

ÁGORA
POLICIAL

Francisco Arenaz Benito

ANÁLISIS FORENSE DE LA APLICACIÓN WHATSAPP EN SISTEMAS ANDROID E IOS



Ediciones Universidad
Salamanca

ANÁLISIS FORENSE DE LA APLICACIÓN WHATSAPP EN SISTEMAS ANDROID E IOS

Francisco Arenaz Benito

ANÁLISIS FORENSE DE LA APLICACIÓN WHATSAPP EN SISTEMAS ANDROID E IOS

Ediciones Universidad
Salamanca



Ediciones Universidad de Salamanca
y Francisco Arenaz Benito

1.ª edición:

ISBN (PDF): 978-84-1091-202-1

DOI: <https://doi.org/10.14201/OAP0003>

Ediciones Universidad de Salamanca
eusal.es

Hecho en UE-Made in EU



Usted es libre de: Compartir — copiar y redistribuir el material en cualquier medio o formato Ediciones Universidad de Salamanca no revocará mientras cumpla con los términos:

-  Reconocimiento — Debe reconocer adecuadamente la autoría, proporcionar un enlace a la licencia e indicar si se han realizado cambios. Puede hacerlo de cualquier manera razonable, pero no de una manera que sugiera que tiene el apoyo del licenciador o lo recibe por el uso que hace.
-  NoComercial — No puede utilizar el material para una finalidad comercial.
-  SinObraDerivada — Si remezcla, transforma o crea a partir del material, no puede difundir el material modificado.



Ediciones Universidad de Salamanca es miembro de la UNE
Unión de Editoriales Universitarias Españolas www.une.es

*A mi mujer, Nayra,
y a mis amigos y compañeros,
gracias por vuestra paciencia
ante los innumerables mensajes
y notificaciones que hicieron posible
la elaboración de este libro.*

Índice general

1. Introducción	17
1.1. Notas aclaratorias	20
1.1.1. JID	23
1.1.2. LID	24
1.1.3. Identificador único de mensaje	25
1.1.4. Hashes	26
1.1.5. Protobuf	29
1.1.6. Sincronizaciones	31
2. Estructura de la instalación de la aplicación Whatsapp (Android – iOS)	33
3. Tipos de mensajes y comunicaciones de Whatsapp (Android – iOS)	39
3.1. Tipos de mensaje por su contenido	39
3.2. Tipos de mensajes por su destinatario	41
3.3. Tipos especiales de comunicaciones	42
4. Bases de datos de Whatsapp (Android)	43
4.1. Base de datos axolotl.db	44
4.1.1. identities	45
4.1.2. Sessions	45

4.2. Base de datos chatsettings.db	46
4.3. Base de datos companion_devices.db	47
4.3.1. Devices	47
4.4. Base de datos emojidictionary.db	48
4.5. Base de datos location.db	49
4.5.1. location_cache	49
4.5.2. location_sharer.....	50
4.6. Base de datos msgstore.db	52
4.6.1. backup_changes.....	57
4.6.2. bot_message_info.....	57
4.6.3. call_link	58
4.6.4. call_log	58
4.6.5. call_log_participant_v2	60
4.6.6. chat	60
4.6.7. chat_ephemeral.....	63
4.6.8. group_participant_device.....	63
4.6.9. group_participant_user.....	64
4.6.10. group_past_participant_user.....	65
4.6.11. jid	65
4.6.13. labeled_jid	68
4.6.14. labels.....	69
4.6.15. lid_display_name.....	69
4.6.17. message.....	70
4.6.18. message_add_on.....	76
4.6.19. message_add_on_event_response.....	78
4.6.20. message_add_on_keep_in_chat.....	78
4.6.21. message_add_on_pin_in_chat.....	79
4.6.22. message_add_on_poll_vote	80
4.6.23. message_add_on_poll_vote_selected_option	80
4.6.24. message_add_on_reaction.....	81
4.6.25. message_add_on_receipt_device.....	81
4.6.26. message_album	82
4.6.27. message_association.....	83

4.6.28. message_call_log.....	83
4.6.29. message_details.....	84
4.6.30. message_edit_info	84
4.6.31. message_ephemeral	85
4.6.32. message_ephemeral_setting.....	85
4.6.33. message_event.....	87
4.6.34. message_forwarded.....	88
4.6.35. message_ftsv2_content	88
4.6.36. message_limit_sharing_setting	89
4.6.37. message_location.....	90
4.6.38. message_media	91
4.6.39. message_mentions.....	93
4.6.40. message_poll	93
4.6.41. message_poll_option.....	94
4.6.42. message_privacy_state.....	94
4.6.43. message_quoted	95
4.6.44. message_revoked	96
4.6.45. message_system.....	97
4.6.46. message_thumbnail	100
4.6.47. message_vcard.....	101
4.6.48. message_vcard_jid.....	101
4.6.49. message_view_once_media	102
4.6.50. newsletter.....	103
4.6.51. newsletter_message	104
4.6.52. newsletter_subscribers	104
4.6.53. played_self_receipt	105
4.6.54. receipt_device.....	105
4.6.55. receipt_user.....	106
4.6.56. status.....	107
4.6.57. status_message_info.....	108
4.6.58. user_device	109
4.7. Base de datos wa.db	110
4.7.1. group_membership_count.....	112
4.7.2. group_relationship.....	112

4.7.3. subgroup_info.....	113
4.7.4. wa_address_book.....	114
4.7.5. wa_block_list.....	114
4.7.6. wa_contacts.....	115
4.7.7. wa_contacts_created_within_wa.....	116
4.7.8. wa_group_add_black_list.....	117
4.7.9. wa_group_admin_settings	117
5. Bases de datos de Whatsapp (iOS)	119
5.1. Base de datos Biz.sqlite	120
5.1.1. ZWABIZPROFILEDATA	121
5.1.2. ZWABIZVERIFIEDNAMEDATA	122
5.2. Base de datos CallHistory.sqlite	123
5.2.1. ZWAAGGREGATECALLEVENT	124
5.2.2. ZWACDCALLEVENT	125
5.2.3. ZWACDCALLEVENTPARTICIPANT	126
5.3. Base de datos ChatStorage.sqlite	127
5.3.1. ZWABLACKLISTITEM	128
5.3.2. ZWACHATPUSHCONFIG.....	129
5.3.3. ZWACHATSESSION.....	129
5.3.4. ZWAGROUPINFO.....	132
5.3.5. ZWAGROUPMEMBER.....	135
5.3.6. ZWAGROUPMEMBERSCHANGE.....	136
5.3.7. ZWAMEDIAITEM	137
5.3.8. ZWAMESSAGE.....	140
5.3.9. ZWAMESSAGEDATAITEM.....	147
5.3.10. ZWAMESSAGEINFO	149
5.3.11. ZWAPROFILEPICTUREITEM.....	153
5.3.12. ZWAPROFILEPUSHNAME	153
5.3.13. ZWAVCARDMENTION	154
5.4. Base de datos ContactsV2.sqlite	155
5.4.1. ZWAADDRESSBOOKCONTACT	155
5.5. Base de datos DeviceAgents.sqlite	157
5.5.1. ZWASMBDEVICEAGENT	158

5.6. Base de datos emoji.sqlite	159
5.7. Base de datos ExtChatDatabase.sqlite	160
5.7.1. message_parent_association	161
5.8. Base de datos Labels.sqlite	162
5.9. Base de datos LID.sqlite	163
5.9.1. ZWALIDPROPERTIES	164
5.9.2. ZWAPHONENUMBERLIDPAIR	165
5.9.3. ZWAZACCOUNT	165
5.10. Base de datos Sticker.sqlite	166
5.11. Base de datos AppState.sqlite	167
5.11.1. ZAPPSTATECONFIRMEDMUTATIONENTITY	168
5.11.2. ZAPPSTATEENCRYPTIONKEYENTITY	170
5.12. Base de datos Axolotl.sqlite	170
5.12.1. ZWAAXOLOTLIDENTITY	171
5.12.2. ZWAAXOLOTLSESSION	172
5.13. Base de datos ChatSearchV5f.sqlite	173
5.13.1. docs_content	173
5.13.2. metadata	175
5.14. Base de datos LocalKeyValue.sqlite	175
5.14.1. ZWAKEYVALUEELEMENT	176
5.15. Base de datos Location.sqlite	176
5.15.1. ZWAFINALLOCATIONRECIPIENT	177
5.15.2. ZWALOCATIONSENDER	178
6. Archivos de interés de Whatsapp (Android)	179
6.1. Directorio /data/data/com.whatsapp/files	179
6.1.1. /data/data/com.whatsapp/files/	180
6.1.2. /data/data/com.whatsapp/files/.Shared/	180
6.1.3. /data/data/com.whatsapp/files/.Trash/	180
6.1.4. /data/data/com.whatsapp/files/decompressed/libs. spo/.superpack_version	181
6.1.5. /data/data/com.whatsapp/files/Logs/	181
6.1.6. /data/data/com.whatsapp/files/ViewOnce/	185

6.2. Directorio /data/data/com.whatsapp/shared_prefs/	185
6.2.1. backup_prefs.xml	185
6.2.2. com.whatsapp_preferences.xml	185
6.2.3. com.whatsapp_preferences_light.xml	186
6.2.4 disappearing_mode_prefs.xml	188
6.2.5. reg_prefs.xml	188
6.2.6. register_phone_prefs.xml	189
6.2.7. startup_prefs.xml	189
6.3. Directorio /data/media/0/Android/media/com.whatsapp/WhatsApp/	190
6.3.1. /data/media/0/Android/media/com.whatsapp/WhatsApp/Shared/	190
6.3.2. /data/media/0/Android/media/com.whatsapp/WhatsApp/Backups/	190
6.3.3. /data/media/0/Android/media/com.whatsapp/WhatsApp/Databases/	191
6.3.4. /data/media/0/Android/media/com.whatsapp/WhatsApp/Media/	191
7. Archivos de interés de Whatsapp (iOS)	193
7.1. Directorio "Shared"	193
7.1.1. /gif/	194
7.1.2. /Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist	195
7.1.3. /Media/Profile/	196
7.1.4. /Message/Media/	196
7.1.5. /stickers/	197
7.1.6. /AppState/<GUID>/AppState.sqlite	197
7.1.7. /Logs/WhatsApp_2/	197
7.2. Directorio "Data"	201
7.2.1. /Camera/	201
7.2.2. /Caches/	202
7.2.3. /SplashBoard/	204

8. Análisis de características y funcionalidades de interés (Android – iOS)

205

8.1. Usuarios, grupos, listas de difusión, comunidades y canales.....	205
8.1.1. Contactos.....	206
8.1.2. Grupos.....	211
8.1.3. Difusiones.....	215
8.1.4. Comunidades.....	218
8.1.5. Canales.....	226
8.2. Nomenclatura de archivos transmitidos por Whatsapp.....	229
8.3. Confirmación de recepción y lectura de mensajes.....	232
8.3.1. Mensajes enviados y recibidos (Android).....	234
8.3.2. Mensajes enviados y recibidos (iOS).....	239
8.4. Vinculación de dispositivos.....	241
8.5. Restringir un chat.....	251
8.6. Descarga de archivos recibidos.....	254
8.7. Copias de seguridad / backups.....	257
8.7.1. Copia de seguridad en Google Drive (Android).....	258
8.7.2. Copia de seguridad local (Android).....	260
8.7.3. Copia de seguridad en iCloud (iOS).....	263
8.7.4. Copia de seguridad local (iOS).....	263
8.8. Inteligencia artificial.....	265
8.9. Privacidad avanzada del chat.....	268

9. Análisis de mensajes

(Android – iOS)	273
9.1. Mensajes de texto.....	273
9.1.1. Mensajes editados.....	273
9.2. Notas de voz y vídeo.....	279
9.3. Mensajes adjuntando imágenes y vídeos.....	281
9.4. Mensajes adjuntando documentos.....	293
9.5. Mensajes de ubicación.....	296

9.5.1. Ubicación en tiempo real.....	296
9.5.2. Ubicación actual o lugares cercanos.....	296
9.6. Reacción a un mensaje.....	298
9.7. Mensaje reenviado.....	300
9.8. Citar un mensaje.....	303
9.9. Mensaje fijado.....	313
9.10. Estados.....	315
10. Eliminación de mensajes (Android – iOS)	319
10.1. Mensajes temporales.....	319
10.1.1. Mensajes conservados	325
10.2. Mensajes de visualización única.....	329
10.3. Mensajes eliminados por el usuario.....	335
10.3.1. Eliminar para mí	335
10.3.2. Eliminar para todos.....	338
10.3.3. Eliminar para todos (como administrador)	342
10.4. Vaciado de chat.....	349
10.5. Eliminación de chat	351
Apéndice: recuperación de datos	355
Referencias.....	359

1. Introducción

WhatsApp es una aplicación de mensajería instantánea adquirida por Meta (anteriormente Facebook) en 2014. La aplicación permite, a través de internet, enviar y recibir mensajes de texto, voz o vídeo, así como compartir archivos multimedia (audios, imágenes o vídeos), documentos, ubicaciones, contactos, GIFs, stickers, realizar llamadas de voz y videollamadas con uno o varios participantes simultáneamente.

Es una aplicación multiplataforma cuyo ámbito inicial se limitaba a dispositivos móviles (iOS y Android), pero que posteriormente amplió su compatibilidad a ordenadores mediante navegadores web y aplicaciones de escritorio para Windows y macOS, también para el sistema operativo KaiOS, y por último, para sistemas iPadOS. Actualmente, es la aplicación de mensajería más utilizada a nivel global, superando ampliamente a alternativas como Telegram o Signal, con más de 2.000 millones de usuarios en todo el mundo, incluyendo más de 35 millones en España.

Dada su popularidad en la población española, no es sorprendente que WhatsApp también sea utilizado para cometer ilícitos, ya sea de manera directa (amenazas, grooming, distribución de pornografía infantil, entre otros) o indirecta (mediante conversaciones o transmisión de archivos que vinculen a los interlocutores con un delito).

Desde una perspectiva forense, es crucial tener en cuenta que WhatsApp está en constante evolución. Los desarrolladores introducen cambios frecuentes en la aplicación, que van desde modificaciones menores hasta actualizaciones significativas. Aunque estas actualizaciones puedan parecer irrelevantes para el usuario final, pueden incluir alteraciones importantes en la estructura de las bases de datos. Por lo tanto, este análisis debe considerarse como una guía inicial para entender la interacción con los diferentes archivos de la aplicación y adaptarse a los cambios futuros que puedan surgir con nuevas versiones.

Es probable que, en el momento en que este documento sea consultado, ya esté desactualizado respecto a la última versión de WhatsApp. Sin embargo, su objetivo principal sigue siendo proporcionar una comprensión básica del funcionamiento de la aplicación e incentivar al analista a experimentar y estudiar casos específicos, utilizando la información inicial como base para ampliarla con las nuevas implementaciones. Cabe destacar que la mayoría de las actualizaciones son menores, orientadas principalmente a añadir funcionalidades, manteniendo la estructura de las bases de datos y el significado de sus valores. Por ejemplo, los identificadores asignados a los diferentes tipos de mensajes (texto, audio, etc.) se han mantenido constantes, al menos, durante los últimos diez años, salvo por la incorporación de nuevos tipos.

La cantidad de información que WhatsApp puede almacenar en sus bases de datos y archivos es inmensa. Este estudio se centra en la información más relevante desde un punto de vista forense, incluyendo ejemplos prácticos aplicables al análisis de casos. La mayoría de los datos de uso de la aplicación se registran en bases de datos SQLite v3. Estas bases de datos contienen múltiples tablas organizadas en campos (columnas) con sus respectivos valores. Debido a su volumen y complejidad, no es práctico ni posible abordar todos los campos. Por ello, las explicaciones se complementan con imágenes de las tablas relevantes, destacando únicamente los campos que clarifican el análisis, reorganizados para facilitar la comprensión visual. Además, se han convertido los valores de fechas en formato Unix Epoch u OS X Epoch a fechas entendibles para el lector.

Columna o Campo

Fila o Registro

_id	chat_row_id	from_me	key_id	sender_jid_row_id	status
6	3	1	E1BE8B6FAEF52B474EE4468BC140B13	3	6
7	4	1	FB5084578F84401CF364C3DFE6703935	0	6
8	4	1	FC50D68D1D64B81B696D92616BC48E9B	9	6
9	4	1	D0D2D7625867F8E0038A58ED97C89FC5	3	6

Ilustración 1. Base de datos SQLite

Existen diferentes bases de datos, tablas o campos entre los ficheros de la aplicación WhatsApp que se obvian, ya sea por la carencia de interés, por contener duplicidad de información en relación con otras tablas o campos, o por desconocer el significado del registro.

No hay información oficial del funcionamiento interno de la aplicación publicada por Meta, habiendo obtenido todo el contenido que se expone a partir de la investigación propia realizada para el desarrollo de la presente publicación. Para llevar a cabo este estudio se han utilizado tres terminales con sistema operativo Android, Poco X3 NFC (Android 12), Samsung J4+ (Android 8.1) y Xiaomi Redmi 4 (Android 10), con diferentes versiones de la aplicación para sistemas Android (2.23.15.3, 2.23.17.72, 2.24.4.76, 2.24.10.79, 2.24.12.78, 2.24.23.78, 2.24.25.77, 2.25.1.75, 2.25.22.80 y 2.25.32.75). Para el análisis de la versión para iOS se ha hecho uso de un iPhone SE 2 (iOS 17.5.1, 18.4.1 y 26.2) y iPhone 7 (iOS 15.8.2 y 15.8.5), con las versiones de WhatsApp (2.24.15.79, 2.24.17.78, 2.24.25.93, 2.25.1.80, 2.25.23.82 y 2.25.33.77).

Se ha observado, principalmente en Android, que la integración de los datos de una versión antigua en otra más moderna es diferente dependiendo de las versiones implicadas. Hay que entender que, con la salida de nuevas versiones de la aplicación, los desarrolladores crean nuevas tablas y cambian campos de tablas viejas. Por ello hay datos contenidos en “viejas tablas” que se conservan en campos de nuevas tablas de la versión actualizada.

Todo este dinamismo en el desarrollo de la aplicación implica que muchos datos grabados en las bases de datos sean redundantes, con importantes implicaciones como son la “facilidad” para poder obtener

algún tipo concreto de dato o la posibilidad de contrastar si un dato ha podido ser modificado maliciosamente.

Las posibles solicitudes de informes sobre el uso de WhatsApp, tanto en el ámbito penal como en el civil, pueden ser tan diversas como la información que la aplicación registra. Esta variedad resulta inabarcable para un estudio de este tipo, por lo que el analista debe ser imaginativo y meticuloso al buscar la información en el dispositivo digital.

Actualmente, la mayoría del software forense especializado en el procesamiento de datos de teléfonos móviles es capaz de mostrar la información principal de la aplicación. Sin embargo, es fundamental que el analista verifique manualmente dicha información, ya que, en ocasiones, el software puede presentar errores de interpretación o no proporcionar los datos necesarios para llegar a conclusiones precisas.

La información que genera y almacena la aplicación en los dispositivos móviles es inconmensurable, por lo que ha sido necesario acotar esta investigación y es la razón por la que hay temas, funcionalidades o particularidades de la aplicación que no se exponen.

No obstante, se intenta proporcionar suficientes datos para ofrecer un punto de partida desde el cual, si la naturaleza del análisis lo requiere, el investigador pueda continuar y profundizar en el funcionamiento de la aplicación.

1.1. Notas aclaratorias

El propósito de este punto es facilitar la comprensión de este estudio, fijando unos conceptos claros de la aplicación. Con relación a los tipos de mensajes que se pueden intercambiar en WhatsApp, es muy importante ser consciente de la diferencia que hay entre un mensaje de voz o un mensaje de vídeo, y los mensajes en los que se adjunta un archivo de tipo audio o de vídeo. Para evitar la confusión, en adelante serán nombrados por su traducción de la versión inglesa de los directorios o carpetas donde se almacenan este tipo de archivos en sistemas

Android (WhatsApp Voice Notes y WhatsApp Video Notes). Por ello, el mensaje de voz será denominado como "**nota de voz**" y el mensaje de vídeo como "**nota de vídeo**".

En este estudio, siempre que se utilice el término enviado o recibido, se hace teniendo como referencia el dispositivo cuya aplicación instalada se está analizando. Puede ser que en alguna ocasión se especifique que la dirección de la comunicación es desde o hacia el usuario investigado, pero en todos los casos el punto de observación es el del dispositivo de este usuario.

En el mismo sentido, el usuario de la cuenta que se analiza se denomina "usuario" o "usuario de esta cuenta" y el resto de los usuarios individuales con los que interactúa serán "contactos". En casos muy concretos puede que se llegue a denominar "contacto" a un usuario que no sea un contacto de la cuenta analizada, y no esté grabado en su agenda, pero que se encuentre relacionado de alguna forma a través de la aplicación.

Las marcas de tiempo (timestamp) se registran en la aplicación en formato UTC. En la versión de Android se almacena en formato UNIX Epoch, la mayoría de los registros en milisegundos (13 dígitos) y algunos en segundos (10 dígitos) o nanosegundos (16 dígitos). En su versión de iOS la mayor parte de los registros se almacenan en formato OS X, si bien otros se graban en formato UNIX Epoch. Como norma general, los ejemplos gráficos se observarán con las fechas en formato legible, debido a que previamente han sido transformadas para que sean entendibles por el lector.

Con el mismo fin, en las ilustraciones de tablas de bases de datos se mostrarán los campos que se han estimado como más didácticos, existiendo una clara limitación de espacio. Por el mismo motivo, se han resumido los registros de logs plasmados, a aquellos que son más significativos en cada operación analizada.

Se han realizado diferentes pruebas combinando sistemas operativos, versiones de la aplicación y dispositivos, concluyendo que WhatsApp obtiene la hora automáticamente (desde servidores), con los posibles desfases que se pueden generar por la grabación de registros o las propias comunicaciones. Esto implica que es intrascendente la fecha/

hora que un usuario establezca en su dispositivo, incluso aunque tenga la intención de ocultar un momento concreto, porque no afectará a la grabación de las fechas en las bases de datos de la aplicación que serán automáticas y proporcionadas por servidores en formato UTC. Si el usuario establece un cambio de hora, se actualizará la hora de los mensajes visualizados en la pantalla del dispositivo del usuario a la nueva establecida, pero en las bases de datos no se modificará ninguna fecha.

En un dispositivo que se encuentre con la aplicación instalada y funcional, si se atrasa varios días la fecha del dispositivo, la aplicación indica que la fecha es incorrecta, debiendo ajustar la fecha para que la aplicación se abra. Si se adelanta varios meses, la aplicación presenta un enlace para descargar una versión supuestamente actualizada. Esto es debido a que las distintas versiones tienen una fecha caducidad y una vez que vencen, no permiten abrir la aplicación hasta que se instale una versión acorde con la fecha que se ha establecido en el dispositivo. Este bloqueo no afecta a la extracción de la información del dispositivo en sí, pero cuando por algún motivo se quiere interactuar con la interfaz gráfica de la aplicación es necesario establecer manualmente en el dispositivo una fecha en el rango en el que la versión es operativa.

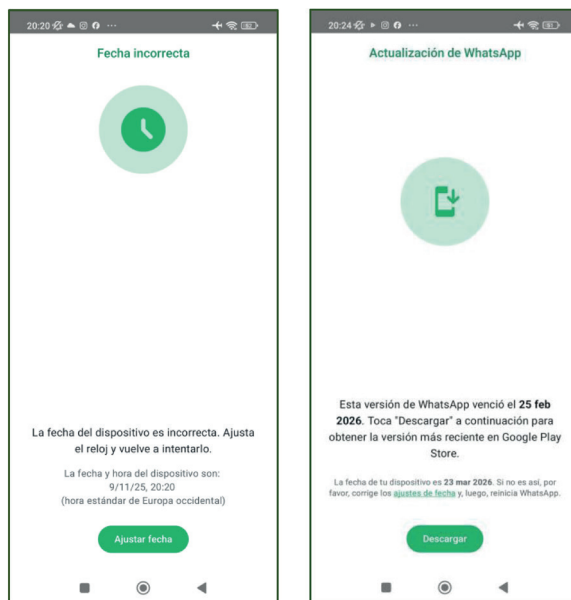


Ilustración 2. Error en el inicio de la aplicación en la versión de Android

1.1.1. JID

Es fundamental tener una noción clara de la forma en la que la aplicación identifica a los usuarios, grupos, difusiones, comunidades o canales, siendo por medio del **Jabber Identifier**¹ o "jid". Es un identificador único, que la aplicación genera y asigna de una forma diferente en cada caso, tal y como se explica a continuación:

- **Usuarios individuales:** prefijo internacional + número de teléfono + @s.whatsapp.net.
Ej: 34677988122@s.whatsapp.net
- **Estados de usuarios:** prefijo internacional + número de teléfono + @status.
Ej: 34677988122@status

Como excepción, el estado del propio usuario de la cuenta siempre estará registrado en su propia cuenta como "status@broadcast".

