a	INF	ORN	/ATI	ON
•	1141	OIV!		VIV

Raw Logs

DATABASE

	Search:	
CLASS	♦ METHOD	A

CLASS	METHOD
android.database.sqlite.SQLiteDatabase	getPath
	Arguments: []
	Result: /data/user/0/com.google.android.apps.maps /databases /portable_geller_nyankosensei452@gmail.com.db
	Return Value: /data/user /0/com.google.android.apps.maps/databases /portable_geller_nyankosensei452@gmail.com.db
	Called From: android.database.sqlite.SQLiteCursor.fillWindow(SQ LiteCursor.java:147)

CLASS	METHOD
android.database.sqlite.SQLiteDatabase	getPath
	Arguments: []
	Result: /data/user/0/com.google.android.apps.maps /databases /portable_geller_nyankosensei452@gmail.com.db
	Return Value: /data/user /0/com.google.android.apps.maps/databases /portable_geller_nyankosensei452@gmail.com.db
	Called From: android.database.sqlite.SQLiteCursor.fillWindow(SQ LiteCursor.java:147)

METHOD

getPath

Arguments: []

/databases

Called From:

LiteCursor.java:147)

Return Value: /data/user

Result: /data/user/0/com.google.android.apps.maps

/portable_geller_nyankosensei452@gmail.com.db

and roid. database. sqlite. SQLite Cursor. fill Window (SQ

/0/com.google.android.apps.maps/databases /portable_geller_nyankosensei452@gmail.com.db

CLASS

and roid. database. sqlite. SQLite Database

CLASS METHOD

android.database.sqlite.SQLiteDatabase

rawQueryWithFactory

Arguments: [None, 'SELECT geller_data_table.data FROM (SELECT DISTINCT data_id, timestamp_micro FROM (SELECT data_id, timestamp_micro, ROW_NUMBER() OVER (PARTITION BY key ORDER BY timestamp_micro DESC) row_index FROM geller_key_table WHERE (timestamp_micro >= 0 AND data_type = ? AND delete_status IS NULL)) ORDER BY timestamp_micro DESC) distinct_data_ids INNER JOIN geller_data_table ON distinct_data_ids.data_id = geller_data_table._id ORDER BY timestamp_micro DESC', ['PRIVACY_SETTINGS'], None, None]

Result: [object Object]

Called From:

android.database.sqlite.SQLiteDatabase.rawQuery(SQLiteDatabase.java:1484)

CLASS METHOD

android.database.sqlite.SQLiteDatabase

rawQuery

Arguments: ['SELECT geller_data_table.data FROM (SELECT DISTINCT data_id, timestamp_micro FROM (SELECT data_id, timestamp_micro, ROW_NUMBER() OVER (PARTITION BY key ORDER BY timestamp_micro DESC) row_index FROM geller_key_table WHERE (timestamp_micro >= 0 AND data_type = ? AND delete_status IS NULL)) ORDER BY timestamp_micro DESC) distinct_data_ids INNER JOIN geller_data_table ON distinct_data_ids.data_id = geller_data_table._id ORDER BY timestamp_micro DESC', ['PRIVACY_SETTINGS']]

Result: [object Object]

Called From: bbag.r(PG:7)

CLASS		METHOD
android.database.sqlite.SQLiteDatabase		getPath
		Arguments: []
		Result: /data/user/0/com.google.android.apps.maps /databases
		/portable_geller_nyankosensei452@gmail.com.db
		Return Value: /data/user
		/0/com.google.android.apps.maps/databases
		/portable_geller_nyankosensei452@gmail.com.db
		Called From:
№ FILE IO		
		Search:
CLASS	METHOD	A V

