQLite SQLite
ntacts_db2 nnistore_ <user_id>_v01.db</user_id>	Various SQLite SQLite SQLite
ntacts_db2 nnistore_ <user_id>_v01.db</user_id>	SQLite SQLite SQLite
ntacts_db2 nnistore_ <user_id>_v01.db</user_id>	SQLite SQLite
nnistore_ <user_id>_v01.db</user_id>	SQLite
efs_db	
	SQLite
reads_db2	SQLite
an_db_ <user_id></user_id>	SQLite
	JPG
	Various
m.facebook.orca_preferences.xml	XML
	an_db_ <user_id> m.facebook.orca_preferences.xml</user_id>

internal App Path	File Name	File Type
/Pictures/Messenger/	*	Various
REFERENCES:		
http://cheeky4n6monkey.blogsp	ot.com/2014/01/facebook-facebook-n	nessenger-android-app.html
http://freeandroidforensics.blo	gspot.com/2015/02/facebook-for-an	droid-artifacts.html
https://www.academia.edu/107	26810/Social_Media_Forensics_on_I	Mobile_Devices
https://www.tandfonline.com/o Code=tajf20	loi/abs/10.1080/00450618.2015.1066	854?src=recsys&journal
http://ijns.jalaxy.com.tw/conte	nts/ijns-v22-n5/ijns-2020-v22-n5-p82	28-837.pdf

https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07s14.html

PLAY STORE URL: https://play.go	oogle.com/store/apps/details?id=com.	google.android.talk
/d Internal App Path	lata/com.google.android.talk/ File Name	File Type
/databases/	Babel <n>.db</n>	SQLite
/shared_prefs/	accounts.xml	XML

Facebook

Messenger

Google

Hangouts	https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07 https://onlinelibrary.wiley.com/doi/10.1111/1556-4029.13164						
	PLAY STORE URL: https://play.go	oogle.com/store/apps/details?id=com.i	mo.android.imous				
	/c Internal App Path	/data/com.imo.android.imous/ Internal App Path File Name File					
	/databases/	accountdb.db	SQLite				
	/databases/	imofriends.db	SQLite				
	/files/	*	ISON				

Internal App Path	File Name	File Type
/databases/	accountdb.db	SQLite
/databases/	imofriends.db	SQLite
/files/	*	JSON
/shared_prefs/	com.imo.android.imous_preferences.xml	XML
	/media/	
	File Name	File Type
Internal App Path	rite name	· ite iyp

http://prr.hec.gov.pk/jspui/bitstream/123456789/13429/1/Muhammad%20Asad%20Khan%20

Sudozai%20electrical%20engg%202019%20NUST%20isb%20prr.pdf

https://onlinelibrary.wiley.com/doi/10.1111/1556-4029.13164

	PLAY STORE URL: https://play.go	oogle.com/store/apps/details?id=kik.android		
	/data/kik.android/ Internal App Path File Name File			
	/databases/	<pre><user_id>.contactProfileEntries.db</user_id></pre>	SQLite	
	/databases/	<user_id>.KikDatabase.db</user_id>	SQLite	
	/databases/	<user_id>.userRosterEntries.db</user_id>	SQLite	
(•	/shared_prefs/	<user_id>.KikPreferences.xml</user_id>	XML	
		/media/		
	Internal App Path	File Name	File Type	
	/Kik/	*	Various	
nger	PETERFACE			

https://ieeexplore.ieee.org/abstract/document/9079092 https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07s20.html https://onlinelibrary.wiley.com/doi/10.1111/1556-4029.13164
PLAY STORE URL: https://play.google.com/store/apps/details?id=jp.naver.line.android

https://www.researchgate.net/publication/321268908_Forensic_Analysis_of_Kik_Messenger_

	File Name	File Type
Internal App Path /databases/	call history	SOLite
	= /	
/databases/	naver_line	SQLite
/databases/	read_notification	SQLite
/databases/	search.sqlite	SQLite
Internal App Path	/media/ File Name	File Type
/Pictures/LINE/	*	Various

https://ojs.unud.ac.id/index.php/JLK/article/download/53164/33065/ https://onlinelibrary.wiley.com/doi/10.1111/1556-4029.13164

Internal App Path	a/org.thoughtcrime.securesms/ File Name	File Type
/cache/log/	*	TXT
/databases/	signal.db	SQLite
/files/avatars/	*	JPG
/shared_prefs/	org.thoughtcrime.securesms_ preferences.xml	XML
/shared_prefs/	SecureSMS-Preferences.xml	XML
	/media/	
Internal App Path	File Name	File Type
/Signal/	*	Various

http://www.ijits-bg.com/contents/IJITS-No4-2019/2019-N4-06.pdf

Internal App Path	m.paypal.android.p2pmobile/	
пестистрртист	File Name	File Type
/cache/picasso-cache/	*	Various
/shared_prefs/	com.paypal.android.p2pmobile.xml	XML
REFERENCES:		
https://www.diva-portal.org/sm	ash/get/diva2:812012/FULLTEXT01.pdf	
DI WOTODE VIDI III III II	4 1 1 1 1 1 2 2 2 1	
PLAY STORE URL: https://play.goo	gle.com/store/apps/details?id=com.venmo	