- **Grupos:**
 - *Formato antiguo* (hasta mediados de noviembre de 2021): prefijo internacional + número de teléfono del creador del grupo – fecha de creación del grupo en formato UTC Unix Epoch (segundos) + @g.us.
Ej: 34699888777-1379114707@g.us
 - *Formato actual:* 18 dígitos + @g.us
Ej: 120363080564732172@g.us
- **Difusión:** fecha en la que se creó la difusión en formato UTC Unix Epoch (segundos) + @broadcast.
Ej: 1690524142@broadcast
- **Comunidades:** 18 dígitos + @g.us
Ej: 120363080564732172@g.us
- **Canales:** 18 dígitos + @newsletter.
Ej: 120363165396843331@newsletter

1. "jid" es un identificador único utilizado en el protocolo de comunicaciones Jabber/XMPP (Extensible Messaging and Presence Protocol). Sirve con una dirección distintiva para individuos o entidades participantes en la mensajería instantánea.

1.1.2. LID

El "lid" es otro identificador único que crea la aplicación y que complementa al "jid". Tiene unas diferencias muy significativas respecto al Jabber Identifier (jid). El "lid" única y exclusivamente se asigna a usuarios individuales (a ningún grupo, difusión, comunidad) y aparentemente tiene la función de mantener la privacidad de los usuarios de WhatsApp. A diferencia del "jid", el identificador "lid" no permite por sí mismo identificar al usuario, ya que es una numeración generada por la aplicación no relacionada con el número de teléfono del usuario. Además, no es posible visualizar el identificador "lid" de un contacto en ningún apartado de la interfaz gráfica de la aplicación.

El identificador "lid" está formado por 15 dígitos + @lid. En el siguiente ejemplo se muestra el modo en el que se registran estos identificadores en la versión de iOS, en la tabla "**ZWAZACCOUNT**" de la base de datos "**LID.sqlite**" (versión para iOS):

ZDISPLAYNAME	ZIDENTIFIER	ZPHONENUMBER
+34.....64	222359768326203@lid	346 [REDACTED]
	262074978558186@lid	346 [REDACTED]
+34.....55	148846453755945@lid	346 [REDACTED]
+34.....14	204101308694769@lid	
+34.....11	242493903896807@lid	346 [REDACTED]
	211213690634324@lid	346 [REDACTED]

Ilustración 3. Tabla **ZWAZACCOUNT** de la base de datos **LID.sqlite**

En las pruebas realizadas a lo largo de un periodo de un par de años, se ha observado que el uso de este identificador "lid" se utilizaba inicialmente en las comunidades para identificar a participantes que no eran contactos del usuario de la cuenta, pero posteriormente se ha ido incrementando su importancia y presencia en la identificación de los participantes en los grupos.

Todo este desarrollo apunta a que, en un futuro cercano, los usuarios de WhatsApp puedan identificarse a través de "nombres de usuario" tipo @usuario como alternativa a compartir el número de teléfono. Posiblemente el nombre se asocie al identificador "lid".

Tanto en las versiones de Android como en las de iOS, hay tablas que vinculan el identificador "lid" de un usuario con el prefijo internacional y los últimos dos dígitos de su número de teléfono. En la versión de Android hay que consultar y vincular las tablas "**lid_display_name**" y "**jid**" de la base de datos "**msgstore.db**", y en la versión de iOS consultar la tabla "**ZWAZACCOUNT**" de la base de datos "**LID.sqlite**".

Cuando se trata de contactos del usuario grabados en la agenda y, por tanto, conocidos, existe una tabla que relaciona el identificador "jid" y el "lid" de cada uno de ellos. En la versión de Android hay que consultar y vincular las tablas "**jid_map**" y "**jid**" de la base de datos "**msgstore.db**". En la versión de iOS nuevamente se debe consultar la tabla "**ZWAZACCOUNT**" de la base de datos "**LID.sqlite**", pero en vez de facilitar el identificador "jid", expone el número de teléfono.

1.1.3. Identificador único de mensaje

Todos los mensajes que se envían a través de la aplicación WhatsApp tienen asignado un identificador único que los individualiza. El único caso en el que dos o más mensajes tienen el mismo identificador es el mensaje que se envía en una difusión. Técnicamente es un solo mensaje y probablemente es el motivo por el que se le asigna un único identificador, remitiéndose el mismo mensaje a tantos contactos como se encuentren incluidos en la difusión de este usuario.

Cuando se envía un mensaje y se le asigna un identificador, dicho identificador se grabará en las bases de datos de ambos interlocutores.

En la versión para Android, el identificador se nombra generalmente como "**key_id**" y en la versión para iOS como "**ZSTANZAID**".

El identificador del mensaje es una secuencia que varía **de 9 hasta 32 caracteres hexadecimales** y se puede determinar la versión de la aplicación desde la que se envió el mensaje por dicho identificador:

- 9-10 dígitos: en algunos mensajes del sistema (únicamente en la versión de Android).

- 18 caracteres hexadecimales: se envió a través de la versión de la aplicación para Windows.
- 20 caracteres hexadecimales, empezando por la secuencia:
 - **3EBO** se envió el mensaje a través de la versión WEB.
 - **3A** se envió el mensaje a través de versión de la aplicación para iOS, iPadOS o la versión para macOS.
 - **5E** se envió el mensaje a través de versión de la aplicación para iOS.
- 30 o 32 caracteres hexadecimales: se envió el mensaje a través de la versión para dispositivos Android.

1.1.4. Hashes

Entre los muchos datos que almacena la aplicación WhatsApp de su propio uso, se encuentran los hashes de los archivos multimedia transmitidos (imágenes, audios, vídeos, documentos, gifs, stickers/avatares, notas de voz y de vídeo). En cualquier análisis forense que conlleve determinar la autenticidad e integridad de un archivo es necesario obtener los hashes. Ciertamente hay una gran variedad de hashes que proporcionan una mayor o menor seguridad, y en el caso de esta aplicación hace uso del SHA-256, un hash que actualmente está considerado libre de colisiones (no se ha conseguido generar dos ficheros diferentes con el mismo hash) y por tanto seguro.

Android

La tabla en la que se graban estos datos no es otra que la que registra la información de los archivos transmitidos "**message_media**" de la base de datos "**msgstore.db**". Aunque en dicha tabla se almacenan varios hashes, por cada archivo transmitido, nos vamos a centrar en los que se encuentran en los campos "**file_hash**" y "**original_file_hash**". A continuación, se profundiza en el método para decodificar el hash en cualquier archivo transmitido, con la excepción que presenta cuando se envía desde la cuenta analizada una imagen o un vídeo en "calidad HD" cuya decodificación es un poco más compleja.

- **file_hash**: este campo almacena el hash SHA-256 del archivo enviado o recibido, codificado en Base64. Siempre se registra el hash del archivo transmitido, incluso cuando un archivo es recibido pero el usuario no lo ha descargado en su dispositivo y por tanto no se encuentra en la memoria del teléfono.
- **original_file_hash**: en este campo se graba el hash del archivo original, codificado en Base64. Cuando se envía un archivo como imagen o vídeo, la aplicación genera una versión comprimida, que es la que realmente se transmite y cuyo hash se almacena en el campo "**file_hash**". En estos casos se puede relacionar el archivo original y su versión comprimida enviada por el usuario de la cuenta analizada. El archivo original puede ser una imagen o un vídeo que se encuentre en el sistema de archivos del dispositivo o uno generado desde la propia aplicación con la cámara. Hay que subrayar que en ningún caso se registrará el hash del archivo original desde el que se generó su versión comprimida de una imagen o vídeo que se haya recibido.

Es importante recordar que los hashes son un cálculo matemático con salida **hexadecimal**. Cuando se proceda a decodificar el hash habrá que indicar que la conversión sea de **Base64 a hexadecimal**. En caso de que se seleccionara de **Base64 a texto** el resultado sería completamente **erróneo**.

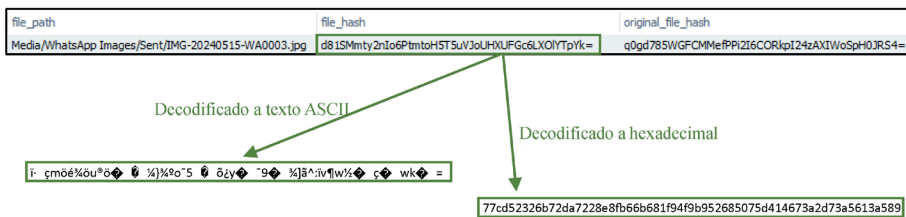


Ilustración 4. Decodificación del hash del archivo transmitido

Imágenes y vídeos en calidad HD:

Cuando se envían desde la cuenta analizada imágenes o vídeos en "calidad HD" se puede verificar que se ha aplicado esta opción debido a que en el campo "**original_file_hash**" se grabará el hash del archivo

original con 64 caracteres en vez de 44 que se graba cuando la calidad es estándar, y siempre terminará este hash codificado con los caracteres "T0taGQ=". El hash está codificado doblemente en Base64 y en una primera instancia hay que decodificar de **Base64** a **ASCII**, obteniendo el hash SHA-256 codificado en Base64 junto con el texto que indica que se trata de un archivo en calidad HD ("-hd"), siendo ésta la razón de la diferencia del número de caracteres. El segundo paso es el explicado en el párrafo anterior, que no es otro que decodificar el resultado (sin los caracteres "-hd") de **Base64** a **hexadecimal**, obteniendo el hash SHA-256 del archivo original.

En el ejemplo que a continuación se muestra, se ha enviado la misma imagen que en el ejemplo anterior, pero en calidad HD. Como podrá observar el lector, tras la primera decodificación del hash original, se obtiene el mismo hash SHA-256 codificado en Base64 que el registrado en el ejemplo anterior (campo "**original_file_hash**"), puesto que es el mismo archivo original enviado en diferentes calidades.

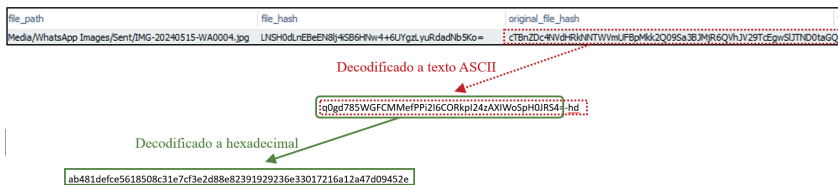


Ilustración 5. Decodificación del hash del archivo original en envío en calidad HD

iOS

La aplicación WhatsApp almacena los hashes de los archivos en la tabla "**ZWAMEDIAITEM**" de la base de datos "**ChatStorage.sqlite**", concretamente en el campo "**ZVCARDNAME**". Cuando son mensajes multimedia (imágenes, audios, vídeos, documentos, gifs, stickers/ avatares, notas de voz y de vídeo) almacena sus hashes SHA-256 codificados en Base64. Como se ha mencionado anteriormente, el hash se debe decodificar de Base64 a hexadecimal. A diferencia de la versión de Android, el campo en el que se almacenan los hashes no es exclusivo para este propósito, sino que, dependiendo del tipo de mensaje, puede

contener distintos datos. Tampoco existe un campo en el que almacene los hashes de los archivos de imagen o vídeo originales antes de ser comprimidos por la aplicación para enviarlos.

- **ZVCARDNAME:** este campo almacena el hash SHA-256 del archivo enviado o recibido, codificado en Base64. Siempre se registra el hash del archivo transmitido, incluso cuando un archivo es recibido pero el usuario no lo ha descargado en su dispositivo y por tanto no se encuentra en la memoria del teléfono.

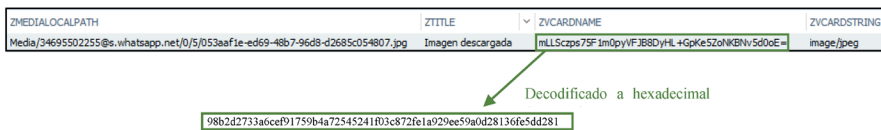


Ilustración 6. Decodificación del hash del archivo transmitido

1.1.5. Protobuf

Protocol Buffers, también denominado **Protobuf**, es un formato binario de almacenamiento de datos de código abierto desarrollado por Google, cuyo objetivo es ser más compacto y rápido que XML. La facilidad con la que permite el intercambio de información es, probablemente, el motivo por el que los desarrolladores de WhatsApp lo han implementado en diversos campos de las bases de datos de la versión para iOS. Su uso implica que sea necesario un número significativamente menor de tablas en la base de datos principal para registrar la información, en comparación con la versión de Android.

Para el analista, Protobuf supone un hándicap a la hora de obtener e interpretar la información almacenada en este tipo de archivos, especialmente si se tiene en cuenta que concentran la mayoría de las características aplicadas a los mensajes: temporalidad, si se ha citado, fijado, reenviado, entre otras.

En la actualidad, ninguna de las principales herramientas comerciales de análisis forense digital (Cellebrite, Oxygen, Magnet...) automatiza la extracción ni la interpretación de los archivos Protobuf presentes en diferentes campos de la base de datos "**ChatStorage.sqlite**".

La búsqueda y el análisis de estos campos pueden automatizarse si el analista desarrolla el código necesario para tal fin. Como alternativa, es posible realizar un análisis manual, aunque se trata de un proceso especialmente tedioso debido a que el formato no es especialmente intuitivo.

Habitualmente, la información Protobuf se encuentra almacenada en archivos con extensión **".proto"**; sin embargo, cuando se embebe en bases de datos, como ocurre en WhatsApp, se registra en campos de tipo **BLOB (Binary Large Object)**. En estos campos, los datos pueden encontrarse codificados directamente en **hexadecimal**, o bien en **Base64**. Según el decodificador empleado, puede ser necesario convertir previamente la información de Base64 a hexadecimal.

Existen diferentes decodificadores de código abierto como "Protobuf Decoder" (aplicación ejecutable en línea y en local) que son capaces de interpretar directamente información protobuf en formato hexadecimal y en Base64. Para un análisis forense, lo recomendado es que la estación de trabajo se encuentre sin conexión a internet y se trabaje con herramientas en local.

Cuando se decodifican estos archivos están divididos en campos (fields), los cuales pueden estar subdivididos en otros campos (fields) con la información de interés. En el presente estudio solo se hará referencia e interpretará los campos cuyo significado se haya podido deducir de las pruebas realizadas y contengan datos presumiblemente importantes para una investigación.

En los archivos protobuf, la información de los valores en ocasiones se puede interpretar de varias formas. Es importante que cuando el campo sea de tipo "varint" se tome el valor mostrado "As uint" y cuando sea de tipo "fixed64" se tome el valor mostrado "As double".

Como ejemplo, se muestra gráficamente cómo realizar la interpretación de una reacción a un mensaje en el que se ha seleccionado un emoticono del pulgar hacia arriba. Esta información se encuentra en hexadecimal en el campo **"ZRECEIPTINFO"** de la tabla **"ZWAMESSAGEINFO"** en la base de datos **"ChatStorage.sqlite"**

The image shows a screenshot of a Protobuf Decoder application. At the top, there's a table labeled 'Tabla ZWAMESSAGEINFO' with columns Z_PK, Z_ENT, Z_OPT, ZMESSAGE, and ZRECEIPTINFO. Below it, a hex dump shows binary data. The main part of the image is the 'Protobuf Decoder' interface, which has a text input field containing a long hex string. Below the input, the 'Result' section displays a table of decoded fields. Annotations with red boxes and arrows point to specific parts of the result table: 'campos (field)' points to the 'Field Number' column; 'Id. del mensaje de reacción a un mensaje' points to the 'Content' of field 1; 'emoticono' points to the 'Content' of field 2; and 'Fecha de la reacción a mensaje en formato UTC Unix Epoch' points to the 'Content' of field 3.

Byte Range	Field Number	Type	Content
0-41	7	protobuf	
0-39	2	protobuf	
0-22	1	string	3AD0BEDE34ECE4A056D4
22-28	2	string	8
28-35	3	varint	As uint: 1724966901122 As sint: 882482430581
35-37	4	varint	As uint: 1 As sint: -1

Ilustración 7. Resultado de la decodificación de archivo protobuf mediante la aplicación “Protobuf Decoder”

Cuando se haga mención en este estudio a los campos y subcampos de un archivo protobuf, se utilizará la separación por guiones para individualizarlos. Como ejemplo, tomando la ilustración anterior, para referenciar el “emoticono” se indicaría que se encuentra en el campo 7-2-2.

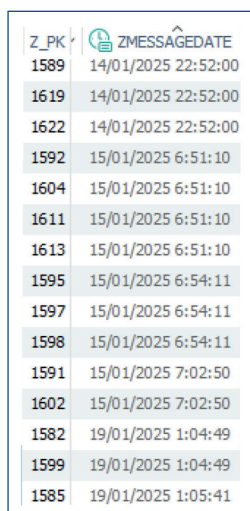
1.1.6. Sincronizaciones

La aplicación se debe sincronizar con los servidores de WhatsApp para actualizar la información de los mensajes enviados y recibidos. Aunque pueda parecer un hecho menor, es preciso señalar que la sincronización no es perfecta en relación con la fecha de recepción de los mensajes. Así es que hay ocasiones en las que cuando se sincroniza el dispositivo

y recibe varios mensajes a la vez, se graban mensajes más recientes antes que otros más antiguos en las bases de datos internas.

La mayoría de los programas que analizan las bases de datos de WhatsApp ordenarán los mensajes por la fecha de envío o recepción, y no se observará este desfase entre los números de registro y las fechas. Pero si se analizan directamente las bases de datos y se observa que la numeración de posición del registro en la tabla **"message"** en Android (campo **"_id"**) o la tabla **"ZWAMESSAGE"** en iOS (campo **"Z_PK"**) puede presentar un desfase, por lo que es conveniente ordenar los mensajes por la fecha de transmisión, para queden cronológicamente ordenados.

Este desfase es mucho más común en la versión de iOS que en la de Android, aunque cuando se sincroniza por primera vez un dispositivo vinculado, en ambas versiones se produce un desfase en la numeración del registro respecto a la fecha de transmisión importante.



Z_PK	ZMESSAGEDATE
1589	14/01/2025 22:52:00
1619	14/01/2025 22:52:00
1622	14/01/2025 22:52:00
1592	15/01/2025 6:51:10
1604	15/01/2025 6:51:10
1611	15/01/2025 6:51:10
1613	15/01/2025 6:51:10
1595	15/01/2025 6:54:11
1597	15/01/2025 6:54:11
1598	15/01/2025 6:54:11
1591	15/01/2025 7:02:50
1602	15/01/2025 7:02:50
1582	19/01/2025 1:04:49
1599	19/01/2025 1:04:49
1585	19/01/2025 1:05:41

*Ilustración 8. Mensajes registrados en la tabla **"ZWAMESSAGE"** ordenados por fecha de transmisión (versión iOS).*

2. Estructura de la instalación de la aplicación Whatsapp (Android – iOS)

La estructura de directorios de la aplicación difiere enormemente entre ambos sistemas operativos. Por ello, se muestra la estructura de una forma visual y en secciones posteriores del estudio se ampliará la información sobre los ficheros que contiene.

Android

En la instalación de WhatsApp en el sistema de archivos de teléfonos con sistema operativo Android se generan dos localizaciones importantes donde se almacenan los datos de la aplicación. La primera ubicación es considerada de máxima seguridad y el usuario común no puede acceder a su contenido a través de un explorador de archivos, a no ser que modifique el teléfono para obtener permisos de administrador (rootear el teléfono). La segunda localización almacena archivos transmitidos por medio de la aplicación, copias de seguridad, etc., a los que el usuario puede acceder sin restricciones.

Los sistemas operativos de Android y las capas de personalización aplicadas por los fabricantes de teléfonos son heterogéneas y, por tanto,

las rutas que a continuación se relacionan pueden diferir ligeramente dependiendo de la variante.

En el directorio localizado en la ruta **"/data/data/com.whatsapp"** se encuentran las bases de datos que almacenan los mensajes, contactos, etc., así como otros archivos de la aplicación de gran importancia como es la clave de cifrado o los archivos de configuración de la cuenta:

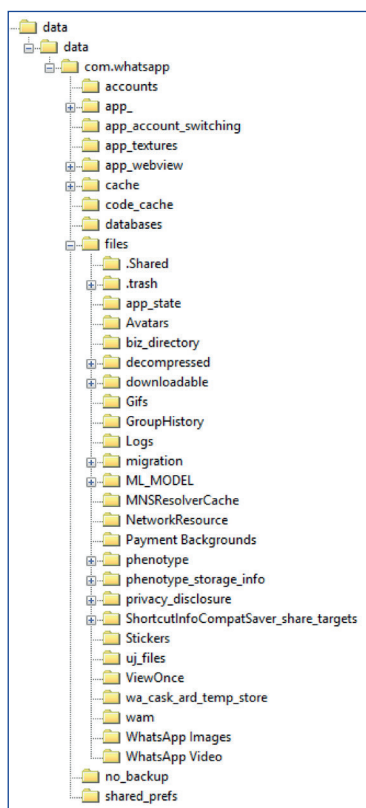


Ilustración 9. Estructura del directorio "data/data" de la versión Android

La otra ubicación de interés alberga entre otros ficheros, los archivos multimedia intercambiados o las copias de seguridad (backups) que realiza automáticamente la aplicación. A estas carpetas cualquier usuario puede acceder sin restricciones, como ya se ha mencionado anteriormente. Se encuentra en la ruta **"/data/media/0/Android/media/com.whatsapp"**:

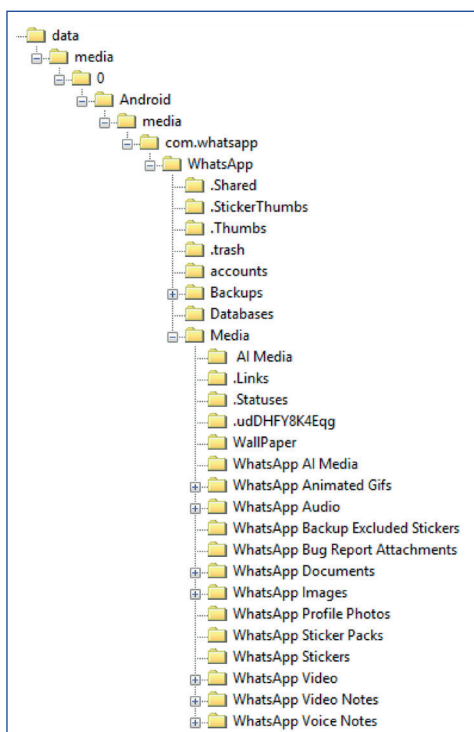


Ilustración 10. Estructura del directorio "data/media" de la versión de Android

iOS

En el sistema operativo iOS presenta una complejidad añadida en la adquisición de la información del dispositivo. Lo más probable es que el investigador adquiera una extracción de tipo iTunes backup o sus variaciones. Es una copia de seguridad que se genera a través del teléfono y que el desarrollador ha elegido los archivos que contendrá entre todos los que se almacenan en el dispositivo. Si bien esta extracción permite analizar las principales bases de datos, lo cierto es que no contiene toda la información de la aplicación. Dependiendo de las herramientas forenses de las que disponga el investigador, el modelo de iPhone y la versión de iOS, se podrá llevar a cabo una extracción completa de sistema de archivos (Full File System (FFS)) con toda la información de la aplicación. De todos modos, la estructura general de directorios es parcialmente similar en ambos tipos de extracciones.

Cuando se analiza una extracción FFS se observará que cada aplicación, en este caso WhatsApp se guarda en contenedores con **GUID** (Globally Unique Identifier, Identificador Único Global). Estos identificadores se generan cuando se instalan y la numeración no está asignada a una aplicación específica. Por tanto, la misma aplicación tendrá identificadores diferentes en diferentes iPhones. La numeración está formada por 32 valores hexadecimales divididos en 5 grupos y separados por guiones (8-4-4-4-12 valores). Incluso a la misma aplicación se le asigna diferentes GUID en el contenedor del directorio "Data" (en el iPhone analizado: **3B9F9C04-CE77-4788-AF30-D864A53D93C1**) y el directorio "Shared" (en el iPhone analizado: **8D324614-450B-4229-90E8-09389EE5E4F6**).

La aplicación WhatsApp almacena la mayor parte de su información operativa en el contenedor **"Shared"**, mientras que el contenedor **"Data"** conserva principalmente archivos temporales o residuales.

Los permisos de usuario y la interfaz del sistema operativo iOS no permiten que el usuario pueda acceder a ningún fichero de la aplicación, excepto a los archivos transmitidos.