CLASS	METHOD
libcore.io.loBridge	open
	Arguments: ['/data/user/0/com.google.android.apps.maps/files/phenotype /shared /com.google.android.libraries.notifications#com.google.android.apps.maps.
	pb', 0] **Result: java.io.FileDescriptor@742cbe6
	Called From: java.io.FileInputStream. <init>(FileInputStream.java:160)</init>
libcore.io.loBridge	open
	Arguments: ['/data/user/0/com.google.android.apps.maps/cache/image_manager_disk_cache/journal', 0]
	Result: java.io.FileDescriptor@73a5058
	Called From: java.io.FileInputStream. <init>(FileInputStream.java:160)</init>

CLASS	METHOD
libcore.io.loBridge	open
	Arguments: ['/data/user/0/com.google.android.apps.maps/cache/image_manager_disk_cache/journal', 1089]
	Result: java.io.FileDescriptor@9f05fd2
	Called From: java.io.FileOutputStream. <init>(FileOutputStream.java:236)</init>
libcore.io.loBridge	open
	Arguments: ['/data/user/0/com.google.android.apps.maps/shared_prefs /settings_preference.xml', 577]
	Result: java.io.FileDescriptor@6132b3d

CLASS	METHOD
libcore.io.loBridge	open
	Arguments: ['/data/user/0/com.google.android.apps.maps/cache /image_manager_disk_cache /1410b6fa31ebdb53cbaa35a0c88d0332c06dfed70a6ed5f3ac74e359b813eaed .0', 0]
	Result: java.io.FileDescriptor@98c3e39
	Called From: java.io.RandomAccessFile. <init>(RandomAccessFile.java:289)</init>
libcore.io.loBridge	open
	Arguments: ['/data/user/0/com.google.android.apps.maps/cache/image_manager_disk_cache/a8f77f7622996643cfabb887683350c5658c9283b61bb45661da6685efb9827b.0', 0]
	Result: java.io.FileDescriptor@ecf8c5a
	Called From: java.io.RandomAccessFile. <init>(RandomAccessFile.java:289)</init>

CLASS	METHOD	
libcore.io.loBridge	open	
	Arguments: ['/data/user/0/com.google.android.apps.maps	s/cache
	/image_manager_disk_cache	
	/ah10n1a5h255a57a2daad51a07c1h12an52hn5722a52270	cf06cc7070263665
CRYPTO - HASH		
CRYPTO - HASH	Search:	
CRYPTO - HASH	Search: METHOD	

ava.security.MessageDigest	update
	Arguments: [[104, 116, 116, 112, 115, 58, 47, 47, 103, 122, 48, 46, 103, 111, 111, 103, 1 1 1, 117, 115, 101, 114, 99, 111, 110, 116, 101, 110, 116, 46, 99, 111, 109, 47, 112, 47, 65, 70, 49, 81, 105, 112, 77, 49, 84, 48, 70, 69, 112, 69, 84, 72, 57, 69, 76, 71, 49, 51, 74,
	109, 85, 57, 83, 85, 45, 98, 76, 82, 107, 75, 101, 57, 49, 103, 110, 69, 69, 66, 111, 106, 61, 119, 57, 55, 56, 45, 104, 55, 55, 49, 45, 110, 45, 107, 45, 110, 111, 45, 118, 49]]
	Called From: hod.a(PG:2)

CLASS	METHOD
java.security.MessageDigest	update
	Arguments: [[0, 0, 3, -46, 0, 0, 3, 3]]
	Called From: hmd.a(PG:5)
java.security.MessageDigest	
, , , , ,	update
	update Arguments: [[97, 110, 100, 114, 111, 105, 100, 46, 103, 114, 97,
	·
	Arguments: [[97, 110, 100, 114, 111, 105, 100, 46, 103, 114, 97,