 		/data/com.ubercab/	
	Internal App Path	File Name	File Type
	/cache/picasso-cache/	*	Various
	/databases/	mparticle.db	SQLite
	/databases/	venmo.sqlite	SQLite
o l	/shared_prefs/	Venmo.xml	XML

/data/	/com.skype.raider/	
Internal App Path	File Name	File Type
/databases/	s4l-live: <user_id>.db</user_id>	SQLite
/files/live#3 <user_id>/</user_id>	eascache.db	SQLite
/files/live#3 <user_id>/</user_id>	main.db	SQLite
/files/live#3 <user_id>/</user_id>	qik_main.db	SQLite
/files/live#3 <user_id>/media_messaging</user_id>	<i>[</i> *	Various
	/media/	
Internal App Path	/media/ File Name	File Type
Internal App Path /Pictures/Skype/		File Type Various
	File Name	

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.skype.raider

https://onlinelibrary.wiley.com/doi/10.1111/1556-4029.13164 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.6279&rep=rep1&type=pdf https://bebinary4n6.blogspot.com/2020/01/skype-on-android-images-in-web-cache.html https://www.researchgate.net/publication/311299201_Forensics_Acquisition_and_Analysis_of_ instant_messaging_and_VoIP_applications https://www.researchgate.net/publication/258244243_Skype_Forensics_in_Android_Devices https://www.researchgate.net/publication/328568587_Forensics_Analysis_of_Skype_Viber_

and_WhatsApp_Messenger_on_Android_Platform https://www.oreilly.com/library/view/learning-android-forensics/9781789131017/b4ed4526-33cd-4316-bd83-4d68bb0a5627.xhtml PLAY STORE URL: https://play.google.com/store/apps/details?id=org.telegram.messenger

/data/	org.telegram.messenger/	
Internal App Path	File Name	File Type
/cache/	*	Various
/files/	cache4.db	SQLite
/shared_prefs/	userconfig.xml	XML
	/media/	
Internal App Path /Android/data/org.telegram.	/media/ File Name *	File Type Various
/Android/data/org.telegram. messenger/cache/	File Name *	Various
/Android/data/org.telegram.	File Name	

https://www.sciencedirect.com/science/article/abs/pii/S1742287617301767 https://blog.digital-forensics.it/2020/04/teleparser.html https://dflab.blogspot.com/2019/01/cache4db-file-of-telegram-for-and roid.htmlhttps://codeby.net/resources/digital-forensic-analysis-of-telegram-messenger-on-android-devices.809/download https://onlinelibrary.wiley.com/doi/10.1111/1556-4029.13164

PLAY STORE URL: https://play.g	oogle.com/store/apps/details?id=com.pinge	r.textfree
Internal App Path	/data/com.pinger.textfree/ File Name	File Type
/databases/	tfa	SQLite
/files/logs/	*	Various
/shared_prefs/	com.pinger.textfree.application.x	ml XML

TextFree	/files/logs/ /shared_prefs/ REFERENCES: https://forensicstats.org/wp-content/up	* com.pinger.textfree.application.xml ploads/2018/06/conference-paper.pdf	Various XML
	PLAY STORE URL: https://play.google.com /data/com.e	/store/apps/details?id=com.enflick.andr	oid.TextNow

Internal App Path	File Name	File Ty
/cache/org.chromium.android_webview/	*	Variou
/databases/	leanplum.db	SQLite
/databases/	textnow_data.db	SQLite
/shared prefs/	com.enflick.android.TextNow_	XML
· · · · · · · - · · · · · · · · · · · ·	preferences.xml	
-	preferences.xml /media/ File Name	File Tv
Internal App Path /Android/data/com.enflick.android. TextNow/cache/	/media/	File Ty Variou

		,	
TextNow	Internal App Path	File Name	File Type
	/Android/data/com.enflick.android. TextNow/cache/	*	Various
	/TextNow/	*	Various
	REFERENCES: https://books.google.it/books?id=bE8	BADQAAQBAJ&pg=PA259	
	PLAY STORE URL: https://play.google.co	om/store/apps/details?id=com.viber.voip	
	/da Internal App Path	ata/com.viber.voip/ File Name	File Type
	/databases/	viber_data	SQLite
	/databases/	viber_messages	SQLite

/ualabases/	viner_inessages	SQLILE
/databases/	viber_prefs	SQLite
/shared_prefs/	com.viber.voip.ViberPrefs.xml	XML
	/media/	
Internal App Path	File Name	File Typ
/Android/data/com.viber.voip/cache/	*	Various
	*	Various
/Pictures/Viber/	"	various