En la siguiente ilustración se muestra la estructura de directorios, tal y como se genera en una copia de seguridad de iTunes Backup y en una extracción completa de sistema de archivos (FFS):

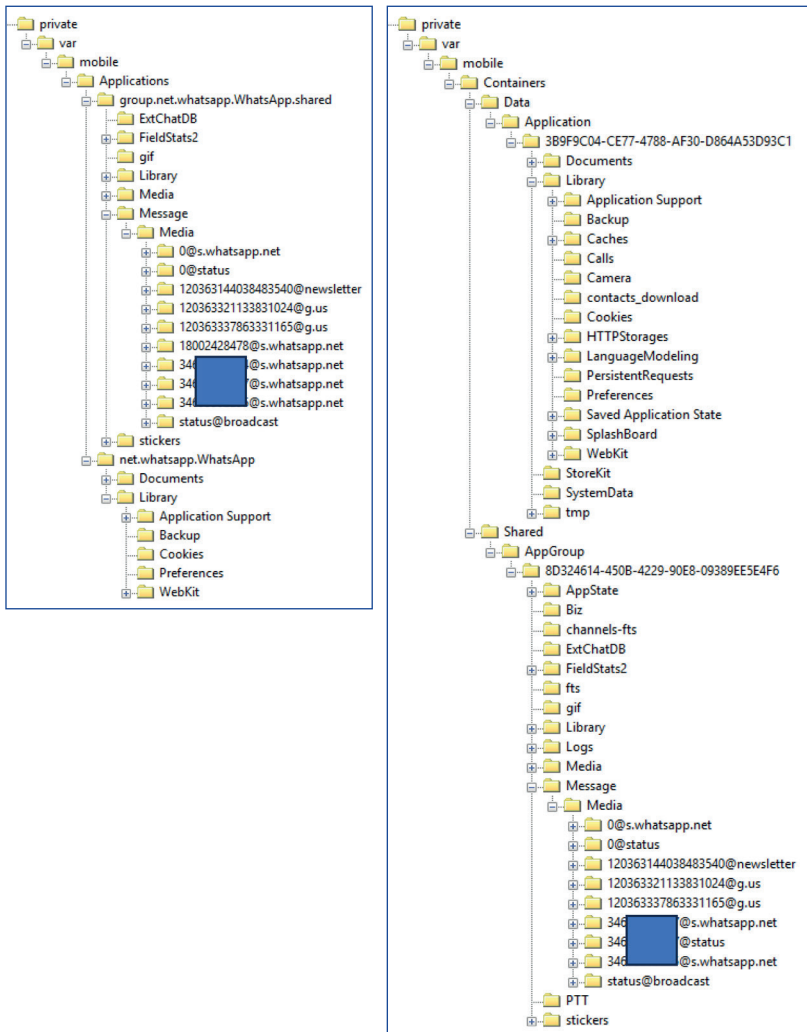


Ilustración 11. Estructura de directorios de la versión iOS en extracción iTunes Backup (izq.) y Full File System (dcha.)

3. Tipos de mensajes y comunicaciones de Whatsapp (Android – iOS)

Se ofrece una breve explicación sobre los tipos de comunicaciones que pueden realizarse con esta aplicación. Posteriormente, se amplía y profundiza, a nivel forense, en el análisis de los datos generados por las transmisiones consideradas a priori más relevantes.

3.1. Tipos de mensaje por su contenido

- **Mensajes de texto:** es el mensaje básico, en el que se envía texto.
- **Emojis:** pictogramas que pueden enviarse como mensaje de texto.
- **GIF:** Graphics Interchange Format (Formato de Intercambio de Gráficos). Los GIF son imágenes fijas o animaciones de corta duración que se repiten en bucle.
- **Stickers/Avatares:** los stickers son colecciones de imágenes con las que también se pueden expresar sentimientos, pero utilizando unos dibujos más grandes, temáticos y visibles que los emojis.

Los avatares son imágenes que intentan representar físicamente al usuario, pudiéndose crear con la propia aplicación.

- **Mensajes de voz o notas de voz:** mensajes generados a través de la grabadora de audio del teléfono.
- **Mensajes de vídeo o notas de vídeo:** mensajes generados con alguna de las cámaras del teléfono (con una duración máxima de 60 segundos).
- **Llamadas de audio y videollamadas:** se pueden realizar tanto con un contacto como grupales.
- **Archivos de imágenes y vídeos:** archivos con formatos de imagen (jpg, png...) o de vídeo (mp4, avi, 3gp...)
- **Archivos de audio:** archivos con formato de audio (mp3, wav...).
- **Documentos:** la aplicación permite enviar cualquier tipo de archivo con esta opción, hasta un tamaño máximo de 2 GB.
- **Ubicación:** existen dos formas de compartir la localización, la ubicación en tiempo real (dinámica) y la ubicación actual o lugares cercanos (estática).
- **Contacto:** tarjeta de contacto con los datos (nombre, teléfonos, correo electrónico, etc.) que el usuario dispone en su agenda de uno o varios contactos y quiera compartir con un tercero.
- **Encuestas:** permite generar una encuesta en un chat, en la que los usuarios pueden votar diferentes opciones aportadas por el creador de la encuesta.
- **Evento:** es un recordatorio de ocasiones especiales y tiene la posibilidad de planificar una llamada o videollamada entre los participantes en el chat.

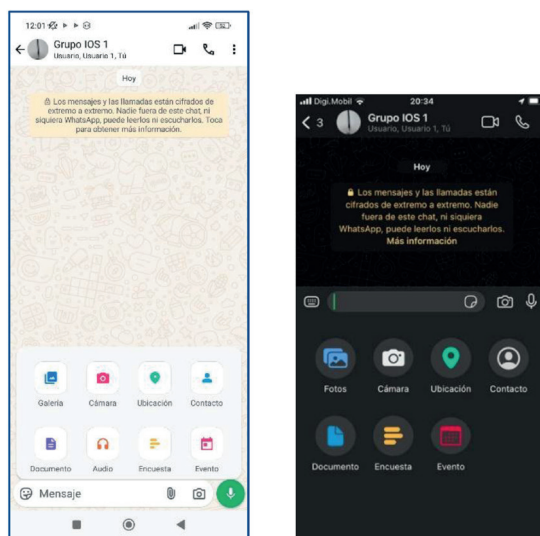


Ilustración 12. Capturas de pantalla de chat en Android (izq.) y en iOS (dcha.) con los tipos de mensaje seleccionables

3.2. Tipos de mensajes por su destinatario

- **Mensajes individuales:** comunicación con un único usuario de la aplicación.
- **Mensajes grupales:** comunicación con un grupo de usuarios. Para tal efecto, se tendrá que haber creado el grupo y haber agregado a los participantes (usuarios).
- **Mensajes en comunidades:** una novedad es la creación de comunidades, que permite reunir grupos relacionados. Por cada comunidad se crea un grupo de "Avisos" en el que los administradores pueden enviar avisos para comunicar novedades a los miembros. Los administradores pueden enviar todo tipo de mensajes. El resto de los participantes no pueden enviar ningún tipo de mensaje al grupo de "Avisos" de la comunidad. La comunidad puede estar formada por hasta 50 grupos, añadiendo un máximo de 5000 miembros al grupo de "Avisos" de la comunidad. Cuando se crea la comunidad también se genera un grupo "General", que es administrado por el creador de la

comunidad y al que se pueden unir voluntariamente cada uno de los miembros de la comunidad.

- **Lista de difusión o Difusión:** permite enviar un mensaje o archivo multimedia a varios contactos a la vez. A cada contacto añadido a la lista de difusión le aparecerá en su dispositivo como un mensaje individual del usuario de esta cuenta.
- **Canales:** los canales son una herramienta de transmisión unidireccional para que los administradores envíen texto, fotos, vídeos, stickers, notas de voz, notas de vídeo y encuestas, informando de novedades de personas y organizaciones. El usuario puede crearlos y/o seguir a otros creadores de contenido.

3.3. Tipos especiales de comunicaciones

- **Reacción a un mensaje:** es un emoji de pequeño tamaño que se añade a un mensaje recibido como respuesta al mismo.
- **Citar un mensaje:** es un tipo de respuesta en el que sobre el mensaje que se envía se incluye el mensaje al que se hace referencia para que su emisor sea consciente que es una respuesta a su mensaje.
- **Estados:** se puede publicar actualizaciones de texto, archivos multimedia (imágenes, vídeos y GIF) y notas de voz, que desaparecen después de que transcurran 24 horas desde que se compartieran.
- **Responder a un estado:** la aplicación permite que se envíe un mensaje de cualquier tipo como respuesta a un “estado” de un contacto.
- **Mención privada en un estado:** se envía una notificación que informa que el usuario ha mencionado a uno, varios contactos/grupos o viceversa. Las menciones son privadas y no se muestran a otros contactos que no estén mencionados, pudiéndose volver a compartir un estado con una mención como si fuera su propio estado.
- **Chat de audio:** es una especie de llamada de voz que se puede realizar en chats grupales, los cuales se pueden unir voluntariamente tras recibir una notificación push.

4. Bases de datos de Whatsapp (Android)

La aplicación WhatsApp centra el registro de la información de la interacción entre los usuarios en sus bases de datos. Éstas son de tipo SQLite versión 3 y usan archivos WAL (Write-Ahead Logging) donde se registran los cambios más recientes. Esta forma de operar tiene una serie de implicaciones en su análisis forense que hay que tener en consideración. Las herramientas comerciales permiten automatizar parte de la recuperación de datos a partir del archivo "WAL", pero tanto la base de datos como el archivo "WAL" pueden contener información borrada de interés que, en ocasiones, únicamente es posible recuperar mediante procedimientos manuales.

A continuación, se exponen las principales bases de datos, no obstante, hay que poner un límite en el presente estudio y, por ello, hay tablas que se han considerado de menor relevancia para los análisis habituales y no se describen. Igualmente, hay campos que no se muestran o detallan, ya sea porque resultan intrascendentes, repitan información de otros campos ya descritos o no haya sido posible dilucidar el significado de sus valores.

Tanto las diferentes bases de datos como las tablas que las componen se presentan en orden alfabético, no siendo su orden un indicador de la importancia relativa en las investigaciones. De hecho, sin desmerecer

otras tablas, la tabla **"message"** de la base de datos **"msgstore.db"** se puede considerar el núcleo de información de WhatsApp. Otras tablas de gran importancia son **"message_media"**, **"chat"** y **"jid"**, de la misma base de datos, que permiten relacionar los mensajes y archivos transmitidos con los participantes del chat. Por último, destaca la tabla **"wa_contacts"** de la base de datos **"wa.db"**, que registra los contactos que tiene almacenado el usuario en su cuenta.

4.1. Base de datos *axolotl.db*

Esta base de datos almacena las claves públicas de los contactos. Todos los contactos con los que se haya intercambiado las claves públicas se encontrarán en esta base de datos, incluso cuando se borre el usuario de la agenda del dispositivo y/o de WhatsApp.

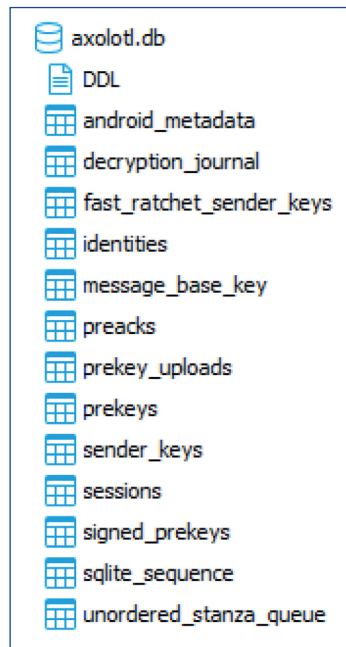


Ilustración 13. Tablas que conforman la base de datos "axolotl.db"

4.1.1. identities

Tabla que registra el intercambio de las claves públicas con cada contacto.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
recipient_id	Número parcial del identificador "jid" o "lid" del contacto que ha compartido la clave pública, sin el dominio. Se corresponde con el campo "user" de la tabla "jid" de la base de datos "msgstore.db".
recipient_type	Tipo de cuenta registrado en el campo "recipient_id": 0 : identificador "jid" del contacto. 1 : identificador "lid" del contacto.
device_id	Número de identificador del dispositivo del contacto. Se corresponde con el mismo campo "device" de la tabla "jid" de la base de datos "msgstore.db".
public_key	Clave pública compartida por el contacto. Un contacto tendrá dos identificadores, correspondientes a los tipos "jid" y "lid", pero ambos tendrán la misma clave pública al tratarse de un único contacto.
private_key	Clave privada del usuario de esta cuenta.
timestamp	Fecha de recepción o comprobación de la clave pública en formato UTC Unix Epoch (segundos).

Ilustración 14. Descripción de los campos de la tabla "identities"

4.1.2. Sessions

Tabla que registra la fecha de inicio de las conversaciones con cada contacto, desde que se instaló la aplicación en este dispositivo.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).

Campo	Descripción
recipient_id	Número parcial del identificador "jid" o "lid" del contacto que ha compartido la clave pública, sin el dominio. Se corresponde con el campo "user" de la tabla "jid" de la base de datos "msgstore.db".
recipient_type	Tipo de cuenta registrado en el campo "recipient_id": 0 : identificador de tipo "jid" del contacto. 1 : identificador de tipo "lid" del contacto.
device_id	Número de identificador del dispositivo del contacto. Se corresponde con el campo "device" de la tabla "jid" de la base de datos "msgstore.db".
timestamp	Fecha de inicio de la sesión de comunicación con el contacto en formato UTC Unix Epoch (segundos) desde la instalación de WhatsApp en este dispositivo.

Ilustración 15. Descripción de los campos de la tabla "sessions"

4.2. Base de datos *chatsettings.db*

Almacena datos sobre la configuración de las notificaciones de la aplicación (vibración, silenciar, luz, sonido de notificación, anclar el inicio de chats, fecha del anclaje de un chat en la barra de chats...) que el usuario aplica por defecto a sus chats individuales o grupales, y la configuración individualizada de cada chat si así lo ha dispuesto.

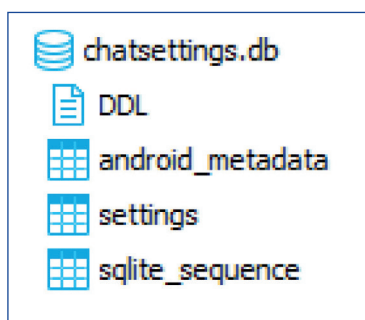


Ilustración 16. Tablas de la base de datos "chatsettings.db"

4.3. Base de datos *companion_devices.db*

Almacena información sobre los dispositivos vinculados con el dispositivo principal (no se han realizado pruebas con dispositivos con sistema operativo KaiOS).

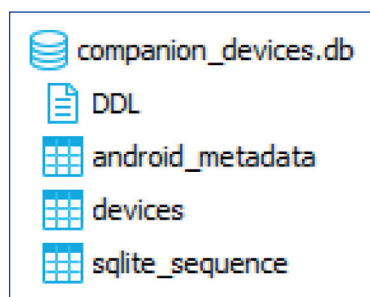


Ilustración 17. Tablas de la base de datos “*companion_devices.db*”

4.3.1. Devices

Tabla que contiene la información sobre los dispositivos que actualmente se encuentran vinculados con el dispositivo principal.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
device_id	Número de identificador “jid” del dispositivo vinculado. Ejemplo: 34612123123.0:5@s.whatsapp.net En este caso el “device” vinculado es el número “5”.
device_os	Sistema operativo del dispositivo vinculado: Windows, macOS (ordenador Mac), Linux , versión numérica de Android (en dispositivos con Android), iOS (iPhone), iPad y Wear OS .

Campo	Descripción
platform_type	Tipo de plataforma a través de la cual se ha vinculado la cuenta: 1: Navegador Chrome. 2: Navegador Firefox. 4: Navegador Opera. 5: Navegador Safari. 6: Navegador Edge. 7: Aplicación de escritorio para macOS. 8: Aplicación para iPad 9: Aplicación para tableta Android 14: Aplicación para iPhone. 16: Aplicación para teléfono Android. 18: Smartwatch. 21: Aplicación de escritorio para Windows 22: Dispositivo de Realidad Virtual (Oculus).
last_active	Última fecha en la cuenta estuvo activa en el dispositivo vinculado, en formato UTC Unix Epoch (milisegundos).
login_time	Fecha en la que se inició la vinculación de la cuenta en el dispositivo, en formato UTC Unix Epoch (milisegundos).
logout_time	Fecha en la que se desactivó la cuenta en el dispositivo vinculado, en formato UTC Unix Epoch (milisegundos).
place_name	Localización en la que se vinculó el dispositivo. En las pruebas realizadas únicamente se ha registrado este valor cuando se ha vinculado un Smartwatch con Wear OS.

*Ilustración 18. Descripción de los campos de la tabla “**devices**”*

4.4. Base de datos **emojidictionary.db**

Almacena todos los emojis de los que dispone el usuario. Consta de tres tablas, siendo “**emoji_search_tag**” donde se encuentran registrados los emojis.

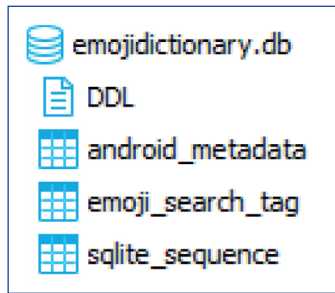


Ilustración 19. Tablas de la base de datos “**emojidictionary.db**”

4.5. Base de datos *location.db*

Almacena *temporalmente* información sobre las geolocalizaciones en tiempo real que ha recibido o enviado a otros usuarios. **Generalmente la base de datos está vacía** o con apenas datos, pero a partir del archivo “WAL” se puede llegar a recuperar gran cantidad de información.

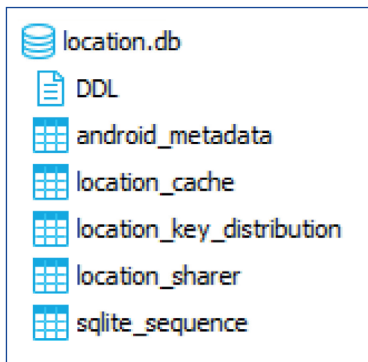


Ilustración 20. Tablas de la base de datos “**location.db**”

4.5.1. location_cache

Tabla que puede contener la información de los puntos que se han estado compartiendo durante la transmisión de la ubicación en tiempo real.

Son datos de ubicación compartidos por otros usuarios al usuario de esta cuenta. En ningún caso registra los datos compartidos por el usuario de esta cuenta hacia otros.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
jid	Identificador "lid" del contacto que ha compartido la ubicación.
latitude	Latitud geográfica del dispositivo.
longitude	Longitud geográfica del dispositivo.
accuracy	Precisión en metros de la posición facilitada por el dispositivo.
speed	Teóricamente registra la velocidad del dispositivo, pero en las pruebas realizadas carece de precisión, no siendo útil la información que aporta.
bearing	Teóricamente registra la dirección del movimiento en grados, pero en las pruebas realizadas carece de precisión, no siendo útil la información que aporta.
location_ts	Fecha en formato UTC Unix Epoch (milisegundos) en el que se ha compartido este punto de localización.

Ilustración 21. Descripción de los campos de la tabla "location_cache"

Ejemplo:

 _id	jid	latitude	longitude	accuracy	speed	bearing	 location_ts	Recovery info
 186	148846453755945@lid	28,1330762	-15,4368013	-1	-1	-1	05/10/2025 09:42:06	db: 8FC8-8FFF
 187	148846453755945@lid	28,13299	-15,436537	16	0,330000013113022	88	05/10/2025 09:42:47	wal: 5059-5097
 188	148846453755945@lid	28,121684	-15,4254751	16	0,330000013113022	88	06/10/2025 13:24:03	wal: 80A1-80DF
 189	148846453755945@lid	28,128947	-15,44145	0	-1	0	06/10/2025 13:36:04	wal: E13A-E16F
 190	222359768326203@lid	28,1296672821045	-15,4399566650391	-1	-1	-1	06/10/2025 17:32:05	wal: 1114A-11181
 191	222359768326203@lid	28,1213722229004	-15,4259042739868	-1	-1	-1	09/10/2025 08:14:26	wal: 171DA-17211
 192	148846453755945@lid	28,120755	-15,4256097	0	-1	0	09/10/2025 08:43:02	wal: 1D2A2-1D2D7

Ilustración 22. Tabla "location_cache"

4.5.2. location_sharer

Esta tabla puede contener un registro cuando se ha compartido la ubicación en tiempo real, con el usuario de esta cuenta o por él.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
remote_jid	Identificador "jid" del chat individual o grupal en el que se ha enviado la ubicación.
from_me	En el caso de que la transmisión la haya iniciado el usuario de esta cuenta, se registra con el valor "1". En caso contrario y sea el otro usuario quien comparta su ubicación el valor es "0".
remote_resource	Identificador "lid" del contacto que ha enviado o recibido la ubicación (es el contacto con el que se ha comunicado el usuario de esta cuenta).
expires	Es la fecha en formato UTC Unix Epoch (milisegundos) programada por el usuario para la finalización de la transmisión de la ubicación en tiempo real. Cuando el usuario de esta cuenta emite la ubicación (from_me = "1") puede forzar el cierre de la transmisión cuando lo desee, en cuyo caso se generará otro registro (con el mismo "message_id") con la fecha del cierre forzado de la comunicación y se borrará el registro previo con la fecha programada de cierre. Dependiendo del tiempo y uso de la aplicación, es posible recuperar el registro borrado con esta fecha.
message_id	Identificación del mensaje que se ha generado para la comunicación de la ubicación en tiempo real. Se corresponde con el campo "key_id", de la tabla "message" de la base de datos "msgstore.db".

Ilustración 23. Descripción de los campos de la tabla "location_sharer"

Ejemplo:

	_id	remote_jid	from_me	remote_resource	expires	message_id	Recovery info
15	346	@s.whatsapp.net	1	222359768326203@lid	04/10/2025 09:30:15	AC159892D9E7F44161402740D6C3C13	db: 3FA4-3FFF
19	120363422189343426@g.us	0	148846453755945@lid	05/10/2025 10:42:06	ACB97BF098C784FADD880C79D1E059D9	wal: F83-FD8	
20	120363422189343426@g.us	0	148846453755945@lid	06/10/2025 13:39:02	AC8C28F67C79D6916D077F738246ACSE	wal: A002-A05A	
21	346	@s.whatsapp.net	0	222359768326203@lid	07/10/2025 01:32:03	3AD2F96C8944C4C7475D	wal: 1308A-130D9
22	120363423174459161@g.us	0	222359768326203@lid	09/10/2025 16:14:22	3ADB1EBBE880471F6FFD	wal: 190CD-19119	
23	120363422189343426@g.us	0	148846453755945@lid	09/10/2025 08:58:02	ACAF410A87B46F62BACB16EDEF86267F	wal: 1F104-1F15C	
24	120363403584961735@g.us	0	222359768326203@lid	11/10/2025 10:08:16	3A2A5A2211B1F598F763	wal: 3146B-314B7	
13	346	@s.whatsapp.net	1	222359768326203@lid	29/09/2025 16:57:36	AC437A423C34B35E1D1F72D864A492C5	wal: 495E4-4963F
11	346	@s.whatsapp.net	1	222359768326203@lid	29/09/2025 16:48:32	ACE52D631E67115A4F18C0B02E6040A9	wal: 49640-49698

Ilustración 24. Tabla "location_sharer"

4.6. Base de datos *msgstore.db*

Es la base de datos que contiene la información de las comunicaciones transmitidas a través de WhatsApp (mensajes y llamadas/videollamadas). A continuación, se muestran las tablas de las que consta esta base de datos (muchas de ellas no están activas) en la versión 2.25.22.80 de la aplicación, y se expone el contenido de las tablas más significativas. Dependiendo del análisis que estemos realizando, es posible que tablas no descritas contengan información de interés.