CLASS	METHOD
java.security.MessageDigest	digest
	Arguments: []
	Result: 100,-61,-110,-115,62,34,-64,42,127,-8,-2,-16,-53,-121,35,16,76,-59,31,-100,82,-33,-60,66,-3,121,54,42,102,94,-86,91
	Return Value:
	100-61-110-1156234-6442127-8-2-16-53-121351676-5931-10082- 33-6066-3121544210294-8691
	Called From: kxd.J(PG:5)
java.security.MessageDigest	update
	Arguments: [[104, 116, 116, 112, 115, 58, 47, 47, 103, 122, 48, 46,
	103, 111, 111, 103, 108, 101, 117, 115, 101, 114, 99, 111, 110, 116, 101, 110, 116, 46, 99, 111, 109, 47, 112, 47, 65, 70, 49, 81, 105,
	112, 77, 49, 84, 48, 70, 69, 112, 69, 84, 72, 57, 69, 76, 71, 49, 51, 74,
	109, 85, 57, 83, 85, 45, 98, 76, 82, 107, 75, 101, 57, 49, 103, 110,
	69, 69, 66, 111, 106, 61, 119, 57, 55, 56, 45, 104, 55, 55, 49, 45,
	110, 45, 107, 45, 110, 111, 45, 118, 49]]
	Called From: hod.a(PG:2)

CLASS	METHOD
java.security.MessageDigest	update
	Arguments: [[47, 99, 108, 105, 101, 110, 116, 95, 115, 116, 114, 101, 97, 109, 122, 47, 103, 101, 108, 108, 101, 114, 47, 99, 97, 99, 104, 101, 47, 99, 108, 101, 97, 110, 117, 112, 47, 100, 101, 108, 101, 116, 105, 111, 110, 95, 114, 101, 97, 115, 111, 110, 95, 119, 105, 116, 104, 95, 99, 111, 114, 112, 117, 115]] Called From: biau.a(PG:2)
ava.security.MessageDigest	digest
	Arguments: []
	Result: -3,-104,101,-48,-26,-43,110,-121,48,7,-103,69,90,10,2,-101
	Return Value: -3-104101-48-26-43110-121487-1036990102-101
	Called From: biau.a(PG:3)

		Search:	
CLASS	*	METHOD	A V
dalvik.system.DexClassLoader		\$init .	
		Arguments: ['/data/data/com.google/cache/frida5362665045325383304.c/data/com.google.android.apps.map' <instance: \$cdalvik.system.pathclassloader="" java.lang.classloader,="">']</instance:>	ex', '/data os/code_cache', None,
		Called From: None	
Showing 1 to 1 of 1 entries			
			Previous 1 Next
♣ BASE64			
		Search:	
CLASS	♦ METHOD	1	A

CLASS	METHOD
android.util.Base64	decode
	Arguments: [[67, 103, 81, 89, 65, 67, 65, 66], 0, 8, 3]
	Result: 10,4,24,0,32,1
	Return Value: 104240321
	Called From: android.util.Base64.decode(Base64.java:138)
android.util.Base64	decode
	Arguments: ['CgQYACAB', 3]
	Result: 10,4,24,0,32,1
	Return Value: 104240321
	Decoded String:
	Called From: bgvp.a(PG:3)

CLASS	METHOD
android.util.Base64	decode
	Arguments: [[69, 103, 56, 83, 68, 81, 104, 118, 69, 78, 122, 78, 111, 113, 47,
	108, 77, 82, 103, 66, 75, 65, 65, 83, 68, 120, 73, 78, 67, 70, 81, 81, 111, 53, 113
	55, 116, 101, 85, 120, 71, 65, 69, 111, 65, 65, 61, 61, 10, 32, 32, 32, 32], 0, 53,
	0]
	Result: 18,15,18,13,8,111,16,-36,-51,-94,-81,-
	27,49,24,1,40,0,18,15,18,13,8,84,16,-93,-102,-69,-75,-27,49,24,1,40,0
	Return Value:
	18151813811116-36-51-94-81-27492414001815181388416-93-102-69-75-27
	49241400
	Called From: android.util.Base64.decode(Base64.java:138)
CLASS	METHOD
	METHOD decode
CLASS android.util.Base64	
	decode
	decode Arguments:

Return Value:

Decoded String: ol(T1(

Called From: aofl.aU(PG:2)

49241400

 $18151813811116 \hbox{-} 36 \hbox{-} 51 \hbox{-} 94 \hbox{-} 81 \hbox{-} 27492414001815181388416 \hbox{-} 93 \hbox{-} 102 \hbox{-} 69 \hbox{-} 75 \hbox{-} 27$

CLASS	METHOD
android.util.Base64	encode
	Arguments: [[10, 10, 8, 4, 16, -92, -86, -33, -81, 6, 24, 1, 10, 8, 8, 3, 16, -10, -46, -54, -81, 6, 10, 8, 8, 2, 16, -110, -93, -34, -81, 6], 0, 32, 0]
	Result: 67,103,111,73,66,66,67,107,113,116,43,118,66,104,103,66,67,103,103,73,65, 120,68,50,48,115,113,118,66,103,111,73,67,65,73,81,107,113,80,101,114,119 ,89,61,10
	Return Value: 671031117366666710711311643118661041036667103103736512068504811 511311866103111736765738110711380101114119896110
	Called From: android.util.Base64.encode(Base64.java:496)

CLASS	METHOD
android.util.Base64	encodeToString
	Arguments: [[10, 10, 8, 4, 16, -92, -86, -33, -81, 6, 24, 1, 10, 8, 8, 3, 16, -10, -46, -54, -81, 6, 10, 8, 8, 2, 16, -110, -93, -34, -81, 6], 0]
	Result: CgoIBBCkqt+vBhgBCggIAxD20sqvBgoICAIQkqPerwY=
	Return Value: CgoIBBCkqt+vBhgBCggIAxD20sqvBgoICAIQkqPerwY=
	Decoded String: 한 년 펜
	Called From: aofl.aQ(PG:1)
android.util.Base64	encode
	Arguments: [[10, 10, 8, 4, 16, -92, -86, -33, -81, 6, 24, 1], 0, 12, 0]
少 DEVICE DATA	
	Search:
CLASS	♦ METHOD ♦

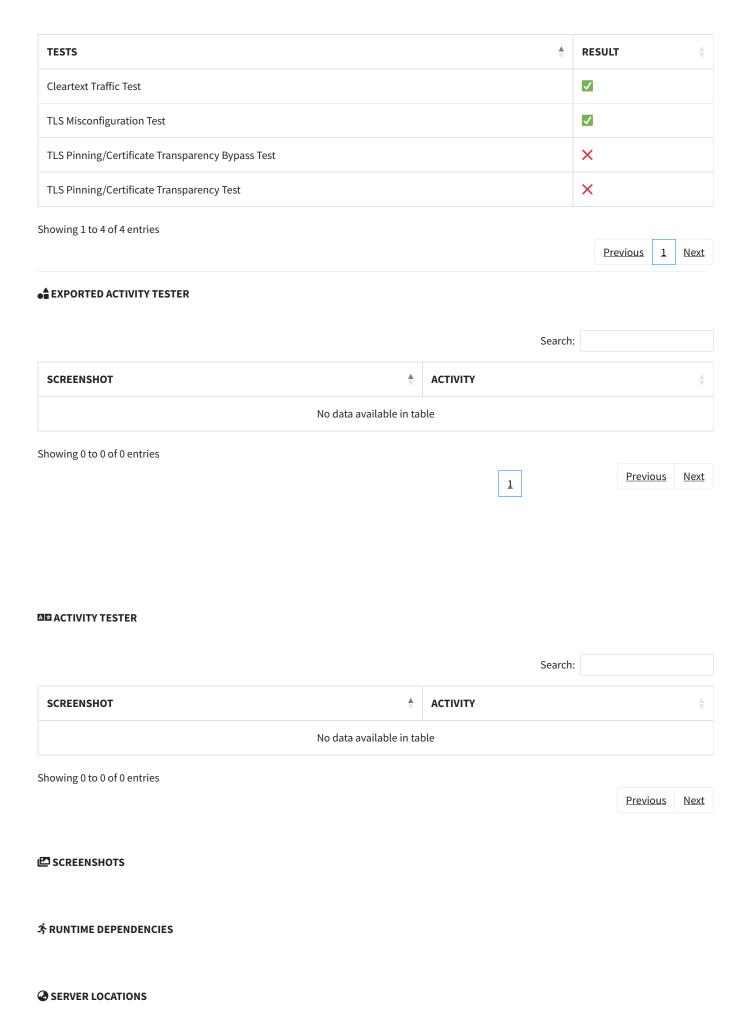
CLASS	METHOD
android.content.ContentResolver	query
	Arguments: [' <instance: \$classname:="" android.net.uri\$stringuri="" android.net.uri,="">', ['value'], '<instance: android.os.bundle="">', None]</instance:></instance:>
	Result: [object Object]
	Called From: android.content.ContentResolver.query(ContentResolver. ava:1115)
android.content.ContentResolver	query
	Arguments: [' <instance: \$classname:="" android.net.uri\$stringuri="" android.net.uri,="">', ['value'], 'name=?', ['use_location_for_services'], None]</instance:>
	Result: [object Object]