/Viber/	*	Various
REFERENCES:		
https://onlinelibrary.w	iley.com/doi/10.1111/1556-4029.13164	
https://arxiv.org/ftp/a	rxiv/papers/1304/1304.4915.pdf	
	gate.net/publication/283666189_Implement sApp_and_Viber_Android_Applications	tation_of_Forensic_Analysis_
http://sdiwc.net/digita	al-library/forensics-analysis-of-skype-viber	-and-whatsapp-messenger-

http://sdiwc.net/digital-library/forensics-analysis-of-skype-viber-and-whatsapp-messeng on-android-platform.html
https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07s17.h https://blog.oxygen-forensic.com/viber-messenger-forensics/
PLAY STORE URL: https://play.google.com/store/apps/details?id=com.tencent.mm

		/data/com.tencent.mm/	
	Internal App Path	File Name	File Type
	/MicroMsg/ <user_id>/</user_id>	EnMicroMsg.db	SQLite
	/MicroMsg/ <user_id>/</user_id>	SnsMicroMsg.db	SQLite
		/media/	
	Internal App Path	File Name	File Type
	/Tencent/MicroMsg/	*	Various
WeChat			

REFERENCES:
https://www.sciencedirect.com/science/article/abs/pii/S1742287616301220
https://www.oreilly.com/library/view/learning-android-forensics/9781782174578/ch07s21.html
https://www.oreilly.com/library/view/learning-android-forensics/9781789131017/08a8bbfd- 988a-455c-aa09-87832ac8c1b0.xhtml
https://www.forensicfocus.com/articles/decrypt-wechat-enmicromsgdb-database/
https://www.ictsecuritymagazine.com/articoli/wechat-forensics-parte-ii/

PLAY STORE URL: https://play.google.com/store/apps/details?id=com.whatsapp

		/data/com.whatsapp/	
Internal A	pp Path	File Name	File Type
/databases	1	axolotol.db	SQLite
/databases	1	chatsettings.db	SQLite
/databases	1	location.db	SQLite
/databases	1	media.db	SQLite
/databases	1	msgstore.db	SQLite
/databases	1	wa.db	SQLite
/files/Avata	ars/	*	Various
/files/Logs	1	*	TXT
/shared_pr	efs/	com.whatsapp_preferences.xml	XML
/shared_pr	efs/	RegisterPhone.xml	XML
		/media/	
Internal A	pp Path	File Name	File Type
/WhatsApp	/Backups/	*	SQLite
/WhatsApp	/Databases/	*	SQLite

/databases/	wa.db	SQLite
/files/Avatars/	*	Various
/files/Logs/	*	TXT
/shared_prefs/	com.whatsapp_preferences.xml	XML
/shared_prefs/	RegisterPhone.xml	XML
·	/media/	
Internal App Path	/media/ File Name	File Type
		File Type
Internal App Path /WhatsApp/Backups/ /WhatsApp/Databases/	File Name	

REFERENCES:
https://www.sciencedirect.com/science/article/abs/pii/S1742287614000437
https://onlinelibrary.wiley.com/doi/10.1111/1556-4029.13164
https://www.researchgate.net/publication/328568587_Forensics_Analysis_of_Skype_Viber_ and_WhatsApp_Messenger_on_Android_Platform
https://www.oreilly.com/library/view/learning-android-forensics/9781789131017/b4a45cd1- 8ce8-4dfc-9587-be46ecf45ad1.xhtml

https://www.group-ib.com/blog/whatsapp_forensic_artifacts
https://www.ictsecuritymagazine.com/articoli/whatsapp-forensics/
https://sudonull.com/post/30099-WhatsApp-in-the-palm-of-your-hand-where-and-how-can you-detect-forensic-artifacts-Group-IB-Blog
hater the control of

https://www.ukessays.com/essays/security/forensic-analysis-of-whatsapp-on-android.php
https://sudonull.com/post/30099-WhatsApp-in-the-palm-of-your-hand-where-and-how-can- you-detect-forensic-artifacts-Group-IB-Blog
nttps://www.ictsecuritymagazine.com/articoli/wnatsapp-forensics/

https://www.ukessays.com/essays/security/forensic-analysis-of-whatsapp-on-android.php
PLAY STORE URL: https://play.google.com/store/apps/details?id=com.mywickr.wickr2
/data/com.mywickr.wickr2/

A A
Wickr
VVICKI

/data/com.mywickr.wickr2/		
Internal App Path	File Name	File Type
/cache/dec/	*	Various
/databases/	wickr_db	SQLite
REFERENCES:		
https://www.researchgate.net/	nublication/308996221 Forensic An	alusis of the Recovery of

REFERENCES:
https://www.researchgate.net/publication/308996221_Forensic_Analysis_of_the_Recovery_of_ Wickr's_Ephemeral_Data_on_Android_Platforms
https://thebinaryhick.blog/2019/08/23/wickr-alright-well-call-it-a-draw/
https://repository.canterbury.ac.uk/download/3e59ded778529baaf67e0be4d5c9b31b7fca48bb1 4ef965948fa5cc6d578c3c6/685125/15054.pdf
https://blog.oxygen-forensic.com/wickr-some-forensics-up/



FOR578: Cyber Threat Intelligence | GCTI