- msgstore.db - DDL - addon_message_media - agent_chat_assignment - agent_devices - agent_message_attribution - ai_agentic_metadata - ai_rich_response_message_additional_info - ai_rich_response_message_core_info - android_metadata - audio_data - away_messages - backup_changes - bcall_session - bot_chat_info - bot_memory_metadata - bot_message_info - bot_message_prompts - bot_plugin_metadata - business_message_forward_info - call_link - call_log - call_log_participant_v2 - call_unknown_caller - chat - chat_ephemeral - community_chat - composition - composition_media - composition_mention - data_sharing_disclosure_metadata - deleted_chat_job - extended_media_data - favorite - forwarded_newsletter_message_info - frequent - frequent_forward_chat - gap_enforcement_business_chat_thread_info_cache - group_history_bundle - group_history_bundle_association - group_history_metadata - group_notification_version - group_participant_device - group_participant_label_metadata	- group_participant_user - group_past_participant_user - integrator_display_name - integrity_chat_info - invoice_transactions - jid - jid_map - jid_user_metadata - joinable_call_log - keywords - labeled_jid - labels - lid_chat_state - lid_display_name - media_hash_thumbnail - media_processed_video - media_refs - message - message_add_on - message_add_on_event_response - message_add_on_keep_in_chat - message_add_on_pin_in_chat - message_add_on_poll_vote - message_add_on_poll_vote_selected_option - message_add_on_question_response - message_add_on_reaction - message_add_on_receipt_device - message_add_on_scheduled_call_edit - message_add_on_status_question_answer - message_album - message_association - message_bcall_session - message_bot_feedback - message_broadcast_ephemeral - message_call_log - message_comment - message_comment_parent - message_details - message_edit_info - message_ephemeral - message_ephemeral_setting - message_ephemeral_sync_response - message_event - message_external_ad_content
--	---

- message_fixed_content_placeholder
- message_forwarded
- message_ftsv2
- message_ftsv2_content
- message_ftsv2_docsize
- message_ftsv2_segdir
- message_ftsv2_segments
- message_ftsv2_stat
- message_future
- message_group_invite
- message_invoice
- message_limit_sharing_setting
- message_link
- message_location
- message_logging_funnel_id
- message_media
- message_media_interactive_annotation
- message_media_interactive_annotation_embedded_music
- message_media_interactive_annotation_vertex
- message_media_map
- message_media_vcard_count
- message_mentions
- message_newsletter_admin_invite
- message_newsletter_fts
- message_newsletter_fts_content
- message_newsletter_fts_docsize
- message_newsletter_fts_segdir
- message_newsletter_fts_segments
- message_newsletter_fts_stat
- message_order
- message_orphan
- message_orphaned_edit
- message_parent_association
- message_payment
- message_payment_invite
- message_payment_status_update
- message_payment_transaction_reminder
- message_poll
- message_poll_option
- message_privacy_state
- message_product
- message_question
- message_quote_invoice
- message_quoted

- message_quoted_blank_reply
- message_quoted_call_log
- message_quoted_group_invite
- message_quoted_location
- message_quoted_media
- message_quoted_mentions
- message_quoted_order
- message_quoted_payment_invite
- message_quoted_product
- message_quoted_text
- message_quoted_ui_elements
- message_quoted_ui_elements_reply
- message_quoted_vcard
- message_rating
- message_revoked
- message_scheduled_call
- message_secret
- message_send_count
- message_span_indices
- message_status_psa_campaign
- message_sticker_pack
- message_sticker_pack_stickers
- message_streaming_sidecar
- message_system
- message_system_biz_callback_disabled
- message_system_biz_callback_enabled
- message_system_biz_per_customer_3pd_data_share_state
- message_system_block_contact
- message_system_business_broadcast
- message_system_business_state
- message_system_chat_assignment
- message_system_chat_participant
- message_system_community_link_changed
- message_system_detected_outcomes_labeled_chat
- message_system_device_change
- message_system_ephemeral_setting_not_applied
- message_system_event_updates
- message_system_group
- message_system_group_auto_restrict
- message_system_group_with_parent
- message_system_initial_privacy_provider
- message_system_lid_change
- message_system_linked_group_call
- message_system_number_change

Francisco Arenaz Benito
Bases de datos de Whatsapp (Android)

community_chat	message_add_on_poll_vote
composition	message_add_on_poll_vote_selected_option
composition_media	message_add_on_question_response
composition_mention	message_add_on_reaction
data_sharing_disclosure_metadata	message_add_on_receipt_device
deleted_chat_job	message_add_on_scheduled_call_edit
extended_media_data	message_add_on_status_question_answer
favorite	message_album
forwarded_newsletter_message_info	message_association
frequent	message_bcall_session
frequent_forward_chat	message_bot_feedback
frequents	message_broadcast_ephemeral
gap_enforcement_business_chat_thread_info_cache	message_call_log
group_history_bundle	message_comment
group_history_bundle_association	message_comment_parent
group_history_metadata	message_details
group_notification_version	message_edit_info
group_participant_device	message_ephemeral
group_participant_label_metadata	message_ephemeral_setting
group_participant_user	message_ephemeral_sync_response
group_past_participant_user	message_event
integrator_display_name	message_external_ad_content
integrity_chat_info	message_fixed_content_placeholder
invoice_transactions	message_forwarded
jid	message_ftsv2
jid_map	message_ftsv2_content
jid_user_metadata	message_ftsv2_docsize
joinable_call_log	message_ftsv2_segdir
keywords	message_ftsv2_segments
labeled_jid	message_ftsv2_stat
labels	message_future
lid_chat_state	message_group_invite
lid_display_name	message_invoice
media_hash_thumbnail	message_limit_sharing_setting
media_processed_video	message_link
media_refs	message_location
message	message_logging_funnel_id
message_add_on	message_media
message_add_on_event_response	message_media_interactive_annotation
message_add_on_keep_in_chat	message_media_interactive_annotation_embedded_music
message_add_on_orphan	message_media_interactive_annotation_vertex
message_add_on_pin_in_chat	message_media_map

-  message_media_vcard_count
-  message_mentions
-  message_newsletter_admin_invite
-  message_newsletter_fts
-  message_newsletter_fts_content
-  message_newsletter_fts_docsize
-  message_newsletter_fts_segdir
-  message_newsletter_fts_segments
-  message_newsletter_fts_stat
-  message_order
-  message_orphan
-  message_orphaned_edit
-  message_parent_association
-  message_payment
-  message_payment_invite
-  message_payment_status_update
-  message_payment_transaction_reminder
-  message_poll
-  message_poll_option
-  message_privacy_state
-  message_product
-  message_question
-  message_quote_invoice
-  message_quoted
-  message_quoted_blank_reply
-  message_quoted_call_log
-  message_quoted_group_invite
-  message_quoted_location
-  message_quoted_media
-  message_quoted_mentions
-  message_quoted_order
-  message_quoted_payment_invite
-  message_quoted_product
-  message_quoted_text
-  message_quoted_ui_elements
-  message_quoted_ui_elements_reply
-  message_quoted_vcard
-  message_rating
-  message_revoked
-  message_scheduled_call
-  message_secret
-  message_send_count

-  message_span_indices
-  message_status_psa_campaign
-  message_sticker_pack
-  message_sticker_pack_stickers
-  message_streaming_sidecar
-  message_system
-  message_system_biz_callback_disabled
-  message_system_biz_callback_enabled
-  message_system_biz_per_customer_3pd_data_share_state
-  message_system_block_contact
-  message_system_broadcast_list_entry_point
-  message_system_business_broadcast
-  message_system_business_state
-  message_system_chat_assignment
-  message_system_chat_participant
-  message_system_community_link_changed
-  message_system_detected_outcomes_labeled_chat
-  message_system_device_change
-  message_system_ephemeral_setting_not_applied
-  message_system_event_updates
-  message_system_group
-  message_system_group_auto_restrict
-  message_system_group_with_parent
-  message_system_initial_privacy_provider
-  message_system_lid_change
-  message_system_linked_group_call
-  message_system_number_change
-  message_system_opt_out
-  message_system_payment_invite_setup
-  message_system_photo_change
-  message_system_privacy
-  message_system_reminder_sent
-  message_system_reminder_setup
-  message_system_scheduled_call_start
-  message_system_sibling_group_link_change
-  message_system_username_change
-  message_system_value_change
-  message_system_with_group_nodes
-  message_template
-  message_template_button
-  message_template_quoted
-  message_text

 message_thumbnail	 quick_reply_usage
 message_translation_request	 receipt_device
 message_ui_elements	 receipt_orphaned
 message_ui_elements_reply	 receipt_user
 message_vcard	 reminder
 message_vcard_jid	 reporting_info
 message_view_once_media	 reporting_info_content
 messages_hydrated_four_row_template	 scheduled_calls
 missed_call_log_participant	 scheduled_reminder_message
 missed_call_logs	 smart_suggestions_key_value
 mms_metadata	 sqlite_sequence
 mms_thumbnail_metadata	 status
 newsletter	 status_attribution
 newsletter_linked_account	 status_crossposting
 newsletter_message	 status_crossposting_v3
 newsletter_message_enforcements	 status_info_ranking_signals
 newsletter_message_reaction	 status_message_info
 newsletter_my_reaction_orphan_message	 status_notification_info
 newsletter_subscribers	 status_quoted_message
 optimised_delivery_info	 suggest_as_you_type
 parent_group_participants	 suggested_replies
 pay_transaction	 support_citation_metadata
 payment_background	 tee_message_info_table
 payment_background_order	 template_messages_metadata
 payment_link_metadata	 thread_jid
 played_self_receipt	 thread_messages
 premium_message_info	 transcription_segment
 primary_device_version	 url_tracking_map_element
 priority_inbox	 user_device
 props	 user_device_info
 question_reply_quoted_message	 available_message_view
 quick_replies	 chat_view
 quick_reply_attachments	 deleted_messages_ids_view
 quick_reply_keywords	 deleted_messages_view

Ilustración 25. Tablas de la base de datos “msgstore.db”

4.6.1. backup_changes

Tabla que registra los cambios que se graban en la copia de seguridad. Esta tabla se añadió a la base de datos cuando se implementaron las copias de seguridad incrementales en la aplicación. Registra todas las eliminaciones ("DELETE") de mensajes de la tabla **"message"** que se ejecutarán en la copia de seguridad.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
operation	Operación que se ha producido en la correspondiente tabla de esta base de datos: DELETE : eliminación. INSERT : inserción. UPDATE : actualización o creación.
table_name	Nombre de la tabla de la base de datos en la que se ha producido la operación.
table_row_id	Número de registro o fila de la tabla en la que se ha producido la operación.

Ilustración 26. Descripción de los campos de la tabla "backup_changes"

4.6.2. bot_message_info

Tabla que registra las respuestas recibidas del bot de "META AI". Se desconoce si se han implementado otros bots cuyas respuestas sean registradas en esta tabla.

Campo	Descripción
message_row_id	Valor que se corresponde con el valor del campo "_id" de la tabla "message" , permitiendo determinar la contestación (texto) del bot.
target_id	Valor que se corresponde con el del identificador del mensaje "key_id" de la tabla "message" , en el que el usuario ha realizado la pregunta al bot y cuya respuesta es el mensaje del campo anterior.

Campo	Descripción
invoker_jid_row_id	Valor que permite la identificación del usuario o contacto que ha invocado al bot. El valor se corresponde con el campo “_id” de la tabla “jid”. El campo se encontrará vacío si el usuario de esta cuenta invoca a Meta AI en el chat de este asistente o en la búsqueda general.

Ilustración 27. Descripción de los campos de la tabla “bot_message_info”

4.6.3. call_link

Tabla que registra los enlaces o links compartidos para iniciar llamadas o videollamadas.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
token	Token compartido para iniciar la llamada o videollamada
creator_jid_row_id	Valor que permite la identificación del creador del enlace para iniciar la llamada o videollamada. El valor se corresponde con el campo “_id” de la tabla “jid”.

Ilustración 28. Descripción de los campos de la tabla “call_link”

4.6.4. call_log

Tabla que registra los datos de las llamadas y videollamadas.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
jid_row_id	Valor que relaciona la llamada con el identificador “jid” del contacto con el que se establece la comunicación. El valor se corresponde con el valor del campo “_id” de la tabla “jid”, posibilitando vincular ambas tablas.

Campo	Descripción
from_me	Si la llamada o videollamada la ha iniciado el usuario de esta cuenta se registra con el valor "1". En caso contrario, el valor es "0".
call_id	Identificador de la llamada (se corresponde con el campo "_id" de la tabla "message").
timestamp	Fecha de inicio de la comunicación en formato UTC Unix Epoch (milisegundos).
video_call	Si es una videollamada se registra con el valor "1". En caso de ser una llamada de voz, el valor es "0".
duration	Duración en segundos de la comunicación.
call_result	Resultado de la llamada: 2: llamada sin contestar. 4: llamada rechazada por todos los participantes. 5: llamada individual descolgada o llamada grupal (entrante o saliente) descolgada por al menos 1 participante. 8: el usuario se unió a un chat de audio en grupo.
bytes_transferred	Bytes transferidos en la comunicación.
group_jid_row_id	Valor que permite identificar el grupo de WhatsApp con el que se establece la comunicación. El valor se corresponde con el valor del campo "_id" de la tabla "jid". Si es una llamada individual el valor es "0".
call_creator_device_jid_row_id	Este valor se corresponde con el campo "_id" de la tabla "jid", que permite identificar el número de dispositivo que ha efectuado la llamada. En dicha tabla podremos identificar el número de dispositivo en los campos "device" y "raw_string".
call_link_row_id	Valor que permite identificar el enlace que ha iniciado la llamada, que se corresponde con el campo "_id" de la tabla "call_link".
call_type	Tipo de llamada: 0: llamada o videollamada en chat individual o grupal. 2: chat de audio en grupo.

Ilustración 29. Descripción de los campos de la tabla "call_log"

4.6.5. call_log_participant_v2

Tabla que registra los participantes en llamadas o videollamadas grupales. Por cada comunicación habrá tantas filas como participantes, presentando todos ellos el mismo valor del campo "**call_log_row_id**", e informando sobre la acción de cada uno, haya participado o no en la llamada o videollamada.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
call_log_row_id	Valor que permite identificar la videollamada/llamada y se corresponde con el campo " _id " de la tabla " call log ", posibilitando vincular ambas tablas.
jid_row_id	Valor que relaciona e identifica al contacto con la videollamada/llamada en la que ha participado. El valor se corresponde con el valor del campo " _id " de la tabla " jid ", permitiendo vincular ambas tablas.
call_result	Acción de cada participante en la llamada/videollamada grupal. En chats de audio, sólo registra los participantes que se han unido. 2 : el usuario o el participante ha rechazado la llamada o no ha descolgado la llamada. 5 : el usuario o el participante ha iniciado la llamada o ha descolgado una llamada entrante.

Ilustración 30. Descripción de los campos de la tabla "call_log_participant_v2"

4.6.6. chat

Tabla que registra los chats creados con los diferentes contactos, grupos, difusiones, comunidades o canales, hayan tenido comunicación o no.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).

Campo	Descripción
jid_row_id	Valor que relaciona el chat con el identificador "jid" del contacto/grupo/difusión/comunidad/canal con el que se establece la comunicación. El valor se corresponde con el valor del campo "_id" de la tabla "jid", permitiendo vincular ambas tablas.
hidden	Si es un chat visible u oculto en la aplicación: 0 : es visible (pestaña chat de la aplicación) 1 : no es visible (el contacto se encuentra en la agenda del teléfono, pero no se ha iniciado ningún chat a través de la aplicación o ha sido eliminado el chat) Los grupos y comunidades a los que se pertenece siempre son visibles (0). Los canales del usuario y a los que sigue siempre son no visibles (1).
subject	Asunto del grupo de chat, difusión, comunidad o canal (nombre que se le ha asignado). Si es el registro de un contacto, este campo se encontrará vacío.
created_timestamp	Fecha de creación del chat con contacto, grupo, comunidad, difusión o canal, en formato UTC Unix Epoch (milisegundos). En el caso de que el contacto estuviese grabado en la agenda del teléfono, pero no se haya iniciado un chat (hidden = 1), este campo estará vacío.
display_message_row_id	Último mensaje mostrado en el chat. El valor se corresponde con el campo "_id" de la tabla "message".
last_message_row_id	Último mensaje intercambiado en el chat. Generalmente es el mismo que el del campo anterior. El valor se corresponde con el campo "_id" de la tabla "message".
last_read_message_row_id	Último mensaje recibido en esta cuenta y leído. El valor se corresponde con el campo "_id" de la tabla "message".
last_read_receipt_sent_message_row_id	Último mensaje recibido en esta cuenta y que se ha confirmado su lectura al remitente del mensaje en el chat. En el caso de los chats individuales, si no hay confirmación de lectura en los dos usuarios, se registrará el último mensaje del sistema generado en el chat. El valor se corresponde con el campo "_id" de la tabla "message".
archived	Si el chat está archivado en la cuenta analizada consta con valor "1". En caso contrario el valor es "0".
sort_timestamp	Fecha del último mensaje que actualmente está registrado en el chat en formato UTC Unix Epoch (milisegundos).

Campo	Descripción
unseen_earliest_message_received_time	Fecha del primer mensaje recibido "no leído" en formato UTC Unix Epoch (milisegundos).
unseen_message_count	Número de mensajes "no leídos".
unseen_missed_calls_count	Número de llamadas perdidas "no leídas".
ephemeral_expiration	Tiempo en segundos de la duración de los mensajes temporales aplicados a este chat antes de eliminarse: "86400" , "604800" o "7776000" . Si los mensajes del chat <u>no</u> son temporales el valor es "0" .
ephemeral_setting_timestamp	Fecha en el que se ajustó la duración de los mensajes temporales en formato UTC Unix Epoch (segundos o milisegundos según el caso). Si no se ha aplicado esta opción el valor es "0" .
group_type	Tipo de agrupación: 0 : contactos, grupos y difusiones. 1 : comunidades. 2 : grupos que forman parte de una comunidad. 3 : grupos "Avisos" de las comunidades. 4 : canales. 6 : grupos "General" de las comunidades.
participation_status	Relación de la participación del usuario de esta cuenta en el chat: Vacío : canales, difusiones y algún chat individual. 0 : chats individuales con el usuario de esta cuenta. 1 : el usuario de esta cuenta ya no forma parte del grupo o comunidad. 2 : el usuario de esta cuenta no es administrador del grupo. 3 : el usuario de esta cuenta ha sido nombrado administrador de un grupo. 4 : el usuario de esta cuenta es administrador porque es el creador del grupo o la comunidad.
chat_lock	Si se ha aplicado la opción de "Bloqueo" de chats el valor es "1" . En caso contrario el valor es "0" .

Ilustración 31. Descripción de los campos de la tabla "chat"

4.6.7. chat_ephemeral

Tabla que registra los chats que tienen o han tenido asignado temporalidad a sus mensajes.

Campo	Descripción
chat_row_id	Identificación del chat en el que se ha aplicado temporalidad a los mensajes. Este valor se corresponde con el valor del campo "_id" de la tabla "chat", permitiendo vincular ambas tablas.
ephemeral_trigger	Motivo por el que se ha activado los mensajes temporales en el chat: 0: en un chat grupal se ha asignado temporalidad a los mensajes. 1: se ha establecido manualmente la temporalidad de los mensajes por uno de los participantes (el usuario de esta cuenta o el contacto con el que mantiene la conversación) en un chat individual activo. 2: se ha iniciado un chat individual y al menos uno de los participantes del chat (el usuario de esta cuenta o el contacto con el que mantiene la conversación) tiene predeterminada la temporalidad de los mensajes cuando se crea el chat.
ephemeral_initiated_by_me	Quién ha establecido la temporalidad a los mensajes en el chat individual: 0: un contacto. 1: el usuario de esta cuenta. Este campo se encontrará vacío en los chats grupales.

Ilustración 32. Descripción de los campos de la tabla "chat_ephemeral"

4.6.8. group_participant_device

Tabla que registra la identificación de los dispositivos utilizados por los contactos integrantes en grupos de los que forma parte el usuario de esta cuenta.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
group_participant_row_id	Este valor se corresponde con el campo " _id " de la tabla " group_participant_user " y relaciona a un usuario/contacto con un grupo concreto.
device_jid_row_id	Este valor se corresponde con el campo " _id " de la tabla " jid ", que permite identificar el número de dispositivo que ha enviado el mensaje. En dicha tabla se puede identificar el número de dispositivo en los campos " device " y " raw_string ".

Ilustración 33. Descripción de los campos de la tabla "group_participant_device"

4.6.9. group_participant_user

Tabla que registra los grupos y sus integrantes.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
group_jid_row_id	Valor a partir del cual se puede localizar el identificador "jid" o "lid" del grupo. El registro se corresponde con el campo " _id " de la tabla " jid ", permitiendo vincular ambas tablas.
user_jid_row_id	Valor a partir del cual se puede localizar el identificador "jid" del usuario o contacto. El registro se corresponde con el campo " _id " de la tabla " jid ", permitiendo vincular ambas tablas.
rank	Cuando el participante es el creador y administrador del Grupo o Comunidad se registra con el valor " 2 ". Si el administrador amplía y designa a más administradores, éstos se registran con el valor " 1 ". En caso de no ser administrador el valor es " 0 ".
add_timestamp	Fecha en la se añadió al miembro en el grupo en formato UTC Unix Epoch (milisegundos).

Ilustración 34. Descripción de los campos de la tabla "group_participant_user"

4.6.10. group_past_participant_user

Tabla que registra los participantes que han abandonado o han sido expulsados de grupos.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
group_jid_row_id	Valor a partir del cual se puede determinar el identificador "jid" del grupo al que pertenecía el contacto/usuario. El valor se corresponde con el valor del campo " _id " de la tabla " jid ".
user_jid_row_id	Valor a partir del cual se puede determinar el identificador "jid" del contacto/usuario perteneciente al grupo indicado en el anterior campo. Este valor se corresponde con el valor del campo " _id " de la tabla " jid ".
is_leave	Si el contacto/usuario dejó voluntariamente el grupo el valor es " 1 ". En caso de que un administrador lo expulsara, el valor es " 0 ".
timestamp	Fecha del abandono/expulsión el grupo en formato UTC Unix Epoch (milisegundos).

Ilustración 35. Descripción de los campos de la tabla "group_past_participant_user"

4.6.11. jid

Tabla que registra los identificadores "jid" (Jabber Identifier) del usuario de esta cuenta y sus dispositivos vinculados, sus contactos y dispositivos vinculados (con los que hayan intercambiado mensajes con el usuario), grupos, difusiones, comunidades y canales.

Conectándola con la tabla "**chat**" de esta base de datos y con la tabla "**wa_contacts**" de la base de datos "**wa.db**", permite identificar los chats con los nº de teléfonos y los nombres con los que están grabados en la agenda de contactos de este dispositivo.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite). Su número se corresponde con el campo " jid_row_id " de la tabla " chat ", permitiendo vincular ambas tablas.
user	Número de usuario codificado con el "prefijo internacional + nº de teléfono del usuario". Ejemplo: 34646222111. Si es un grupo, comunidad, canal o difusión, será el número de identificador de éstos.
server	Servidor que gestiona la comunicación. En individuos el valor es "s.whatsapp.net" o "lid", en grupos o comunidades "g.us", en difusiones es "broadcast", en canales "newsletter" y en bots como Meta AI es "bot".
device	Número de dispositivo registrado en WhatsApp del usuario o de sus contactos. Un mismo usuario o contacto puede tener varios dispositivos registrados, tantos como vinculaciones haya efectuado con su cuenta.
type	Tipo: 0: Registro de identificadores "jid" del usuario o contactos (servidor s.whatsapp.net). 1: Registro de identificadores "jid" de grupos (servidor g.us). 2: (servidor temp). 3: Registro de difusión (servidor broadcast). 5: Registro de difusión de estado (servidor broadcast). 7: (servidor s.whatsapp.net). 11: Registro del usuario de esta cuenta (servidor status_me y lid_me). 17: Registro de identificadores "jid" de dispositivos del usuario o contactos (servidor s.whatsapp.net). 18: Registro de identificadores "lid" del usuario y contactos (servidor lid). 19: Registro de identificadores "lid" de dispositivos del usuario o contactos (servidor lid). 21: Registro de identificadores "jid" de canales (servidor newsletter). 26: Registro de identificador "bot" (En las pruebas solo se ha detectado servidor bot de "Meta AI"). 27: Registro de identificador de dispositivo "bot" (En las pruebas solo se ha detectado el del servidor bot de "Meta AI").

Campo	Descripción
raw_string	Registra el identificador "jid" (Jabber ID) de usuario, contactos, grupos, difusiones y canales, así como los identificadores "lid" del usuario y contactos. Ejemplos: 34646222111@s.whatsapp.net ("jid" de contacto). 34699888777-1379114707@g.us ("jid" de grupo en formato antiguo). 120363080564732172@g.us ("jid" de grupo en formato actual o comunidad). 1690524142@broadcast ("jid" de difusión). 120363165396843331@newsletter ("jid" de canal). 262074978558186@lid ("lid" de contacto). Cuando un usuario utiliza un dispositivo (principal o vinculado a su cuenta de WhatsApp), se registrará en esta tabla el identificador "jid" del dispositivo, constando el campo "type" = "17" y al identificador "jid" del usuario/contacto se le añadirá ".0:", seguido de otro dígito que será el mismo valor que el del campo "device", y que irá incrementando secuencialmente a medida que se vinculen nuevos dispositivos. Cada vez que un dispositivo se vincula a una cuenta de WhatsApp, el valor del campo "device" incrementa en una unidad, siendo "device" = "0" el dispositivo principal en uso, el resto serán dispositivos vinculados que incrementan en una unidad cada vez que se vincula uno nuevo. Ejemplos: 34646222111.0:0@s.whatsapp.net el campo device será "0" (dispositivo principal). 34646222111.0:4@s.whatsapp.net el campo device será "4". 34646222111.0:31@s.whatsapp.net el campo device será "31". El identificador "lid" de los dispositivos del usuario y sus contactos seguirá el mismo patrón que el identificador "jid", con la diferencia de que se le añadirá a la numeración ".1:" en vez de ".0:", y el valor del campo "type" = "19". Ejemplos: 262074978558186.1:0@lid el campo device será "0" (dispositivo principal). 262074978558186.1:4@lid el campo device será "4".