CLASS	METHOD
android.content.ContentResolver	query
	Arguments: [' <instance: \$classname:="" android.net.uri\$stringuri="" android.net.uri,="">', ['value'], '<instance: android.os.bundle="">', None]</instance:></instance:>
	Result: [object Object]
	Called From: android.content.ContentResolver.query(ContentResolver.j ava:1115)
android.content.ContentResolver	query
	Arguments: [' <instance: \$classname:="" android.net.uri\$stringuri="" android.net.uri,="">', ['value'], 'name=?', ['use_location_for_services'], None] Result: [objectect]</instance:>
	Called From: apwy.a(PG:1)

CLASS	METHOD
android.content.ContentResolver	query
	Arguments: [' <instance: \$classname:="" android.net.uri\$stringuri="" android.net.uri,="">', ['value'], '<instance: android.os.bundle="">', None]</instance:></instance:>
	Result: [object Object]
	Called From: android.content.ContentResolver.query(ContentResolver.j ava:1115)
android.content.ContentResolver	query
	Arguments: [' <instance: \$classname:="" android.net.uri\$stringuri="" android.net.uri,="">', ['value'], 'name=?', ['use_location_for_services'], None] Result: [object Object] Called From: apwy.a(PG:1)</instance:>

CLASS	METHOD
android.content.ContentResolver	query
	Arguments: [' <instance: \$classname:="" android.net.uri\$stringuri="" android.net.uri,="">', ['value'], '<instance: android.os.bundle="">', None]</instance:></instance:>
	Result: [object Object]
	Called From: android.content.ContentResolver.query(ContentResolver.j ava:1115)
android.content.ContentResolver	query
	Arguments: [' <instance: \$classname:="" android.net.uri\$stringuri="" android.net.uri,="">', ['value'], 'name=?', ['use_location_for_services'], None]</instance:>
	Result: [object Object]
	Called From: apwy.a(PG:1)
TLS/SSL Security Tester	

Search:





This app may communicate with the following OFAC sanctioned list of countries.

		Sea	arch:	
DOMAIN	A	COUNTRY/REGION		

DOMAIN	COUNTRY/REGION

[®] CALCAL MALWARE CHECK

Search:

DOMAIN	•	STATUS \$	GEOLOCATION
android.googleapis.com		good	IP: 142.251.12.95 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
clients4.google.com		good	IP: 172.217.194.100 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
connectivitycheck.gstatic.com	good	IP: 142.251.175.94
		Country: United States of America
		Region: California
		City: Mountain View
		Latitude: 37.405991
		Longitude: -122.078514
		View: Google Map
geller-pa.googleapis.com	good	IP: 142.251.10.95
		Country: United States of America
		Region: California
		City: Mountain View
		Latitude: 37.405991
		Longitude: -122.078514
		View: <u>Google Map</u>
google.comurlhttps	good	No Geolocation information available.
instantmessaging-pa.googleapis.com	good	IP: 142.250.4.95
		Country: United States of America
		Region: California
		City: Mountain View
		Latitude: 37.405991
		Longitude: -122.078514
		View: Google Map

DOMAIN	STATUS	GEOLOCATION	
mobilemaps-pa-gz.googleapis.com	good	IP: 216.239.38.135	
		Country: United States of America	
		Region: California	
		City: Mountain View	
		Latitude: 37.405991	
		Longitude: -122.078514	
		View: Google Map	
play.googleapis.com	good	IP: 74.125.200.95	
		Country: United States of America	
		Region: California	
		City: Mountain View	
		Latitude: 37.405991	
		Longitude: -122.078514	
		View: Google Map	
source.android.com	good	IP: 172.217.194.100	
		Country: United States of America	
		Region: California	
		City: Mountain View	
		Latitude: 37.405991	
		Longitude: -122.078514	
		View: Google Map	

CLIPBOARD DUMP

Country: United States of America

URLS

https://android.googleapis.com/auth

www.google.com

https://source.android.com/security/selinux/device-policy#label_new_services_and_address_denials

https://mobile maps-pa-gz.googleap is.com/google.internal.mothership.maps.mobile maps.people follow. v1. mobile maps people follows ervice /getpeople followinfo

https://mobilemaps-pa-gz.googleapis.com/google.internal.mothership.maps.mobilemaps.merchantstatus.v1.mobilemapsme 1 htstatusservice /getmerchantstatus

https://www.google.com/generate_204

https://www.googleapis.com/socialuserlocation/v1/userlocationfrontend/readsharingstate

https://google.com&url=https://timeline.google.com

https://play.googleapis.com/play/log?format=raw&proto_v2=true

https://android.googleapis.com/checkin

https://play.googleapis.com/play/log/timestamp

www.googleapis.com

https://www.googleapis.com/auth/android_checkin

https://clients4.google.com/generate_204

http://connectivitycheck.gstatic.com/generate_204

https://instantmessaging.pa.googleap is.com/google.internal.communications.instantmessaging.v1.registration/signingaia. In the property of t

https://mobilemaps-pa-gz.googleapis.com/google.internal.mothership.maps.mobilemaps.passiveassist.v1.mobilemapspassiveassistservice/getcontent

https://geller-pa.googleapis.com/geller.oneplatform.gellerservice/batchsync

https://mobile maps-pa-gz.googleap is.com/google.internal.mothership.maps.mobile maps.v1.mobile maps service/app start to the start of the start o

https://www.googleapis.com/androidantiabuse/v1/x/create? alt=proto&key=aizasybofczsglss7bonbjzpekk4rywzoiz-ltihttps://mobilemaps-pa-gz.googleapis.com/google.internal.mothership.maps.mobilemaps.v1.mobilemapsservice/userinfo

EMAILS

tsbogend@alpha.franken
nyankosensei452@gmail.com
dm-devel@redhat.com
genymotion-build@genymobile.com
240812035@24.08
giometti@linux.it
maxk@qualcomm.com
tigran@aivazian.fsnet
ller_nyankosensei452@gmail.com

₹ TRACKERS

		Search:		
TRACKER NAME	•	CATEGORIES	URL	Å
	No	data available in table		

♣ BASE64 STRINGS DECODED

CALLED	•	DECODED STRING
aofl.aQ(PG:1)		ċų∰
aofl.aQ(PG:1)		*
aofl.aQ(PG:1)		÷ų į į
aofl.aQ(PG:1)		
aofl.aQ(PG:1)		÷ų į.
aofl.aQ(PG:1)		÷
aofl.aQ(PG:1)		ាំ ឬ 🗷