Ilustración 36. Descripción de los campos de la tabla "jid"

4.6.12 jid_map

Tabla que registra la vinculación entre los identificadores "jid" (Jabber Identifier) de los contactos con sus identificadores "lid". Hay que señalar que el identificador "jid" está compuesto a partir del número de teléfono del contacto, y el identificador "lid" tiene la finalidad de proteger la privacidad del participante, estando formado por 15 dígitos asignados por la aplicación, evitando facilitar información sobre el contacto. Aunque esta tabla vincule los dos tipos de identificadores, en la interfaz gráfica de la aplicación en el dispositivo no es posible ver el identificador "lid". Los grupos, difusiones, comunidades o canales carecen de este tipo de identificador "lid".

Campo	Descripción
lid_row_id	Valor que permite localizar el identificador "lid" del contacto o usuario. Este valor se corresponde con el valor del campo "_id" de la tabla "jid".
jid_row_id	Valor que permite localizar el identificador "jid" del contacto o usuario. Este valor se corresponde con el valor del campo "_id" de la tabla "jid".

Ilustración 37. Descripción de los campos de la tabla "jid_map"

4.6.13. labeled_jid

Tabla que registra los chats incluidos en las diferentes listas que dispone el usuario para organizar las conversaciones. Esta tabla debe ser analizada en unión con la tabla "labels".

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
label_id	Valor que permite determinar el identificador "_id" de la lista. Este valor se corresponde con el del campo "_id" de la tabla "labels", posibilitando vincular ambas tablas.
jid_row_id	Valor que permite determinar el identificador "jid" del contacto incluido en la lista. Este valor se corresponde con el del campo "_id" de la tabla "jid", posibilitando vincular ambas tablas.

Ilustración 38. Descripción de los campos de la tabla "labeled_jid"

4.6.14. labels

Tabla que registra las diferentes listas que dispone el usuario de esta cuenta para organizar sus chats. La aplicación incluye de forma predefinida varias listas, pudiendo el usuario añadir listas personalizadas.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
label_name	Nombre de la lista. Las listas "No leídos", "Favoritos" y "Grupos" se encuentran por defecto en la aplicación.
sort_id	Valor que indica el orden (de izquierda a derecha) en el que se muestra la lista en la interfaz gráfica de la aplicación.

Ilustración 39. Descripción de los campos de la tabla "labels"

4.6.15. lid_display_name

Tabla que registra y vincula, los participantes en las comunicaciones que no son contactos del usuario de esta cuenta. Almacena las últimas dos cifras del teléfono del participante en WhatsApp con su identificador "lid". Por ejemplo, este tipo de participante que no es contacto del usuario se puede presentar en comunicaciones de comunidades.

Campo	Descripción
lid_row_id	Valor que permite localizar el identificador "lid" del contacto. Este valor se corresponde con el del campo " _id " de la tabla " jid ", posibilitando vincular ambas tablas.
display_name	Información parcial del participante, compuesto por el prefijo internacional y las dos últimas cifras de su número de teléfono.

Ilustración 40. Descripción de los campos de la tabla "lid_display_name"

4.6.16 media_refs

Tabla que registra los archivos que se han transmitido en más de una ocasión (enviados y/o recibidos). En las pruebas realizadas, se ha observado el registro de stickers con numerosas copias transmitidas y que realmente no han sido enviados, pero la información que registra del resto de tipo de archivos (imágenes, vídeos, documentos...) es fiable.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
display_namepath	Ruta en el sistema de archivos del dispositivo en el que se encuentra almacenado el archivo.
ref_count	Número de copias del archivo que se han transmitido (enviado o recibido). La primera vez que se transmite un archivo no se contabiliza, por lo tanto, el número total es = ref_count + 1.

Ilustración 41. Descripción de los campos de la tabla "media_refs"

4.6.17. message

Esta tabla es la columna vertebral de la aplicación. Contiene información esencial de los mensajes enviados, recibidos y mensajes del sistema, como son fechas de transmisión, contenido del texto, tipo de mensaje (texto, audio, archivo de vídeo, encuesta...), tipo de dispositivo que ha emitido el mensaje, etc.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite). Es un número que autoincrementa en una unidad por cada mensaje recibido o enviado a través de la aplicación.
chat_row_id	Valor que permite la identificación del chat al que pertenece la conversación. Este valor se corresponde con el del campo " _id " de la tabla " chat ", posibilitando vincular ambas tablas.

Campo	Descripción
from_me	Dirección del mensaje: 0: mensaje recibido por el usuario de esta cuenta. 1: mensaje enviado por el usuario de esta cuenta. Los mensajes del sistema (message_type = "7") son una excepción, ya que todos tendrán siempre el valor igual a "1", independientemente del motivo de su generación.
key_id	El identificador del mensaje, que es una secuencia que varía desde 9 y 32 caracteres hexadecimales. Se puede identificar el tipo de dispositivo que envió un mensaje dependiendo del número de caracteres y/o los caracteres por los que empiece el identificador: 9-10 dígitos: En algunos mensajes del sistema en chats de grupo o comunidades se presentan con una longitud de 9 o 10 dígitos. (En el estudio no se ha podido dilucidar en qué casos concretos se dan unos u otros). 18 caracteres hexadecimales: <u>se envió</u> el mensaje a través de la versión de la aplicación para Windows o Wear OS. 20 caracteres hexadecimales, empezando por la secuencia: 3EBO <u>se envió</u> el mensaje a través de la versión WEB. 3A <u>se envió</u> el mensaje a través de versión de la aplicación para iOS, iPadOS o la versión para macOS. 5E <u>se envió</u> el mensaje a través de versión de la aplicación para iOS. 30 o 32 caracteres hexadecimales: <u>se envió</u> el mensaje a través de la versión para dispositivos Android.
sender_jid_row_id	Valor que permite localizar el identificador "jid" del emisor del mensaje. Este valor se corresponde con el del campo "_id" de la tabla "jid". Si el mensaje es enviado por el usuario del dispositivo en chats individuales o difusiones el valor es "0".

Campo	Descripción
status	Estado de la entrega/recepción en el que se encuentra el mensaje (<i>ver apartado 8.3.1 Mensajes enviados y recibidos (Android)</i>). 6: Mensaje del sistema. <u>Mensajes enviados:</u> 0 - 1: mensaje enviado no ha salido del teléfono (falta de conexión). 4: mensaje ha llegado al servidor. 5: mensaje entregado a su destinatario. 13: mensaje abierto en el chat del contacto. 8: nota de voz/vídeo o mensaje de visualización única reproducido por el contacto. <u>Mensajes recibidos:</u> 0: mensaje recibido en el dispositivo principal (todo tipo de mensaje). 9: nota de voz o mensaje de visualización única recibido y reproducido por el usuario de esta cuenta. (sin conexión a red). 10: nota de voz/vídeo o mensaje de visualización única recibido y reproducido por el usuario de esta cuenta. (con conexión a red). 17: Mensaje recibido y abierto con un dispositivo vinculado (si posteriormente se abre con el dispositivo principal no cambia el status).
broadcast	Mensaje enviado en una difusión: 0: no. 1: sí.
recipient_count	Número de contactos que han recibido el mensaje (en chats grupales, comunidades o difusiones).
participant_hash	Contiene un valor cuando el usuario ha publicado un mensaje (texto, audio, imagen...) en su estado para compartirlo con otros contactos durante 24 horas, si no se encuentra vacío.

Campo	Descripción
origination_flags	Bandera del mensaje. Las pruebas realizadas sugieren que la numeración hace referencia a los tipos y características de los mensajes. Los tipos de banderas que se describen son los más frecuentes. Como aclaración a la información presentada más adelante, la aplicación considera un mensaje reenviado cuando el emisor lo ha recibido previamente de otro contacto, y no cuando un usuario envía varias veces su propio mensaje. 0: mensaje sin temporalidad (incluidos algunos mensajes del sistema). 1: mensaje reenviado sin temporalidad. 64: el usuario de esta cuenta ha enviado un archivo de imagen a múltiples contactos a la vez y concretamente este archivo es transmitido a un chat sin temporalidad. 65: el usuario de esta cuenta ha reenviado un archivo de imagen a múltiples contactos a la vez y concretamente este archivo es transmitido a un chat sin temporalidad. 256: mensaje temporal. 257: mensaje temporal reenviado. 320: el usuario de esta cuenta ha enviado un archivo de imagen a múltiples contactos a la vez y concretamente este archivo es transmitido a un chat con temporalidad. 321: el usuario de esta cuenta ha reenviado un archivo de imagen a múltiples contactos a la vez y concretamente este archivo es transmitido a un chat con temporalidad. 512: mensajes del sistema. 2048: documento pdf, mensaje con un enlace a una URL, en un chat sin temporalidad. Video o gif publicado por el usuario o un contacto en su respectivo estado. 2049: documento pdf reenviado, mensaje reenviado con un enlace a una URL, en un chat sin temporalidad. 2304: documento pdf, mensaje con un enlace a una URL o enlace de invitación a un canal, en un chat con temporalidad. 2305: documento pdf reenviado, mensaje reenviado con enlace a una URL, en un chat con temporalidad. 32768: nota de voz, en chat sin temporalidad. 32769: nota de voz reenviado, en un chat sin temporalidad. 33024: nota de voz, en un chat con temporalidad. 33025: nota de voz reenviada, en un chat con temporalidad. 131072: mensaje editado en un chat sin temporalidad o mensaje recibido del bot de "Meta AI". 131328: mensaje editado, en un chat con temporalidad. 67108864: álbum multimedia compartido en un chat sin temporalidad. 67109120: álbum multimedia compartido en un chat con temporalidad. 537001984: evento creado por el usuario de esta cuenta y editado en un chat sin temporalidad. 537002240: evento creado por el usuario de esta cuenta y editado en un chat con temporalidad.

Campo	Descripción
origin	Origen del archivo transmitido: 0: restos de casos. 1: notas de voz o notas de voz de visualización única generados por medio de la aplicación, tanto enviadas como recibidas ("message_type" = "2" (algunos) y "82"). 2: archivos enviados por el usuario que han sido adjuntados a través de la propia aplicación de WhatsApp (icono del clip); imagen, vídeo, y sus versiones de visualización única ("message_type" = "1", "3", "42" y "43"). 3: mensajes reenviados por el usuario: imagen, audio, vídeo, tarjeta de contacto, ubicación estática, documento, gif y sticker/avatar ("message_type" = "0", "1", "2", "3", "4", "5", "9", "13" y "20"). 12: archivos adjuntados por el usuario a través de una 3ª aplicación (explorador de archivos del teléfono, navegador web, aplicación de almacenamiento en la nube...): imagen, vídeo, sus versiones de visualización única y gif ("message_type" = "1", "3", "13", "42" y "43"). 20: texto publicado en "Mi estado" del usuario de esta cuenta ("message_type" = "0"). 21: imagen, vídeo o gif publicado en "Mi estado" del usuario de esta cuenta ("message_type" = "1", "3" y "13"). 28: imagen generada a través de la aplicación WhatsApp publicada en "Mi estado" del usuario de esta cuenta. ("message_type" = "1"). 29: mensajes enviados de tipo imagen, vídeo, sus versiones de visualización única, gif y notas de vídeo ("message_type" = "1", "3", "13", "42", "43" Y "81") generados a través de la cámara de la aplicación WhatsApp.
timestamp	Fecha inicio del envío del mensaje desde este dispositivo (mensajes enviados) o del envío desde el dispositivo del contacto (mensajes recibidos) en formato UTC Unix Epoch (milisegundos).
received_timestamp	Fecha de salida del mensaje del dispositivo tras el procesamiento del envío (mensajes enviados) o fecha de recepción del mensaje (mensajes recibidos) en formato UTC Unix Epoch (milisegundos). El valor es "0" en mensajes enviados de texto, tarjetas de contacto, encuestas, registros de llamada saliente, mensajes de cambio de temporalidad o mensajes del sistema.

Campo	Descripción
receipt_server_timestamp	Fecha de la recepción del mensaje en el servidor en formato UTC Unix Epoch (milisegundos) cuando el mensaje se ha enviado desde este dispositivo. Si se trata de un envío desde otro dispositivo vinculado a esta cuenta, un mensaje del sistema o un mensaje recibido el valor será "-1".
message_type	Tipo de mensaje: 0: mensaje de texto y/o emoji. 1: imagen. 2: audio (archivo) o nota de voz. 3: vídeo (archivo) 4: tarjeta de contacto. 5: ubicación actual o lugares cercanos (ubicación estática). 7: mensaje del sistema (chat creado, usuario añadido, xxx cambió el icono de este grupo, xxx cambió el asunto de este grupo, etc.). 9: documento (archivo). 10: se desconoce su significado. En las pruebas realizadas, se ha observado que lo registra el sistema tras recibir una llamada/videollamada individual y no contestar (siempre que sea perdida, no rechazada). 13: gif. 15: mensaje borrado por el remitente para todos sus destinatarios. 16: ubicación en tiempo real. 20: sticker o avatar. 28: mensaje de la cuenta oficial de WhatsApp con información de novedades de la aplicación. 36: activación/desactivación de mensajes temporales de forma manual (no predeterminado) en chats individuales. 42: imagen de visualización única. 43: vídeo de visualización única. 64: mensaje de grupo borrado para todos los participantes por un administrador (que no fue quien envió el mensaje). 66: encuesta. 81: nota de vídeo. 82: nota de voz de visualización única. 88: feedback (positivo o negativo del desempeño del bot de Meta AI, enviado por el usuario). 90: llamada o videollamada, siempre que no se haya generado a través un enlace o link de llamada. 92: evento. 94: invitación para ser administrador de un canal. 99: álbum multimedia (mensaje con varios archivos de imagen y/o vídeo). 103: mención de un contacto en el "Estado" del usuario de esta cuenta o viceversa. 112: mensaje del sistema por la activación o desactivación de la privacidad avanzada del chat por un participante. La información se complementa con los datos de la tabla "message_limit_sharing_setting".

Campo	Descripción
text_data	Texto del mensaje (en mensajes de texto o de otro tipo al que se le ha añadido texto). Nombre del contacto cuando se transmite una tarjeta de contacto. En mensajes del sistema: nombre del grupo, difusión o comunidad cuando se crea, descripción del grupo o comunidad... En eventos, el nombre del evento.
starred	Mensaje seleccionado por el usuario como destacado cuando su valor es "1", en caso contrario su valor es "0". Permite una búsqueda directa de estos mensajes desde el menú principal de la aplicación.

Ilustración 42. Descripción de los campos de la tabla "message"

4.6.18. message_add_on

Tabla que registra la información de las características añadidas sobre determinados mensajes, como pueden ser reacciones a mensajes, fijar mensajes en chats o datos sobre las encuestas.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
chat_row_id	Valor que permite la identificación del chat al que pertenece el mensaje. Este valor se corresponde con el valor del campo "_id" de la tabla "chat", posibilitando vincular ambas tablas.
from_me	Indica quién ha realizado el añadido al mensaje: 0: Un contacto. 1: El usuario de esta cuenta.
key_id	Identificador del mensaje de la propia característica. El valor no se corresponde con el valor del campo "key_id" de la tabla "message" del mensaje al que se le ha añadido la característica.

Campo	Descripción
sender_jid_row_id	Valor que permite determinar el identificador "jid" del contacto que ha añadido la característica cuando pertenece a un chat grupal o comunidad, y no lo ha añadido el usuario de esta cuenta. Este valor se corresponde con el valor del campo " _id " de la tabla " jid ", posibilitando vincular ambas tablas. Si la característica la ha añadido el usuario de esta cuenta ("from_me" = "1") o un contacto lo ha añadido en un chat individual el valor será -1 .
parent_message_row_id	Valor que permite identificar el mensaje al que se la ha añadido la característica. Este valor se corresponde con el valor del campo " _id " de la tabla " message ".
timestamp	Fecha en la se ha añadido la característica al mensaje en formato UTC Unix Epoch (milisegundos).
message_add_on_type	Tipo de característica añadida al mensaje: 56 : reacción a un mensaje. 67 : votación en encuesta. 68 : se mantiene el mensaje temporal en el chat cuando se cumpla la fecha de eliminación. 74 : mensaje editado. 79 : se ha "fijado" el mensaje en el chat. 93 : evento.
received_timestamp	Fecha en la se ha recibido (from_me = "0") la característica del mensaje en formato UTC Unix Epoch (milisegundos). Este campo se registra en los tipos (message_add_on_type) con valores " 56 ", " 67 ", " 68 " y " 93 ".
expiry_duration_in_secs	Tiempo en segundos que se mantendrán fijados los mensajes en su correspondiente chat. Este campo se registra en los tipos (message_add_on_type) con valor " 79 ". Las opciones disponibles son 86400 (24 horas), 604800 (7 días) o 2292000 (30 días).
server_timestamp	Fecha de la recepción de la característica añadida del mensaje en el servidor en formato UTC Unix Epoch (milisegundos). Este campo se registra en todos los tipos (message_add_on_type) excepto con valor " 74 ".
expiry_timestamp	Fecha en formato UTC Unix Epoch (milisegundos) en la que dejará de estar "fijado" el mensaje en su correspondiente chat. Sólo registra valores para los tipos (message_add_on_type) con valor " 79 ".

*Ilustración 43. Descripción de los campos de la tabla "**message_add_on**"*

4.6.19. message_add_on_event_response

Tabla que registra la respuesta de los participantes de un chat a un evento.

Campo	Descripción
message_add_on_row_id	Valor que permite identificar el mensaje al que se la ha añadido la característica (respuesta a un evento). Este valor se corresponde con el campo " _id " de la tabla " message_add_on ", posibilitando vincular ambas tablas.
response	Respuesta del participante en el chat a la propuesta del evento: 1 : asistiré o asistiré con invitado (dependiendo del campo " extra_guest_count "). 2 : no asistiré. 3 : tal vez.
sender_timestamp	Fecha en la que el participante en el chat respondió a la propuesta del evento en formato UTC Unix Epoch (milisegundos).
extra_guest_count	0 : no hay invitado. 1 : asistirá con invitado. Cuando la respuesta del asistente es "asistiré con invitado".

Ilustración 44. Descripción de los campos de la tabla "message_add_on_event_response"

4.6.20. message_add_on_keep_in_chat

Tabla que registra la información de los mensajes temporales a los que se les ha añadido la característica de mantenerse en el chat una vez cumplida la fecha de eliminación.

Campo	Descripción
message_add_on_row_id	Valor que permite identificar el mensaje al que se la ha añadido la característica (mantenerse en el chat). El valor se corresponde con el campo " _id " de la tabla " message_add_on ", posibilitando vincular ambas tablas.

Campo	Descripción
keep_in_chat_state	Estado en el que se encuentra la característica que mantiene el mensaje en el chat: 0 : desactivado, el mensaje será eliminado cuando se cumpla la temporalidad que se le asignó. Para poder tener el valor "0", en algún momento anterior ha debido presentar el valor "1". 1 : activado. El mensaje temporal se mantiene en el chat.
sender_timestamp	Fecha en la que se activó o desactivó la característica añadida (mantenerse en el chat) al mensaje en formato UTC Unix Epoch (milisegundos).
keep_count	Número de veces que se ha conservado el mensaje. Si el valor es mayor de "1", el mensaje previamente ha tenido que dejar de estar conservado, para poder volver a estar conservado.
actor_device_jid_row_id	En las pruebas realizadas siempre toma el valor "-1".

Ilustración 45. Descripción de los campos de la tabla "message_add_on_keep_in_chat"

4.6.21. message_add_on_pin_in_chat

Tabla que registra la información de los mensajes que han sido fijados en su correspondiente chat.

Campo	Descripción
message_add_on_row_id	Valor que permite identificar el mensaje al que se le ha añadido la característica ("fijar" en el chat). Dicho valor se corresponde con el valor del campo "_id" de la tabla "message_add_on", posibilitando vincular ambas tablas.
pin_in_chat_state	Estado en el que se encuentra la característica "fijar" el mensaje en el chat: 0 : desactivado, el mensaje no se encuentra fijado en el chat. Para poder presentar el valor "0", en algún momento anterior ha debido tener el valor "1". 1 : activado. El mensaje está fijado en el chat.

Campo	Descripción
sender_times-tamp	Fecha en la que se activó o desactivó la característica añadida ("fijar" mensaje en el chat) en formato UTC Unix Epoch (milisegundos).

Ilustración 46. Descripción de los campos de la tabla "message_add_on_pin_in_chat"

4.6.22. message_add_on_poll_vote

Tabla que registra las fechas en las que el usuario o los contactos han realizado votaciones en las encuestas en las que han participado.

Campo	Descripción
message_add_on_row_id	Valor que permite identificar el mensaje al que se la ha añadido la característica (se ha votado). Dicho valor se corresponde con el valor del campo "_id" de la tabla "message_add_on", posibilitando vincular ambas tablas.
sender_times-tamp	Fecha en la que se aplicó la característica añadida (se votó en la encuesta) en formato UTC Unix Epoch (milisegundos). En caso de que el usuario o contacto haya votado en más de una ocasión, será la última.

Ilustración 47. Descripción de los campos de la tabla "message_add_on_poll_vote"

4.6.23. message_add_on_poll_vote_selected_option

Tabla que registra las opciones elegidas (votaciones) por los distintos contactos o el propio usuario en las encuestas en las que han participado. Si la encuesta se ha generado con la posibilidad de que los usuarios puedan elegir más de una opción, por cada elección que seleccione un usuario se generará una fila, pero con el mismo valor en el campo "message_add_on_row_id".

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
message_add_on_row_id	Valor que permite identificar el mensaje al que se le ha añadido la característica (se ha votado). Dicho valor se corresponde con el valor del campo " _id " de la tabla " message_add_on ", posibilitando vincular ambas tablas.
message_poll_option_id	Valor que permite identificar la opción seleccionada en la votación. Dicho valor se corresponde con el campo " _id " de la tabla " message_poll_option ", posibilitando vincular ambas tablas.

*Ilustración 48. Descripción de los campos de la tabla "**message_add_on_poll_vote_selected_option**"*

4.6.24. message_add_on_reaction

Tabla que registra la información de los mensajes a los que algún contacto o el usuario les ha añadido un emoji como reacción al mensaje.

Campo	Descripción
message_add_on_row_id	Valor que permite identificar el mensaje al que se le ha añadido la característica (reacción con un emoji). Dicho valor se corresponde con el valor del campo " _id " de la tabla " message_add_on ", posibilitando vincular ambas tablas.
reaction	Emoji añadido como reacción a un mensaje.
sender_times-tamp	Fecha de envío de la característica añadida (reacción a un mensaje) en formato UTC Unix Epoch (milisegundos).

*Ilustración 49. Descripción de los campos de la tabla "**message_add_on_reaction**"*

4.6.25. message_add_on_receipt_device

Tabla que registra la información de los dispositivos que han recibido los mensajes a los que ha añadido alguna característica desde esta

cuenta, como pueden ser reacciones a mensajes, fijar mensajes en chats o encuestas. También registra la recepción en los dispositivos vinculados, incluso los vinculados del usuario de esta cuenta.

Campo	Descripción
receipt_device_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
message_add_on_row_id	Valor que permite identificar el mensaje al que se la ha añadido la característica. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message_add_on ", posibilitando vincular ambas tablas.
receipt_device_jid_row_id	Este valor se corresponde con el campo " _id " de la tabla " jid ", que permite identificar el número de dispositivo que ha recibido la característica añadida al mensaje. En dicha tabla podremos identificar el número de dispositivo en los campos " device " y " raw_string ".
receipt_device_timestamp	Fecha de la recepción de la característica añadida del mensaje en el dispositivo identificado en el campo anterior en formato UTC Unix Epoch (milisegundos).

*Ilustración 50. Descripción de los campos de la tabla "**message_add_on_receipt_device**"*

4.6.26. message_album

Tabla que registra la información la transmisión de álbumes, es decir varios archivos multimedia (imágenes y/o vídeos) en un único envío.

Campo	Descripción
message_row_id	Valor que se corresponde con el valor del campo " _id " de la tabla " message ", permitiendo identificar el mensaje del sistema que informa del envío de múltiples archivos multimedia de una sola vez.
image_count	Número de imágenes adjuntadas en el álbum.
video_count	Número de vídeos adjuntados en el álbum.

*Ilustración 51. Descripción de los campos de la tabla "**message_album**"*

4.6.27. message_association

Tabla que registra la información de los archivos multimedia que han sido enviados agrupados en un álbum. Se genera un registro por cada uno de los archivos enviados en una agrupación, compartiendo el mismo valor del campo "**parent_message_row_id**" todos los archivos que se han enviado juntos.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
child_message_row_id	Valor que se corresponde con el valor del campo " _id " de la tabla " message ", permitiendo identificar el mensaje de uno de los archivos transmitidos.
parent_message_row_id	Valor que se corresponde con el valor del campo " _id " de la tabla " message ", permitiendo identificar el mensaje del sistema que informa de la transmisión de un álbum.

Ilustración 52. Descripción de los campos de la tabla "message_association"

4.6.28. message_call_log

Tabla que registra la información sobre las llamadas/videollamadas realizadas a través de la aplicación. La función de esta tabla es la de vincular la tabla "**message**" con la tabla "**call_log**".

Campo	Descripción
message_row_id	Valor que se corresponde con el valor del campo " _id " de la tabla " message ".
call_log_row_id	Valor que identifica la llamada efectuada. El valor que se corresponde con el valor del campo " _id " de la tabla " call_log ".

Ilustración 53. Descripción de los campos de la tabla "message_call_log"

4.6.29. message_details

Tabla que registra información del dispositivo que ha enviado el mensaje, tanto si es un mensaje entrante como saliente.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje transmitido. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ", posibilitando vincular ambas tablas.
author_device_jid	Este valor se corresponde con el campo " _id " de la tabla " jid ", que permite identificar el número de dispositivo que ha enviado el mensaje. En dicha tabla se puede identificar el número de dispositivo en los campos " device " y " raw_string ".

Ilustración 54. Descripción de los campos de la tabla "message_details"

4.6.30. message_edit_info

Tabla que registra los mensajes editados, tanto si son mensajes recibidos como enviados por el usuario de esta cuenta.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje editado. Dicho valor se corresponde con el campo " _id " de la tabla " message ".
original_key_id	Identificador del mensaje original antes de ser editado (tras la edición, cambia la " key_id " de la tabla " message " del mensaje).
edited_times-tamp	Fecha de la grabación de la edición del mensaje en esta base de datos en formato UTC Unix Epoch (milisegundos).
sender_times-tamp	Fecha del envío el mensaje editado en formato UTC Unix Epoch (milisegundos).

Ilustración 55. Descripción de los campos de la tabla "message_edit_info"

4.6.31. message_ephemeral

Tabla que registra todos los mensajes temporales que se han intercambiado a través de la aplicación, el motivo por el que se ha aplicado la temporalidad y si la aplicó el usuario de esta cuenta.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje temporal. Dicho valor se corresponde con el valor del campo "_id" de la tabla "message" , posibilitando la vinculación entre ambas tablas.
duration	Duración aplicada al mensaje antes de ser eliminado. Las opciones disponibles son 86400 (24 horas), 604800 (7 días) o 7776000 (90 días).
expire_timestamp	Fecha prevista en la que se eliminará el mensaje en formato UTC Unix Epoch (milisegundos).
keep_in_chat	Si se ha seleccionado la opción de <i>"conservarlo"</i> , el mensaje no se eliminará cuando se cumpla el tiempo establecido y su valor será "1" . En caso contrario y por defecto el valor es "0" , siendo eliminado el mensaje cuando transcurra el tiempo definido.
ephemeral_trigger	Se desconoce el significado de los valores que se presentan en el rango de "0" a "2" .
ephemeral_initiated_by_me	Quién ha aplicado la temporalidad al chat en el que se encuentra el mensaje: 0 : un contacto. 1 : el usuario de esta cuenta. En ocasiones el campo se encuentra vacío, desconociéndose el motivo.

Ilustración 56. Descripción de los campos de la tabla **"message_ephemeral"**

4.6.32. message_ephemeral_setting

Tabla que registra la activación o desactivación de la temporalidad en los chats. Los mensajes son generados por el sistema en el momento que se aplica temporalidad.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje informativo del cambio de temporalidad de los mensajes en un chat. Dicho valor se corresponde con el valor del campo “_id” de la tabla “ message ”.
setting_duration	Duración aplicada a los mensajes del chat antes de ser eliminados. Las opciones son: 0 (cuando se desactiva la temporalidad que previamente tenían establecida y por tanto no se eliminarán), 86400 (24 horas), 604800 (7 días), 7776000 (90 días)
setting_reason	Motivo por el que se ha activado la temporalidad en los mensajes en el chat: 0: se ha aplicado temporalidad (predeterminada o manualmente) a los mensajes de un chat grupal o en caso de ser un chat individual, se ha aplicado manualmente la temporalidad. 1: los mensajes del chat individual tienen temporalidad porque el usuario de esta cuenta de WhatsApp tenía predeterminada temporalidad en los mensajes cuando se creó el chat. 2: los mensajes del chat individual tienen temporalidad porque el contacto tenía predeterminada temporalidad en los mensajes cuando se creó el chat.
ephemeral_trigger	Motivo por el que se han activado los mensajes temporales: <u>Chats individuales:</u> 0: los demás casos. 2: La temporalidad está predeterminada en chats nuevos en alguno de los dos participantes. <u>Chats grupales:</u> 0: cuando un participante desactiva los mensajes temporales. 1: en los demás casos. 2: un contacto ha creado de forma predeterminada un grupo con mensajes temporales.

Campo	Descripción
ephemeral_initiated_by_me	Quién ha aplicado la temporalidad a los mensajes: 0: un contacto. 1: el usuario de esta cuenta. En ocasiones el campo se encuentra vacío, como cuando se elimina la temporalidad a un chat o cuando en un chat individual se ha aplicado manualmente la temporalidad ("message_type" = "36").

Ilustración 57. Descripción de los campos de la tabla "message_ephemeral_setting"

4.6.33. message_event

Tabla que registra los eventos creados.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje del evento. Dicho valor se corresponde con el campo "_id" de la tabla "message".
is_canceled	Ha sido cancelado el evento: 0: no. 1: sí.
name	Nombre del evento.
description	Descripción del evento.
location_latitude	Cuando se ha nombrado una localización el valor es "0", en caso contrario estará vacío.
location_longitude	Cuando se ha nombrado una localización el valor es "0", en caso contrario estará vacío.
location_name	Nombre de la localización.
join_link	Enlace para unirse a la llamada o videollamada programada en el evento.
start_time	Fecha en la que se inicia el evento en formato UTC Unix Epoch (milisegundos).
chat_row_id	Identificación del chat en el que se ha generado el evento. Este valor se corresponde con el valor del campo "_id" de la tabla "chat"

Campo	Descripción
end_time	Fecha en la que finaliza el evento en formato UTC Unix Epoch (milisegundos).
allow_extra_guests	Se permite que las personas lleven a un invitado adicional: 0 : no. 1 : sí.

Ilustración 58. Descripción de los campos de la tabla "message_event"

4.6.34. message_forwarded

Tabla que registra los mensajes reenviados, tanto si son enviados como recibidos por el usuario de esta cuenta. Se considera mensaje reenviado, cuando el emisor del mensaje lo recibió previamente de otro contacto y no cuando se envía varias veces un mensaje propio a varios contactos.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje reenviado. Dicho valor se corresponde con el campo "_id" de la tabla "message".
forward_score	Número de veces que el mensaje ha sido reenviado entre los usuarios de la aplicación. Cuando el valor es "127", significa que el mensaje se ha reenviado entre diferentes usuarios en 5 ocasiones o más y la aplicación advierte a los participantes que se ha "Reenviado muchas veces".

Ilustración 59. Descripción de los campos de la tabla "message_forwarded"

4.6.35. message_ftsv2_content

Tabla que contiene una copia del texto que se ha intercambiado en los mensajes o en el caso que se haya intercambiado un documento, el nombre de éste. En la base de datos se encuentra la tabla denominada

"message_ftsv2", que es una copia exacta a esta tabla que se va a describir, excepto que no dispone del campo **"docid"**.

En esta tabla no se registran mensajes del sistema ni mensajes de visualización única.

Campo	Descripción
docid	Valor que se corresponde con el valor del campo "_id" de la tabla "message" .
c0content	Texto del mensaje, nombre del documento o transcripción de la nota de voz. En cualquier otro caso se encuentra vacío.
c2fts_namespace	Tipo de mensaje o archivo intercambiado: fa : archivo de audio o nota de voz. fd : documento. fg : gif. fi : archivo de imagen. fl : link o enlace. fo : encuesta. fs : avatar o sticker. fv : archivo de vídeo. En mensaje de texto, evento, sistema, llamada o nota de vídeo, este campo se encuentra vacío .

*Ilustración 60. Descripción de los campos de la tabla **"message_ftsv2_content"***

4.6.36. message_limit_sharing_setting

Tabla que contiene la información de la activación o desactivación de la opción de privacidad avanzada del chat (Ver apartado 8.9 PRIVACIDAD AVANZADA DEL CHAT).

Campo	Descripción
message_row_id	Valor que se corresponde con el valor del campo "_id" de la tabla "message" .

Campo	Descripción
enabled	Estado de la privacidad avanzada del chat: 0 : desactivada. 1 : activada.
trigger	En las pruebas realizadas siempre presenta el valor " 1 ".

Ilustración 61. Descripción de los campos de la tabla "message_limit_sharing_setting"

4.6.37. message_location

Tabla que registra los datos generados cuando se comparte (enviado/ recibido) la ubicación actual (estática) o en tiempo real (dinámica).

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje a través del que se ha compartido la ubicación. Dicho valor se corresponde con el campo " _id " de la tabla " message ", posibilitando vincular ambas tablas.
chat_row_id	Valor que relaciona el chat con el contacto o grupo que ha compartido o con el que se ha compartido la ubicación. El valor se corresponde con el valor del campo " _id " de la tabla " chat ".
latitude	Latitud inicial en ubicación en tiempo real o latitud en ubicación actual.
longitude	Longitud inicial en ubicación en tiempo real o latitud en ubicación actual.
place_name	Cuando se comparte ubicación actual, nombre del lugar elegido entre los lugares cercanos a su posición propuestos por la aplicación (de posible interés como restaurantes, hoteles, comercios...).
URL	URL de la página con información del lugar elegido entre los lugares cercanos a su posición, propuestos por la aplicación (de posible interés).
live_location_share_duration	Tiempo en segundos en el que se ha compartido la <u>ubicación en tiempo real</u> . Por defecto se puede optar entre 15 minutos (900 seg.), 1 hora (3600 seg.) o 8 horas (28800 seg.), aunque el usuario una vez que ha elegido una opción puede dejar de compartir la ubicación cuando lo desee.

Campo	Descripción
live_location_sequence_number	Fecha del inicio de la transmisión en formato UTC Unix Epoch (microsegundos) en ubicación en tiempo real.
live_location_final_latitude	Latitud final en ubicación en tiempo real.
live_location_final_longitude	Longitud final en ubicación en tiempo real.
live_location_final_timestamp	Fecha del final de la transmisión de la ubicación en tiempo real en formato UTC Unix Epoch (milisegundos).

Ilustración 62. Descripción de los campos de la tabla "message_location"

4.6.38. message_media

Tabla que registra información sobre los archivos (notas de voz, notas de vídeo, archivos de audio, imagen, vídeo, documentos, etc.) intercambiados entre el usuario y sus contactos, grupos...

No siempre se graban todos los campos, como por ejemplo la ruta o el nombre del archivo transmitido cuando no se ha descargado en el dispositivo, o es un archivo de visualización única y ha sido eliminado automáticamente tras su reproducción.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje que contiene el archivo transmitido. Dicho valor se corresponde con el valor del campo "_id" de la tabla "message", vinculando ambas tablas.
chat_row_id	Valor que identifica el chat en el que se ha transmitido el archivo. El valor se corresponde con el valor del campo "_id" de la tabla "chat".
multicast_id	Cuando se reenvía un archivo a varios contactos a la vez, se genera un valor de 32 caracteres hexadecimales (el mismo en todos los contactos que reciben el archivo). En los demás casos, el campo se encuentra vacío.
media_job_uuid	Identificador único universal del archivo (32 dígitos hexadecimales).

Campo	Descripción
transferred	El valor es "1" siempre que el archivo se ha enviado o en caso de recibirlo, si se ha descargado en el dispositivo. En caso de recibirlo y no descargarlo el valor es "0".
transcoded	El archivo ha sido transcodificado (comprimido y eliminado metadatos) 0 : no. 1 : sí. Únicamente se transcodifican los archivos enviados de imagen, vídeo, nota de vídeo y gif.
file_path	Ruta en el sistema de archivos del dispositivo analizado en la cual se ubica el archivo que ha sido enviado o recibido. Si se encuentra en blanco, significa que el archivo no se encuentra actualmente en el dispositivo (no se ha descargado, archivo de visualización única eliminado, etc.).
file_size	Tamaño en bytes del archivo transmitido. En numerosas ocasiones no registra el tamaño y graba el valor "0", siendo más preciso el campo "file_length" (descrito en esta tabla más adelante).
media_key	Clave de cifrado del archivo transmitido.
media_key_timestamp	Fecha de creación de la clave de cifrado del archivo en formato UTC Unix Epoch (microsegundos).
width	Número de píxeles de ancho (resolución de imágenes y vídeos).
height	Número de píxeles de alto (resolución de imágenes y vídeos).
thumbnail_height_width_ratio	Ratio altura/anchura del thumbnail (imagen, vídeo o pdf).
message_URL	URL en el que se encuentra el archivo transmitido.
mime_type	Tipo de MIME cuando el archivo transmitido es imagen, audio, vídeo, documento, avatar, gif, nota de vídeo o sticker.
file_length	Tamaño en bytes del archivo multimedia.
media_name	Nombre del archivo.
file_hash	Hash SHA-256 codificado en Base64 del archivo transmitido.
media_duration	Duración en segundos del archivo (vídeo, audio, notas de voz y de vídeo).
page_count	Número de páginas del archivo si es un documento, en cualquier otro caso el valor es "0".

Campo	Descripción
original_file_hash	Hash SHA-256 codificado en Base64 del archivo original, antes de ser comprimido por la aplicación para ser transmitido. Únicamente se presenta en mensajes enviados, que sean imágenes o vídeos.
mute_video	El archivo de vídeo enviado sin sonido toma el valor "1", en cualquier otro caso el valor es "0".
raw_transcription_text	Texto de la transcripción de la nota de voz.

Ilustración 63. Descripción de los campos de la tabla "message_media"

4.6.39. message_mentions

Tabla que registra los mensajes en los que se menciona a otros contactos de la aplicación. Es una opción que se puede realizar en los chats de grupo, en los cuales se utiliza el carácter "@" seguido del nombre del contacto para indicar a quien va dirigido el mensaje.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
message_row_id	Valor que permite identificar el mensaje en el que se menciona a un contacto. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ", posibilitando la vinculación entre ambas tablas.
jid_row_id	Valor que permite localizar el identificador "jid" del contacto mencionado. El valor se corresponde con el valor del campo " _id " de la tabla " jid ".

Ilustración 64. Descripción de los campos de la tabla "message_mentions"

4.6.40. message_poll

Tabla que registra el número de opciones de voto que pueden seleccionar los participantes en cada encuesta.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje en el que se encuentra la encuesta. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ", posibilitando la vinculación entre ambas tablas.
selectable_options_count	Número de opciones seleccionables por cada participante: 0 : una o más opciones. 1 : únicamente una opción.

Ilustración 65. Descripción de los campos de la tabla "**message_poll**"

4.6.41. message_poll_option

Tabla que registra las opciones de voto que pueden seleccionar en cada encuesta, así como el número de votos que han obtenido cada opción.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
message_row_id	Valor que permite identificar el mensaje en el que se encuentra la encuesta. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ", posibilitando la vinculación entre ambas tablas.
option_sha256	Hash SHA-256 codificado en Base64 del texto del campo " option_name ".
option_name	Opción seleccionable en la encuesta por los usuarios.
vote_total	Número total de votos que ha obtenido esta opción.

Ilustración 66. Descripción de los campos de la tabla "**message_poll_option**"

4.6.42. message_privacy_state

Tabla que registra los mensajes enviados por el usuario de esta cuenta a bots, como por ejemplo en de "Meta IA", "ChatGPT" o "LuzIA".

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje enviado por el usuario a un bot. Dicho valor se corresponde con el valor del campo “_id” de la tabla “ message ”, posibilitando la vinculación entre ambas tablas.
actual_actors	Se desconoce la función de este campo. Como ejemplo, en las pruebas realizadas “Meta IA” o “LuzIA” presentan el valor “1” y “ChatGPT” el valor “2”.

Ilustración 67. Descripción de los campos de la tabla “message_privacy_state”

4.6.43. message_quoted

Tabla que registra los mensajes citados o mencionados en otros mensajes.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje en el cual se cita otro mensaje. Dicho valor se corresponde con el valor del campo “_id” de la tabla “ message ”, posibilitando la vinculación entre ambas tablas.
chat_row_id	Identificación del chat al que pertenece el mensaje citado. Este valor se corresponde con el valor del campo “_id” de la tabla “ chat ”.
parent_message_chat_row_id	Valor que permite la identificación del chat al que pertenece la conversación en la que se cita el mensaje. Este valor se corresponde con el valor del campo “_id” de la tabla “chat”. Normalmente este valor y el anterior serán el mismo. Pero como ejemplo, cuando el usuario o un contacto menciona de forma privada en su estado al otro, el anterior campo se corresponde al del chat de su “estado” y este campo al del chat entre el usuario de esta cuenta y el contacto.
from_me	Emisor del mensaje citado: 0: un contacto. 1: el usuario de esta cuenta.

Campo	Descripción
sender_jid_row_id	Valor que permite determinar el identificador "jid" del emisor del mensaje que citado en chats de grupo. Dicho valor se corresponde con el valor el campo "_id" de la tabla "jid". En chats individuales el valor es "0".
key_id	Identificador del mensaje que citado. El valor se corresponde con el campo "key_id" de la tabla "message" del mensaje que se cita.
timestamp	Fecha de envío del mensaje citado en formato UTC Unix Epoch (milisegundos). El campo contiene el mismo valor que el campo "timestamp" de la tabla "message".
message_type	Tipo de mensaje del mensaje citado (ver tabla "message").
text_data	Texto del mensaje citado (en caso de que contuviese texto).

Ilustración 68. Descripción de los campos de la tabla "message_quoted"

4.6.44. message_revoked

Tabla que registra los mensajes que constan como eliminados en la tabla "message". Concretamente los señalados en dicha tabla en el campo "message_type" con el valor "15" y "64" (mensajes borrados para todos, emisor y destinatario/s).

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje borrado. Dicho valor se corresponde con el valor del campo "_id" de la tabla "message", posibilitando vincular ambas tablas.
revoked_key_id	Valor del campo "key_id" de la tabla "message" del mensaje original, previo a ser eliminado.
admin_jid_row_id	Valor que permite localizar el identificador "jid" del administrador de grupo que ha borrado el mensaje (siempre que sea un chat de grupo). El valor se corresponde con el valor del campo "_id" de la tabla "jid".
revoke_timestamp	Fecha del borrado del mensaje en el teléfono analizado en formato UTC Unix Epoch (milisegundos).

Ilustración 69. Descripción de los campos de la tabla "message_revoked"

4.6.45. message_system

Tabla que registra los mensajes del sistema.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje del sistema. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ".
action_type	Tipo de acción. Ejemplos de acciones que generan mensajes del sistema: 2: mensaje del sistema que registra la creación de un grupo por el usuario. 4: "Se añadió a xxxxx" (al grupo o la lista) o "Se te añadió al grupo". Informa que se ha añadido al usuario o a un contacto a un grupo o un contacto a una lista de difusión. 5: "xxxxx salió del grupo." 7: "Se eliminó a xxxxx de la lista". Cuando el usuario elimina a un contacto de una lista de difusión. 9: "Creaste una lista de difusión con x destinatarios". 11: "(Creaste o xxxxx creó) (el grupo o la comunidad "nombre")". 12: "Añadiste a xxxxx o xxxxx te añadió". Informa que se ha añadido al usuario o a un contacto al grupo o la comunidad. 14: "Eliminaste o xxxxx eliminó a (nombre de usuario)". Cuando se elimina a un usuario de un grupo o comunidad. 15: "Ahora eres admin. del grupo". Informa que un administrador de grupo ha asignado al usuario como administrador también. 27: "Cambiaste la descripción del grupo. Toca para verla." 29: "Cambiaste la configuración para que solo los administradores puedan editar los ajustes de grupo." 30: "Cambiaste los ajustes para que todos los miembros puedan editar la configuración de grupo." 31: "Cambiaste los ajustes de este grupo para permitir que solo los administradores puedan enviar mensajes al grupo." 32: "Cambiaste los ajustes de este grupo para permitir que todos los miembros puedan enviar mensajes al grupo."

Campo	Descripción
action_type	56: "(Actualizaste o xxxxx actualizó) la duración de los mensajes. Los mensajes nuevos desaparecerán de este chat después de xx días de haber sido enviados, a menos que se use la opción para conservarlos". Informa de que el creador de un grupo, de forma predeterminada ha asignado temporalidad a los mensajes durante la creación del grupo. 58: "Bloqueaste a este contacto. Toca para desbloquearlo." o "Desbloqueaste a este contacto" 59: "Se desactivaron los mensajes temporales. Toca para cambiar esta opción." 67: "Los mensajes y las llamadas están cifradas de extremo a extremo. Nadie fuera de este chat, ni siquiera WhatsApp, puede leerlos ni escucharlos. Toca para obtener más información". Es un mensaje del sistema cuando se inicia un chat. 68: "Usas una duración predeterminada para los mensajes temporales en chats nuevos. Los mensajes nuevos desaparecerán de este chat después de xx días de haber sido enviados, a menos que se use la opción de conservarlos. Toca para establecer la duración predeterminada que desees." 79: "(Te uniste o xxxxx se unió) desde la comunidad". El usuario o un contacto se ha unido al grupo desde una comunidad a la que pertenece. 81: "(Ahora eres o xxxxx ahora es) admin. de la comunidad." 82: "(Ya no eres o xxxxx ya no es) admin. de la comunidad." 84: "(Activaste o xxxxx activó) la aprobación de los admins. para unirse a este grupo. Toca para cambiar esto." 87: "(Desactivaste o xxxxx desactivó) la comunidad "nombre de la comunidad." 91: "(Cambiaste o xxxxx cambió) los ajustes de este (grupo o comunidad) para permitir que todos los miembros puedan añadir a otras personas." 92: "(Cambiaste o xxxxx cambió) los ajustes de este (grupo o comunidad) para permitir que solo quienes lo administran puedan añadir a otras personas." 99: "Este chat ofrece mayor privacidad para tu número de teléfono. Toca para obtener más información". 102: "Cualquier miembro de la comunidad "nombre de la comunidad" puede unirse al grupo."

Campo	Descripción
action_type	108: "(Añadiste o xxxx añadió) el grupo "nombre del grupo"." Se añadió un grupo a la comunidad. Mensaje que se muestra en "avisos" de la comunidad" 109: "(Eliminaste o xxxxx eliminó) el grupo "nombre del grupo"." Se eliminó un grupo de la comunidad. 110: mensaje del sistema cuando se añade un grupo a la comunidad. No se muestra en ningún chat. 111: mensaje del sistema cuando se elimina un grupo de la comunidad. No se muestra en ningún chat. 116: "(Eliminaste o xxxxx eliminó) este grupo de la comunidad "nombre de la comunidad".". 118: "(Fijaste o xxxxx fijó) un mensaje". 120: "xxxxx solicitó añadir a yyyy." Solicitud del usuario o de xxxxx para añadir al grupo a yyyy, ya que un administrador debe aprobar la unión al grupo. 122: "¡Te damos la bienvenida a tu comunidad!" mensaje informando de que el usuario ha creado su comunidad. 128: "(Añadiste o xxxxx añadió) este grupo a la comunidad "nombre de la comunidad"." Mensaje que se muestra en el chat del grupo. 129: el contacto del que se ha recibido comunicación no se encuentra en la agenda del usuario. 132: "(Creaste o Se creó) el canal "nombre del canal"." 134: "Este canal ofrece mayor privacidad para tu perfil y número de teléfono. Toca para obtener más información", cuando el usuario se une a un canal. Cuando el usuario crea el canal: "Este canal es público y visible para cualquiera, incluido WhatsApp. Tu perfil y número de teléfono tienen más privacidad. Toca para obtener más información." 137: "Ahora, cualquier miembro de esta la comunidad puede añadir grupos. Toca para cambiar esto." 138: "Solo quienes administran la comunidad pueden añadir grupos. Los miembros pueden sugerirles grupos para que los aprueben. Toca para cambiar esto." 144: "¡Te damos la bienvenida a la comunidad!" mensaje informado de que se le ha añadido al usuario a la comunidad porque forma parte de un grupo incluido en esta comunidad.