Ò

Ò

ិ ម្ 🛚

Showing 1 to 10 of 65 entries

<u>Previous</u>	1	2	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	7	Next
-----------------	---	---	----------	----------	----------	----------	---	------

Search:

SQLITE DATABASE

aofl.aQ(PG:1)

aofl.aQ(PG:1)

aofl.aQ(PG:1)

FILES

data/data/com.google.android.apps.maps/app_webview/Default/Cookies

data/data/com.google.android.apps.maps/databases/-1_optimized_threads.notifications.db

data/data/com.google.android.apps.maps/databases/-1_threads.notifications.db

data/data/com.google.android.apps.maps/databases/1_optimized_threads.notifications.db

data/data/com.google.android.apps.maps/databases/1_threads.notifications.db

data/data/com.google.android.apps.maps/databases/juthreads.notifications.db

data/data/com.google.android.apps.maps/databases/gmm_myplaces.db

data/data/com.google.android.apps.maps/databases/gmm_storage.db

data/data/com.google.android.apps.maps/databases/gmm_storage.db

FILES data/data/com.google.android.apps.maps/databases/gnp_fcm_database data/data/com.google.android.apps.maps/databases/google_app_measurement_local.db Showing 1 to 10 of 21 entries 1 **XML FILES** Search: **FILES** data/data/com.google.android.apps.maps/shared_prefs/_has_set_default_values.xml data/data/com.google.android.apps.maps/shared_prefs/com.google.android.gms.appid.xml data/data/com.google.android.apps.maps/shared_prefs/com.google.android.gms.measurement.prefs.xml data/data/com.google.android.apps.maps/shared_prefs/com.google.android.libraries.notifications.GCM.xml $\underline{data/data/com.google.android.apps.maps/shared_prefs/com.google.firebase.messaging.xml}$ data/data/com.google.android.apps.maps/shared_prefs/fcm_registration_data.xml **FILES** data/data/com.google.android.apps.maps/shared_prefs /<u>FirebaseHeartBeatQ0hJTUVfQU5EUk9JRF9TREs+MTo3NDc2NTQ1MjAyMjA6YW5kcm9pZDowMDAwMDAwMDAwMDAwMDAw.xml</u> data/data/com.google.android.apps.maps/shared_prefs /FirebaseHeartBeatW0RFRkFVTFRd+MTo2NTgxMDQzOTU0MTY6YW5kcm9pZDpmOTJhZjkzNWMxN2RjNjU4OTA5MmVk.xml <u>data/data/com.google.android.apps.maps/shared_prefs/gnp_encryption.xml</u> data/data/com.google.android.apps.maps/shared_prefs/phenotype_com.google.android.libraries.social.populous.xml Showing 1 to 10 of 15 entries **B**OTHER FILES 1 Search: **FILES** data/data/com.google.android.apps.maps/app_/testdata/map_cache.key data/data/com.google.android.apps.maps/app_webview/Default/Cookies-journal data/data/com.google.android.apps.maps/app_webview/variations_seed data/data/com.google.android.apps.maps/app_webview/variations_stamp

FILES
data/data/com.google.android.apps.maps/cache/ClearcutDeferredMetrics.txt
data/data/com.google.android.apps.maps/cache/cronet-cache-40719148/disk_cache/index
data/data/com.google.android.apps.maps/cache/cronet-cache-40719148/disk_cache/index-dir/the-real-index
data/data/com.google.android.apps.maps/cache/cronet-cache-40719148/prefs/local_prefs.json
data/data/com.google.android.apps.maps/cache/cronet-cache-40719148/version
data/data/com.google.android.apps.maps/cache/data/user/0/com.google.android.apps.maps/no_backup/androidx.work.workdb.lck

Showing 1 to 10 of 93 entries

Previous 1 2 3 4 5 ... 10 Next

© 2024 Mobile Security Framework - MobSF | <u>Ajin Abraham</u> | <u>OpenSecurity</u>.

Version v3.9.5 Beta