Campo	Descripción
action_type	145: mensaje del sistema para revisar la aprobación de la unión de un grupo a una comunidad. 148: "Te damos la bienvenida al grupo General". Mensaje que informa de la creación automática del grupo "General" cuando el usuario crea una comunidad. 149: "Te damos la bienvenida al grupo General. Te uniste a este grupo. Todos los miembros de la comunidad pueden usar este chat para hablar entre ellos.". Mensaje que informa de que el usuario se ha unido voluntariamente al chat General de una comunidad de la que no es el creador. 152: "Ya no se añadirá automáticamente a los nuevos miembros de la comunidad." Mensaje informando que en el grupo "General" de una comunidad creada por el usuario se debe añadir manualmente a los contactos. 154: "Aumenta los seguidores de "nombre del canal" Para empezar, añade tu primera actualización. Comparte el enlace para invitar a personas". 167: Mensaje del sistema cuando se crea una comunidad. 168: "(Desactivaste o xxxxx desactivó) el grupo "General". Tras desactivar una comunidad, su grupo "General" también se desactiva. 169: "xxxx actualizó (Nombre del evento). Ver evento.". 170: "xxxx canceló (Nombre del evento). Ver evento.". 185: "Meta AI es un servicio opcional de Meta que utiliza modelos de IA para ofrecer respuestas..."

Ilustración 70. Descripción de los campos de la tabla "message_system"

4.6.46. message_thumbnail

Tabla que almacena las miniaturas o thumbnails de archivos transmitidos.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje que contiene el archivo del cual se ha obtenido la miniatura. Dicho valor se corresponde con el valor del campo "_id" de la tabla "message", posibilitando vincular ambas tablas.

Campo	Descripción
thumbnail	Imagen miniatura o thumbnail que representa el archivo transmitido en el mensaje.

Ilustración 71. Descripción de los campos de la tabla **"message_thumbnail"**

4.6.47. message_vcard

Tabla que almacena las tarjetas de contactos transmitidas.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
message_row_id	Valor que permite identificar el mensaje en el que se transmitió la tarjeta de contacto. Dicho valor se corresponde con el valor del campo "_id" de la tabla "message" , posibilitando vincular ambas tablas.
vcard	Información contenida en la tarjeta de contacto.

Ilustración 72. Descripción de los campos de la tabla **"message_vcard"**

4.6.48. message_vcard_jid

Tabla que enlaza las tarjetas de contactos transmitidas con su identificador "jid".

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
vcard_jid_row_id	Valor que permite localizar el identificador "jid" del contacto transmitido en la tarjeta de contacto. Dicho valor se corresponde con el valor del campo "_id" de la tabla "jid" , posibilitando vincular ambas tablas.
vcard_row_id	Valor que se corresponde con el campo "_id" de la tabla "message_vcard" , permitiendo vincular ambas tablas.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje en el que se transmitió la tarjeta de contacto. Dicho valor se corresponde con el valor del campo “_id” de la tabla “ message ”, posibilitando vincular ambas tablas.

*Ilustración 73. Descripción de los campos de la tabla “**message_vcard_jid**”*

4.6.49. **message_view_once_media**

Tabla que registra los mensajes enviados de visualización única (imágenes, vídeos y notas de voz).

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje de visualización única. Dicho valor se corresponde con el valor del campo “_id” de la tabla “ message ”, posibilitando vincular ambas tablas.
state	Estado en el que se encuentra el mensaje: 0: sin visualizar por el receptor (si es un grupo, con un participante que no lo visualice constará este valor). 1: visualizado por el receptor. 2: cuando se ha eliminado el archivo del dispositivo del receptor por haber transcurrido 14 días sin que lo haya visualizado (previamente el valor ha tenido que ser “0” hasta que se han cumplido los 14 días sin visualizar). En un chat individual, si los dos participantes no tienen activada la confirmación de lectura, en los mensajes enviados por el usuario de esta cuenta no se confirmará la visualización por parte del receptor y por tanto, no puede obtener el valor “1” en este campo.

*Ilustración 74. Descripción de los campos de la tabla “**message_view_once_media**”*

4.6.50. newsletter

Tabla que registra los canales a los que está suscrito o es creador el usuario de esta cuenta, así como sus características.

Campo	Descripción
chat_row_id	Valor que permite la identificación del chat del canal. Este valor se corresponde con el valor del campo " _id " de la tabla " chat ", posibilitando vincular ambas tablas.
name	Nombre del canal.
name_id	Fecha en la que se asignó el nombre del canal en formato UTC Unix Epoch (microsegundos).
description	Descripción del canal.
description_id	Fecha en la que se insertó la descripción del canal en formato UTC Unix Epoch (microsegundos).
picture_URL	URL del icono del canal.
picture_id	Fecha en la que se agregó el icono al canal en formato UTC Unix Epoch (microsegundos).
invite_code	Código de invitación que propone seguir un canal. Este código se envía al contacto unido a la URL "https://whatsapp.com/channel/", creando un enlace para seguir este canal.
subscribers_count	Número de suscriptores del canal.
membership	1: seguidor del canal 2: administrador del canal 3: propietario del canal
muted	Silenciadas las notificaciones: 0: no. 1: sí.
reaction_setting	Qué reacciones pueden enviar los seguidores. 0: cualquier emoji. 1: solo predeterminadas. 2: ninguna.
reaction_setting_update_ts	Fecha de última consulta de actualización de los ajustes del campo " reaction_setting " en formato UTC Unix Epoch (milisegundos).
admin_count	Número de administradores del canal.

Ilustración 75. Descripción de los campos de la tabla "newsletter"

4.6.51. newsletter_message

Tabla que registra los mensajes enviados por los canales a los que está suscrito o de los que es creador el usuario de esta cuenta.

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje del canal. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ", posibilitando la vinculación de ambas tablas.
chat_row_id	Valor que permite la identificación del chat del canal. Este valor se corresponde con el valor del campo " _id " de la tabla " chat ".
extra_table_last_update_ts	Fecha de última consulta para actualizar la información del mensaje en formato UTC Unix Epoch (milisegundos).
view_count	Número de visualizaciones del mensaje del canal.

Ilustración 76. Descripción de los campos de la tabla "newsletter_message"

4.6.52. newsletter_subscribers

Tabla que registra los contactos suscriptores a los canales creados por el usuario de esta cuenta.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
chat_row_id:	Valor que permite la identificación del chat del canal administrado por el usuario de esta cuenta. Este valor se corresponde con el valor del campo " _id " de la tabla " chat ", permitiendo vincular ambas tablas.
jid_row_id:	Identificación del contacto suscriptor del canal administrado por el usuario. El valor es el mismo que el campo " _id " de la tabla " jid ", permitiendo identificar al suscriptor por su identificador "lid" (oculta el número de teléfono del suscriptor).

Campo	Descripción
role:	Rol del contacto: 1: suscriptor. 2: administrador (propuesto por el propietario del canal) 3: propietario del canal.
fetched_time:	Fecha de última consulta para actualizar la información del suscriptor en formato UTC Unix Epoch (milisegundos).

Ilustración 77. Descripción de los campos de la tabla **"newsletter_subscribers"**

4.6.53. played_self_receipt

Tabla que registra las notas de voz, notas de vídeo y mensajes de visualización única (archivo de imagen, archivo de vídeo o nota de voz) recibidos en esta cuenta y reproducidos por el usuario, en chats individuales cuando el usuario tiene desactivado la opción de privacidad "confirmaciones de lectura".

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje reproducido voluntariamente por el usuario de esta cuenta. Dicho valor se corresponde con el valor del campo "_id" de la tabla "message" , posibilitando vincular ambas tablas.
to_jid_row_id	Valor que permite localizar el identificador "jid" del contacto que ha enviado el mensaje. Este valor se corresponde con el valor del campo "_id" de la tabla "jid" .
message_id	Número identificativo del mensaje, que se corresponde con el campo "key_id" de la tabla "message" .

Ilustración 78. Descripción de los campos de la tabla **"played_self_receipt"**

4.6.54. receipt_device

Tabla que registra los dispositivos que han recibido un mensaje enviado desde la cuenta de este usuario, incluidos los vinculados a esta cuenta.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
message_row_id	Valor que permite identificar el mensaje enviado por el usuario de esta cuenta. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ", posibilitando la vinculación entre ambas tablas.
receipt_device_jid_row_id	Este valor se corresponde con el campo " _id " de la tabla " jid ", que permite identificar el número de dispositivo que potencialmente ha podido recibir el mensaje. En dicha tabla podremos identificar el número de dispositivo en los campos " device " y " raw_string ". Ejemplos: Dispositivo principal: 34612123123.0:0@s.whatsapp.net Dispositivo vinculado número 82: 34612123123.0:82@s.whatsapp.net
receipt_device_timestamp	Fecha de recepción del mensaje en el dispositivo identificado en el campo anterior en formato UTC Unix Epoch (milisegundos). Cuando es un dispositivo vinculado a esta cuenta, únicamente registrará la fecha si en el momento del envío contaba con conexión a internet.

*Ilustración 79. Descripción de los campos de la tabla "**receipt_device**"*

4.6.55. receipt_user

Tabla que registra la fecha en la que un contacto ha recibido, leído y reproducido un mensaje enviado desde la cuenta de este usuario. Cuando se trata de un mensaje enviado a un grupo, se generará una fila o registro por cada contacto que forme parte del grupo.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje enviado por el usuario de esta cuenta. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ", posibilitando la vinculación entre ambas tablas.
receipt_user_jid_row_id	Valor que permite localizar el identificador "jid" del contacto receptor del mensaje. Este valor se corresponde con el valor del campo " _id " de la tabla " jid ".
receipt_timestamp	Fecha de recepción del mensaje por el contacto en formato UTC Unix Epoch (milisegundos).
read_timestamp	Fecha en la que se ha abierto el chat en el que se encuentra el mensaje por el contacto en formato UTC Unix Epoch (milisegundos). Para que registre la fecha de un chat individual es preciso que se encuentre activada la confirmación de lectura en ambos participantes.
played_timestamp	Fecha en la que se ha reproducido el mensaje por el contacto en formato UTC Unix Epoch (milisegundos), cuando el mensaje es una nota de voz, nota de vídeo o mensajes de visualización única. Para que registre la fecha de un chat individual es preciso que se encuentre activada la confirmación de lectura en ambos participantes.

*Ilustración 80. Descripción de los campos de la tabla "**receipt_user**"*

4.6.56. status

Tabla que registra los mensajes o historias (texto, nota de voz, imagen, vídeo o gif) que se han publicado en un estado y que se han compartido 24 horas con otros contactos. Cada fila o registro aporta información de una publicación en el estado de un contacto o del propio usuario de esta cuenta.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
jid_row_id	Valor que permite localizar el identificador "jid" del contacto o usuario que ha publicado en su estado. Este valor se corresponde con el valor del campo " _id " de la tabla " jid ".

Campo	Descripción
message_table_id	Valor que permite identificar el último mensaje o historia publicada en el estado. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ".
last_read_message_table_id	Valor que permite identificar el último mensaje o historia visualizada por el usuario de esta cuenta entre los publicados en el estado del contacto. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ".
last_read_receipt_sent_message_table_id	Valor que permite identificar el último mensaje o historia visualizada por el usuario de esta cuenta y confirmada su lectura al emisor entre los publicados en su estado. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ".
first_unread_message_table_id	Valor que permite identificar el primer mensaje o historia que aún no ha sido visualizada por el usuario de esta cuenta entre los publicados en el estado del contacto. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ".
autodownload_limit_message_table_id	Valor que permite identificar el último mensaje o historia descargada en la cuenta del usuario entre los publicados en el estado del contacto. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ".
timestamp	Fecha del último mensaje o historia publicada en la cuenta del correspondiente contacto o usuario, en formato UTC Unix Epoch (milisegundos).
unseen_count	Número de mensajes o historias que actualmente se encuentran publicadas en el estado del correspondiente contacto sin visualizar por el usuario de esta cuenta.
total_count	Número total de mensajes o historias que actualmente se encuentran publicadas en el estado del correspondiente contacto.

*Ilustración 81. Descripción de los campos de la tabla "**status**"*

4.6.57. status_message_info

Tabla que registra las características de privacidad de los mensajes (texto, nota de voz, vídeo o gif, imagen) que el usuario o un contacto de esta cuenta ha publicado en su estado (historias).

Campo	Descripción
message_row_id	Valor que permite identificar el mensaje o historia publicada en el estado del usuario de esta cuenta. Dicho valor se corresponde con el valor del campo " _id " de la tabla " message ", posibilitando la vinculación entre ambas tablas.
status_distribution_mode	Quiénes pueden ver el estado del usuario (historias): 0 : mis contactos. 1 : solo compartir con... 2 : mis contactos excepto... 3 : estado de un contacto.
is_mentioned	Ha sido mencionado privadamente el usuario de esta cuenta en el estado de un contacto: 0 : no. 1 : sí.
status_mentions	Identificador "jid" del contacto que ha sido mencionado privadamente por el usuario de esta cuenta.
has_embedded_music	Acompaña música al estado: 0 : no. 1 : sí.
status_mention_source	Identificador "jid" del contacto que ha mencionado privadamente al usuario de esta cuenta.
selected_audience_list	Identificador "jid" de los contactos a los que se les aplica la condición del campo " status_distribution_mode ".

*Ilustración 82. Descripción de los campos de la tabla "**status_message_info**"*

4.6.58. user_device

Tabla que registra y vincula los identificadores "jid" de los dispositivos con sus usuarios. Un único contacto (campo "**user_jid_row_id**") tendrá asignado tantos identificadores de dispositivos (campo "**device_jid_row_id**") como dispositivos haya vinculado con su cuenta de WhatsApp. Pero únicamente estarán registrados en esta tabla los dispositivos que hayan mantenido algún tipo de comunicación con el usuario de esta cuenta.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
user_jid_row_id	Valor que permite comprobar el identificador "jid" del contacto. Este valor se corresponde con el valor del campo "_id" de la tabla "jid".
device_jid_row_id	Este valor que permite comprobar el identificador de dispositivo del contacto. Se corresponde con el campo "_id" de la tabla "jid" en la cual se puede identificar el número de dispositivo en los campos "device" y "raw_string".

Ilustración 83. Descripción de los campos de la tabla "user_device"

4.7. Base de datos *wa.db*

Es la base de datos que contiene la información de los contactos, grupos, difusiones, comunidades y canales. A continuación, se muestran las tablas (muchas de ellas no están activas) presentes en la base de datos "**wa.db**" en esta versión de la aplicación y se desmenuza el contenido de las tablas más significativas. Hay otras tablas que seguramente contengan información de interés dependiendo del análisis que estemos realizando pero que no van a ser descritas en el presente.

wa.db
DDL
android_metadata
community_settings
dismissed_chat
dogfooder_diagnostics_events
group_membership_approval_requests
group_membership_count
group_relationship
member_suggested_groups_v2
meta_ai_memory
mm_notification_impression
non_admin_group_membership_approval_requests
profile_links
quick_promotion_payload
recently_accepted_deeplink_invites
sqlite_sequence
status_ranking
subgroup_info
system_contacts_version_table

	wa_about_block_list
	wa_address_book
	wa_biz_brand_id_list
	wa_biz_category_service_offerings
	wa_biz_integrity_chat_settings
	wa_biz_integrity_signals
	wa_biz_profile_to_service_offerings
	wa_biz_profiles
	wa_biz_profiles_bot_attributes
	wa_biz_profiles_call_hours
	wa_biz_profiles_categories
	wa_biz_profiles_dc_enabled_features
	wa_biz_profiles_direct_connection_allowed_country_codes
	wa_biz_profiles_hours
	wa_biz_profiles_linked_accounts_table
	wa_biz_profiles_price_tiers
	wa_biz_profiles_service_areas
	wa_biz_profiles_websites
	wa_block_list
	wa_block_list_interop
	wa_bot_profiles
	wa_chat_ranking_scores
	wa_contact_storage_usage
	wa_contacts
	wa_contacts_created_within_wa
	wa_group_add_allow_list
	wa_group_add_black_list
	wa_group_admin_settings
	wa_group_descriptions
	wa_last_entry_point
	wa_last_seen_block_list
	wa_logging_entry_point
	wa_ml_models
	wa_newsletter_props
	wa_pix_block_list
	wa_profile_links_deny_list
	wa_profile_photo_block_list
	wa_props
	wa_stickers_allow_list
	wa_trusted_contacts
	wa_trusted_contacts_send
	wa_vnames
	wa_vnames_localized

Ilustración 84. Tablas de la base de datos “**wa.db**”

4.7.1. group_membership_count

Tabla que registra el número de grupos que forman parte de una comunidad.

Campo	Descripción
jid_row_id	Identificación "jid" de la comunidad de WhatsApp. Ejemplo: 120363162357272244@g.us
member_count	Número de grupos que forman parte de esta comunidad.

*Ilustración 85. Descripción de los campos de la tabla
"group_membership_count"*

4.7.2. group_relationship

Tabla que registra los grupos (por su identificador "jid") que forman parte de una comunidad. Se grabará un registro por cada grupo que forme parte de una comunidad, de modo que se generarán tantas filas como grupos la compongan. Todos estos grupos comparten el mismo valor en el campo "**parent_raw_jid**" que identifica la comunidad a la que pertenecen.

Cuando se crea una comunidad se generan dos identificadores únicos "jid" de dicha comunidad. De la misma forma que hay una fila por cada grupo que forma parte de la comunidad, también existirá una fila que relaciona los dos identificadores de la misma comunidad (Ver apartado 8.1.4 Comunidades).

Campo	Descripción
parent_raw_jid	Identificación "jid" de la comunidad de WhatsApp. Ejemplo: 120363162121270372@g.us

Campo	Descripción
subgroup_raw_id	Identificación "jid" del grupo o comunidad de WhatsApp. Ejemplos: 34699888777-1379114707@g.us (formato antiguo de grupos) 120363080564732148@g.us (formato actual de grupos o comunidades)

Ilustración 86. Descripción de los campos de la tabla "group_relationship"

4.7.3. subgroup_info

Tabla que registra las comunidades en las que participa el usuario, así como los grupos que forman parte de estas comunidades, incluyendo el grupo "General" que se genera automáticamente cuando se crea una comunidad.

Campo	Descripción
subgroup_raw_id	Identificación "jid" del grupo o comunidad de WhatsApp. Ejemplos: 34699888777-1379114707@g.us (grupos formato antiguo) 120363080564732148@g.us (grupos formato actual o comunidades)
subject	Nombre asignado al grupo o comunidad.
subject_ts	Fecha de creación en formato UTC Unix Epoch (milisegundos) del grupo o comunidad.
group_type	Tipo de agrupación: 2: grupo. 3: comunidad. 6: grupo "General" de una comunidad.

Ilustración 87. Descripción de los campos de la tabla "subgroup_info"

4.7.4. wa_address_book

Tabla que registra los contactos de la agenda del usuario de esta cuenta.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
jid	Identificador "jid" del contacto de WhatsApp del usuario. Ejemplo: 34646223344@s.whatsapp.net
is_whatsapp_user	En el supuesto de que el contacto sea usuario de WhatsApp, contendrá el valor "1". En caso contrario "0".
display_name	Nombre con el que se grabó el contacto en la agenda del teléfono de la cuenta de WhatsApp analizada.
number	Número de teléfono del contacto, tal y como se haya grabado en la agenda del teléfono en el que está instalado WhatsApp (con prefijo internacional o no).
phone_label	Etiqueta del tipo de dispositivo establecida a este contacto por el usuario la cuenta analizada en su agenda de contactos (ej: Móvil, Fijo, Trabajo...).

Ilustración 88. Descripción de los campos de la tabla "wa_address_book"

4.7.5. wa_block_list

Tabla que registra los identificadores de los contactos bloqueados por el usuario de esta cuenta.

Campo	Descripción
jid	Identificador "jid" o "lid" del contacto de WhatsApp bloqueado por el usuario. Ejemplos: 34646223344@s.whatsapp.net 26010522643912@lid

Ilustración 89. Descripción de los campos de la tabla "wa_block_list"

4.7.6. wa_contacts

Tabla que contiene información de todos los contactos que tiene grabados el usuario de esta cuenta en su agenda, y en el caso de que sean usuarios de WhatsApp, información sobre sus perfiles en la aplicación.

Campo	Descripción
_id	Número secuencial de creación del registro (establecido por la base de datos SQLite).
jid	Identificador único "jid" del contacto, grupo, etc., de WhatsApp. Ejemplos: • 34677988122@s.whatsapp.net (contactos) • 34699888777-1379114707@g.us (formato antiguo de grupos) • 120363080564732172@g.us (formato actual de grupos) • 1690524142@broadcast (difusiones) • 120363165396843331@newsletter (canales)
is_whatsapp_user	En el supuesto de que el contacto sea usuario de WhatsApp, contendrá el valor "1". En caso contrario "0".
status	"info." establecido por el contacto en su perfil. Por defecto <i>"¡Hola! Estoy usando WhatsApp."</i> Solo puede ser un texto limitado y/o emojis.
status_timestamp	Fecha de establecimiento del estado "info." por el contacto en formato UTC Unix Epoch (milisegundos). En caso de no tener estado o mantener el estado por defecto (<i>¡Hola! Estoy usando WhatsApp.</i>) el contacto o grupo, se establece el valor "0".
number	Número de teléfono del contacto, tal y como se haya grabado en la agenda del teléfono en el que está instalado WhatsApp (con prefijo internacional o no). Este campo se encuentra vacío en los grupos, comunidades, lista de difusión o canales.
display_name	Nombre con el que se grabó el contacto en la agenda del teléfono donde se ha instalado la cuenta WhatsApp analizada. En grupos, comunidades y lista de difusión es el nombre que se le ha asignado en WhatsApp, y en el caso de los canales se encuentra vacío.

Campo	Descripción
phone_label	Etiqueta del tipo de dispositivo establecida a este contacto por el usuario la cuenta analizada en su agenda de contactos (ej: Móvil, Fijo, Trabajo...). En los grupos, comunidades y difusiones se registra la fecha de su creación en formato UTC Unix Epoch (milisegundos), y en el caso de los canales se encuentra vacío.
thumb_ts	Fecha en la que se ha instalado en la correspondiente cuenta de WhatsApp la imagen de perfil del contacto/grupo/comunidad/canal, en formato UTC Unix Epoch (segundos). Si el valor es "-1" no se ha establecido imagen de perfil. Se desconoce el significado del valor "0".
photo_id_timestamp	Fecha en formato UTC Unix Epoch (milisegundos) en la que la aplicación ha consultado en sus servidores la imagen de perfil del contacto/grupo/comunidad/canal para actualizarla en caso de que la haya cambiado desde la última consulta.
wa_name	Nombre establecido por el contacto en su propia cuenta de WhatsApp.

Ilustración 90. Descripción de los campos de la tabla "wa_contacts"

4.7.7. wa_contacts_created_within_wa

Tabla que contiene información de los contactos que se han creado en la agenda a través de la aplicación WhatsApp.

Campo	Descripción
_id	Número de teléfono del contacto creado a través de WhatsApp

Ilustración 91. Descripción de los campos de la tabla "wa_contacts_created_within_wa"

4.7.8. wa_group_add_black_list

Tabla que contiene información de los contactos bloqueados por el usuario de esta cuenta para que lo añadan en grupos.

Campo	Descripción
jid	Identificador único "jid" del contacto de WhatsApp bloqueado. Se corresponde con el campo " jid " de la tabla " wa_contacts ". Ejemplo: 34655123123@s.whatsapp.net

*Ilustración 92. Descripción de los campos de la tabla
"wa_group_add_black_list"*

4.7.9. wa_group_admin_settings

Tabla que contiene información de la configuración de la administración de los grupos en los que participa el usuario de esta cuenta.

Campo	Descripción
jid	Identificador único "jid" del grupo de WhatsApp. Se corresponde con el campo " jid " de la tabla " wa_contacts ". Ejemplo: 120363080564732172@g.us
restrict_mode	Si los participantes pueden editar los ajustes del grupo (asunto, icono, descripción, duración de los mensajes temporales y conservar mensajes o dejarlo de hacer), el valor es " 0 ". En caso contrario el valor es " 1 ".
announcement_group	Si los participantes pueden enviar mensajes al grupo, el valor es " 0 ". En caso contrario el valor es " 1 ".
ephemeral_duration	Tiempo en segundos de la duración de los mensajes temporales aplicados a este chat grupal antes de eliminarse: " 86400 ", " 604800 " o " 7776000 ". Si los mensajes del chat <u>no</u> son temporales el valor es " 0 ".
creator_jid	Contacto que ha creado el grupo. Se corresponde con el campo " jid " de la tabla " wa_contacts ".

Campo	Descripción
require_member- ship_approval	Si los administradores del grupo deben aprobar a cualquier persona que quiera unirse al grupo, el valor es "1". En caso contrario el valor es "0".
member_add_ mode	Si los participantes del grupo pueden añadir a otros participantes en grupo, el valor es "1". En caso contrario el valor es "0".

*Ilustración 93. Descripción de los campos de la tabla
"wa_group_admin_settings"*

Aunque no se vayan a desarrollar sus características, mencionar que las tablas **"wa_biz_profiles"**, **"wa_biz_profiles_bot_attributes"**, **"wa_biz_profiles_categories"**, **"wa_biz_profiles_hours"**, **"wa_biz_profiles_linked_accounts_table"** y **"wa_biz_profiles_websites"** contienen información de perfiles de cuentas de WhatsApp Business, como pueden ser el identificador "jid" de la cuenta, correo electrónico, dirección, descripción del negocio, ubicación del negocio, zona horaria, categoría de negocio, etc.

5. Bases de datos de Whatsapp (iOS)

En la versión para sistemas iOS también se hace uso de bases de datos de tipo SQLite versión 3, pero con una diferencia sustancial respecto a la de Android, no utiliza archivos WAL (Write-Ahead Logging) para almacenar los últimos cambios de la base de datos. Lógicamente, esto impide la posibilidad de recuperar información de las diferentes bases de datos en esos archivos.

Por otro lado, es sumamente importante la forma de adquisición de la información de un iPhone, porque dependiendo del procedimiento se generarán en la extracción unas rutas y unos archivos u otros. Las extracciones que se pueden obtener son de tipo Full File System (FFS) o Sistema de Archivos Completo, la cual extrae la información con la estructura tal y como se encuentra en el teléfono y de tipo iTunes Backup o similares, que genera una copia de seguridad con una estructura parcialmente diferente. Otra gran diferencia es que en una extracción de Sistema de Archivos Completo (FFS) se obtienen muchos más archivos de la aplicación que con una de tipo iTunes Backup, ya que en este último caso únicamente se copian los archivos que los desarrolladores de Apple han decidido incluir.

Lógicamente, siempre que sea posible, se debería optar por obtener una extracción de tipo FFS, aunque con las últimas generaciones de

iPhone y versiones de iOS, son muy limitadas las herramientas (todas comerciales) que son capaces de obtener este tipo de extracción.

Primero se expondrán las bases de datos que se pueden obtener en ambos tipos de extracción y posteriormente las exclusivas de una extracción FFS.

Bases de datos comunes en ambos tipos de extracciones

5.1. Base de datos *Biz.sqlite*

Esta base de datos registra la información relacionada con las cuentas de empresa (WhatsApp Business) que han interactuado con el usuario de esta cuenta.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Biz/Biz.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID²>/Biz/Biz.sqlite**

2. GUID (Globally Unique Identifier) identificador global único de la aplicación en este teléfono. Este identificador se genera cuando se instala y la numeración no está asignada o vinculada a una aplicación específica, variando en cada instalación.

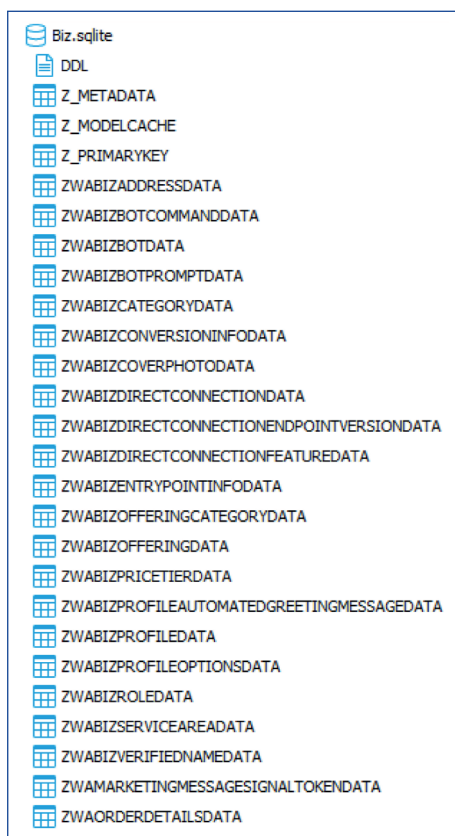


Ilustración 94. Tablas de la base de datos “Biz.sqlite”

5.1.1. ZWABIZPROFILEDATA

Tabla que registra los perfiles de las cuentas business.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor “16”, siendo el número de orden alfabético de la tabla en la base de datos.
ZLATITUDE	Latitud geográfica de la ubicación de la empresa.
ZLONGITUDE	Longitud geográfica de la ubicación de la empresa.

Campo	Descripción
ZADDRESS	Dirección de la empresa.
ZBUSINESSDESCRIPTION	Descripción de la empresa.
ZEMAIL	Correo electrónico de la empresa.
ZJID	Identificador "lid" de la empresa. Como excepción, se ha detectado que registra el identificador "jid" del asistente "Meta AI". El valor que se corresponde con el valor del campo " ZJID " de la tabla " ZWABIZVERIFIEDNAMEDATA ", permitiendo vincular ambas tablas. Ejemplo: 213305759113335@lid (identificador "lid" de una empresa). 13135550002@s.whatsapp.net (identificar "jid" de Meta AI).
ZMEMBERSINCE	Fecha en la que la empresa es miembro de WhatsApp Business.
ZTIMEZONE	Zona horaria por la que se rige la empresa.
ZWEBSITES	Archivo bplist con la página web de la empresa.

*Ilustración 95. Descripción de los campos de la tabla
"ZWAAGGREGATECALLEVENT"*

5.1.2. ZWABIZVERIFIEDNAMEDATA

Tabla que registra los nombres e identificadores de las cuentas business.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor " 20 ", siendo el número de orden alfabético de la tabla en la base de datos.
ZJID	Identificador "lid" de la empresa. Como excepción, se ha detectado que registra el identificador "jid" del asistente "Meta AI". El valor que se corresponde con el valor del campo " ZJID " de la tabla " ZWABIZPROFILEDATA ", permitiendo vincular ambas tablas.

Campo	Descripción
ZNAME	Nombre de la empresa.
ZPHONENUM- BERJID	Identificador "lid" de la empresa.

*Ilustración 96. Descripción de los campos de la tabla
"ZWABIZVERIFIEDNAMEDATA"*

5.2. Base de datos *CallHistory.sqlite*

Esta base de datos registra la información relacionada con las llamadas o videollamadas del usuario de esta cuenta.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.
WhatsApp.shared/CallHistory.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/
CallHistory.sqlite**

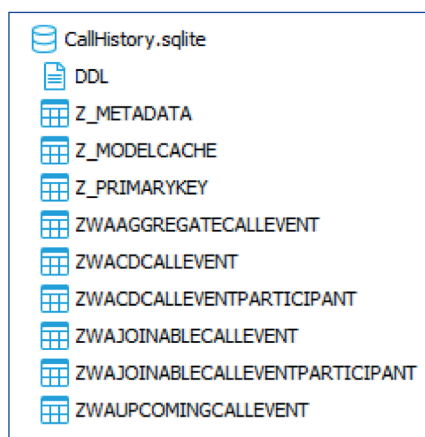


Ilustración 97. Tablas de la base de datos "CallHistory.sqlite"

5.2.1. ZWAAGGREGATECALLEVENT

Tabla que registra las características de las llamadas entrantes o salientes, llamadas de audio o vídeo, etc.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "1", siendo el número de orden alfabético de la tabla en la base de datos.
ZINCOMING	Si la llamada o videollamada la ha iniciado el usuario de esta cuenta se registra con el valor "0". En caso contrario, el valor es "1".
ZMISSED	Respuesta a una llamada: 0: llamada saliente desde esta cuenta, llamada entrante (individual o grupal) contestada por el usuario de esta cuenta o llamada individual rechazada por el usuario de esta cuenta. 1: llamada entrante (individual o grupal) no contestada por el usuario de esta cuenta o llamada entrante grupal rechazada por el usuario.
ZVIDEO	Si se trata de una videollamada el valor es "1" y en caso de una llamada de audio es "0".
ZFIRSTDATE	En llamadas individuales, fecha de la finalización de la llamada en formato UTC OS X Epoch. En llamadas grupales, fecha del inicio de la llamada en formato UTC OS X Epoch. <i>Si hay varios registros de llamadas de la tabla "ZWACD-CALLEVENT" vinculados a esta fila (a través del campo "Z1CALLEVENTS"), la fecha hará referencia a la primera llamada que se produjo.</i>
ZLINKTOKEN	Token cuando se transmite un enlace para unirse a una llamada.

Ilustración 98. Descripción de los campos de la tabla "ZWAAGGREGATECALLEVENT"

5.2.2. ZWACDCALLEVENT

Tabla que registra una fila por cada llamada o videollamada.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "2", siendo el número de orden alfabético de la tabla en la base de datos.
ZBYTESRECEIVED	Bytes recibidos en la comunicación.
ZBYTESENT	Bytes enviados en la comunicación.
ZISLIGHTWEIGHT	Tipo de comunicación: 0 : llamada o videollamada. 1 : chat de audio (chat grupal).
ZOUTCOME	Resultado de la llamada: 0 : llamada individual descolgada. En llamadas grupales, el usuario de esta cuenta ha mantenido una conversación al menos con un contacto del grupo. En chats de audio en grupo, el usuario se ha unido. 1 : llamada sin contestar. 4 : llamada individual rechazada por un participante. En llamadas grupales, el usuario de esta cuenta ha rechazado la llamada. 5 : llamada aceptada en otro dispositivo.
Z1CALLEVENTS	Este valor se corresponde con el del campo " Z_PK " de la tabla " ZWAAGGREGATECALLEVENT " permitiendo vincular ambas tablas.
ZDATE	En llamadas individuales, fecha de la finalización de la llamada en formato UTC OS X Epoch (El inicio se puede obtener del valor del campo " ZMESSAGEDATE " de la tabla " ZWAMESSAGE " de la base de datos " ChatStorage.sqlite "). En llamadas grupales, fecha del inicio de la llamada en formato UTC OS X Epoch.
ZDURATION	Duración en segundos de la comunicación.

Campo	Descripción
ZCALLIDSTRING	Identificador del mensaje generado por la llamada. Se corresponde con el valor del campo "ZSTANZAID" de la tabla "ZWAMESSAGE" de la base de datos "ChatStorage.sqlite" .
ZGROUPCALL-CREATORUSER-JIDSTRING	Identificador "jid" del creador de la llamada.
ZGROUPEJIDSTRING	En las llamadas grupales, el identificador "jid" del grupo.

*Ilustración 99. Descripción de los campos de la tabla **"ZWACDCALLEVENT"***

5.2.3. ZWACDCALLEVENTPARTICIPANT

Tabla que registra los participantes de las llamadas o videollamadas individuales salientes y entrantes, o grupales entrantes. No almacena información de comunicaciones grupales iniciadas por el usuario de esta cuenta. Tampoco registra datos de identificación del usuario de esta cuenta.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "3" , siendo el número de orden alfabético de la tabla en la base de datos.
ZOUTCOME	Resultado de la llamada individual: 0 : Llamada individual descolgada o llamada grupal (todas). 1 : llamada sin contestar. 4 : llamada individual rechazada por el contacto.
Z1PARTICIPANTS	Este valor se corresponde con el del campo "Z_PK" de la tabla "ZWAAGGREGATECALLEVENT" permitiendo vincular ambas tablas.

Campo	Descripción
ZJIDSTRING	Identificador "jid" del participante en la comunicación (nunca el del propio usuario). En llamadas individuales registra el identificador "jid" del contacto, independientemente del resultado de la llamada. En llamadas grupales entrantes, únicamente registra el identificador "jid" del contacto que haya realizado la llamada y del resto de contactos que hayan descolgado y mantenido la conversación (un registro por participante).

*Ilustración 100.Descripción de los campos de la tabla
"ZWACDCALLEVENTPARTICIPANT"*

5.3. Base de datos *ChatStorage.sqlite*

Base de datos que contiene la información referente a la transmisión de los mensajes a través de la aplicación. Sin duda alguna, es la base de datos más importante en la versión de WhatsApp para el sistema operativo iOS.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/ChatStorage.sqlite**

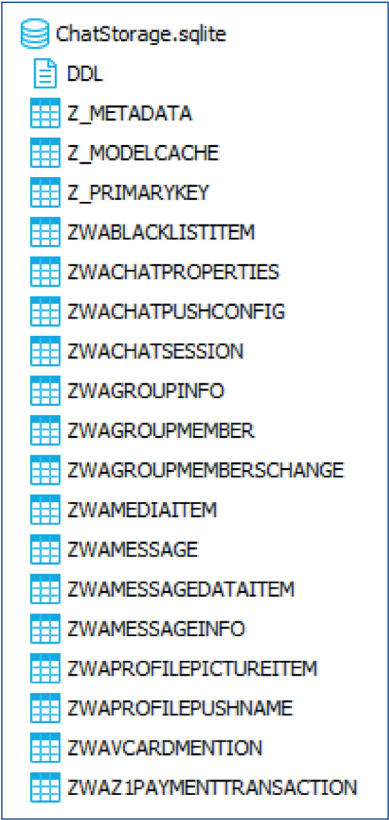


Ilustración 101. Tablas de la base de datos “**ChatStorage.sqlite**”

5.3.1. ZWABLOCKLISTITEM

Tabla que registra los contactos que han sido bloqueados.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor “1”, siendo el número de orden alfabético de la tabla en la base de datos.
ZJID	Identificador “jid” del contacto bloqueado.

Ilustración 102. Descripción de los campos de la tabla “**ZWABLOCKLISTITEM**”

5.3.2. ZWACHATPUSHCONFIG

Tabla que registra los chats (individuales, grupales o canales) que se encuentran con las notificaciones silenciadas.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "3", siendo el número de orden alfabético de la tabla en la base de datos.
ZMUTEDUNTIL	Fecha hasta la que se encontrará el chat silenciado en formato UTC OS X Epoch. La aplicación permite silenciar las notificaciones por 8 horas, 1 semana o siempre. Cuando se selecciona "siempre" el valor de este campo es "63113904000", que se traduce en la fecha 01/01/4001 0:00:00. Las notificaciones de los canales vienen por defecto silenciadas para "siempre".
ZJID	Identificador "jid" del chat que se encuentra silenciado.

Ilustración 103. Descripción de los campos de la tabla "ZWACHATPUSHCONFIG"

5.3.3. ZWACHATSESSION

Tabla que registra los chats creados con los diferentes contactos, grupos, difusiones, comunidades o canales.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "4", siendo el número de orden alfabético de la tabla en la base de datos.
ZARCHIVED	Si el chat está archivado en la cuenta analizada consta con valor "1". En caso contrario el valor es "0".

Campo	Descripción
ZHIDDEN	Si es un chat visible u oculto en la aplicación: 0: es visible (pestaña chat de la aplicación). 1: no es visible (el contacto se encuentra en la agenda del teléfono, pero no se ha iniciado ningún chat a través de la aplicación o ha sido eliminado el chat). Los grupos, difusiones, comunidades y canales a los que se pertenece siempre son “visibles” (0). Los estados del usuario siempre son “no visibles” (1).
ZMESSAGE-COUNTER	Contador de mensajes de este chat. Son la suma de todos los mensajes transmitidos en este chat menos uno. No afecta al contador la eliminación de mensajes.
ZSESSIONTYPE	Tipo de conversación: 0: chat individual. 1: chat grupal (incluido el grupo “Avisos” y “General” de una comunidad). 2: broadcast (difusiones y estados del usuario de esta cuenta). 3: estados de los contactos del usuario de esta cuenta. 4: comunidad. 5: canal.
ZSPOTLIGHTS-TATUS	-5: chats privados, difusiones, estados o canales. 1: chats grupales o comunidades.
ZUNREADCOUNT	Número de mensajes sin leer por el usuario de esta cuenta.
ZGROUPINFO	Valor del grupo que se corresponde con el campo “ Z_PK ” de tabla “ ZWAGROUPINFO ” y permite vincular ambas tablas.
ZLASTMESSAGE	Identificador del último mensaje transmitido en el chat.
ZLASTMESSAGE-DATE	Fecha del último mensaje transmitido en el chat en formato UTC OS X Epoch.
ZCONTACTIDENTIFIER	Fecha de creación del canal en formato UTC Unix Epoch (microsegundos). 1: contactos incluidos en la agenda. Vacío: difusiones, grupos y comunidades y usuarios desconocidos.

Campo	Descripción
ZCONTACTJID	Identificador "jid" del contacto, grupo, comunidad, canal, etc de WhatsApp con el que se mantiene el chat. Ejemplos: 34646222111@s.whatsapp.net ("jid" de contacto). 34646222111@status ("jid" del estado de contacto). 34699888777-1379114707@g.us ("jid" de grupo en formato antiguo). 120363080564732172@g.us ("jid" de grupo en formato actual o comunidad). 1690524142@broadcast ("jid" de difusión). 120363165396843331@newsletter ("jid" de canal).
ZLASTMESSAGE-GETEXT*	Archivo protobuf codificado en Base64. Entre la información que contiene se encuentra el identificador del último mensaje enviado por el usuario de esta cuenta, <i>incluso si el usuario eliminó el mensaje</i> , aunque no se registra la fecha de envío.
ZPARTNERNAME	Nombre del contacto, grupo, difusión, comunidad o canal.
ZSAVEDINPUT	Archivo de tipo JSON que almacena el texto de un mensaje en "borrador", así como la fecha en la que se escribió en formato UTC Unix Epoch (segundos).

Ilustración 104. Descripción de los campos de la tabla "ZWCHATSESSION"

* ZLASTMESSAGEGETEXT: almacena un archivo protobuf que tras ser decodificado informa sobre las características de los chats, como son la aplicación de temporalidad a los mensajes, privacidad avanzada del chat, o el primer y último mensaje del usuario en chats individuales:

Campo	Campo	Descripción
2		Temporalidad aplicada actualmente a los mensajes de este chat en segundos. Si no aparece este campo, actualmente no tiene temporalidad los mensajes.
3		Fecha en la que se estableció la temporalidad aplicada actualmente al chat en formato UTC Unix Epoch (segundos)

Campo	Campo	Descripción
5 (tantos campos como diferentes temporalidades se hayan asignado a este chat. El primer campo será la temporalidad asignada más antigua)	1	Temporalidad aplicada a los mensajes en segundos.
13		Identificador "ZSTANZAID" del primer mensaje enviado por el usuario de esta cuenta en el chat.
26 (último mensaje enviado por el usuario)	1	Identificador "jid" del chat.
	3	Identificador "ZSTANZAID" del último mensaje enviado por el usuario de esta cuenta en el chat.
65		Fecha de inicio de este chat en formato UTC Unix Epoch (segundos)
74		Privacidad avanzada del chat: 0 : desactivada 1 : activada
76		Fecha en la que se activó o desactivó la "Privacidad avanzada del chat" en formato UTC Unix Epoch (milisegundos).

Ilustración 105. Archivo protobuf del campo "ZLASTMESSAGETEXT" de la tabla "ZWCHATSESSION"

5.3.4. ZWAGROUPINFO

Tabla que registra información de la creación de grupos, comunidades y canales.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "5", siendo el número de orden alfabético de la tabla en la base de datos.

Campo	Descripción
ZSTATE	Estado del usuario en el grupo: 0 : el usuario de esta cuenta pertenece al grupo. 5 : el usuario de esta cuenta salió o fue expulsado del grupo.
ZCHATSESSION	Valor que se corresponde con el campo " Z_PK " de la tabla " ZWCHATSESSION " y permite vincular ambas tablas.
ZCREATIONDATE	Fecha de creación del grupo en formato UTC OS X Epoch.
ZCREATORJID	Identificador "lid" del creador del grupo o comunidad. Vacío : canales.
ZPICTUREID*	Archivo protobuf con la información de las características y permisos del grupo o canal, codificado en Base64 (para decodificarlo es necesario eliminar el carácter "+" inicial).
ZPICTUREPATH	En canales, archivo protobuf con la ruta parcial en la que se encuentra la imagen del perfil codificado en Base64 (para decodificarlo es necesario eliminar el carácter "*" inicial).
ZSOURCEJID	Identificador "lid" del creador del grupo o comunidad. Vacío : canales, o cuando el creador del grupo o comunidad sea el usuario de esta cuenta.
ZSUBJECTOWNERJID	Identificador "lid" del propietario del grupo o comunidad. En canales el campo se encuentra vacío.

Ilustración 106. Descripción de los campos de la tabla "ZWAGROUPINFO"

*ZPICTUREID: almacena un archivo protobuf que tras ser decodificado informa sobre las características de los grupos o canales:

Campo	Campo	Descripción
1	2	Fecha en la que se estableció la descripción del grupo o canal en formato UTC Unix Epoch (segundos).
	3	Descripción del grupo o el canal
2	1	Gestión por el administrador de la opción " Editar los ajustes del grupo " para los miembros del grupo: 1 : Está desactivada la edición. 0 : Está activada la edición. Si no existe este campo, por defecto es " 0 ".

Campo	Campo	Descripción
2	2	Fecha en la que un administrador activó o desactivó para los miembros del grupo la opción "Editar los ajustes del grupo" en el grupo en formato UTC Unix Epoch (segundos).
	3	Gestión por el administrador de la opción "Enviar mensajes" para los miembros del grupo: 1: Está desactivado el envío. 0: Está activado el envío. Si no existe este campo, por defecto es "0" .
	7	Fecha en la que se cambió la opción de temporalidad en los mensajes del grupo en formato UTC Unix Epoch (segundos).
	8	Fecha en la que un administrador desactivó para los miembros del grupo la opción "Enviar mensajes" en formato UTC Unix Epoch (milisegundos).
	13	Gestión por el administrador de la opción "Añadir a otros miembros" para los miembros del grupo: 1: Está desactivado añadir. 0: Está activado añadir.
	14	Fecha en la que un administrador activó o desactivó, para los miembros del grupo, la opción "Añadir a otros miembros" en el grupo en formato UTC Unix Epoch (segundos).
	15	administrador de la opción "Aprobar miembros nuevos" . Los administradores deberán aprobar a cualquier persona que quiera unirse al grupo: 1: Está activado. 0: Está desactivado.
	16	Fecha en la que un administrador activó o desactivó, para los miembros del grupo, la opción "Aprobar a otros miembros" en el grupo en formato UTC Unix Epoch (segundos).
4		Identificador "jid" del creador del grupo.
6		Fecha en la que se asignó al último administrador en formato UTC Unix Epoch (milisegundos). Fecha en la que usuario abandonó o fue expulsado del grupo en formato UTC Unix Epoch (miliseg.). (En caso de que se den los dos supuestos, el segundo tiene prioridad sobre el primero)
20		Número de seguidores del canal.

Campo	Campo	Descripción
30 (tantos campos como seguidores tenga el canal del usuario)	1	Identificador "lid" del seguidor del canal administrado por el usuario. En canales que siga el usuario no existe ese campo.

Ilustración 107. Archivo protobuf del campo "ZPICTUREID" de la base de datos "ZWAGROUPINFO"

5.3.5. ZWAGROUPMEMBER

Tabla que registra los miembros de los grupos, comunidades o difusiones. También registra la opción predeterminada que el usuario ha asignado a cada contacto respecto a la posibilidad de recibir sus actualizaciones de estado.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "6", siendo el número de orden alfabético de la tabla en la base de datos.
ZISACTIVE	Define si un contacto está activo en el chat registrado en el campo "ZCHATSESSION". 1 : activo. 0 : inactivo. Por ejemplo, si un usuario ha pertenecido a un grupo, pero actualmente no lo es, aparecerá en esta tabla, pero como inactivo. Cuando el usuario de esta cuenta actualiza con mensaje/s su estado (status@broadcast), todos los contactos almacenados en la agenda del usuario son potenciales receptores del mensaje y tendrán una entrada en este registro, pero debido a la posibilidad de privacidad que proporciona la aplicación, solo considerará como contacto activo a los que "puede ver mi estado".

Campo	Descripción
ZISADMIN	El miembro identificado en el campo " ZMEMBERJID " es administrador del grupo o comunidad. 1 : cierto. 0 : falso.
ZCHATSESSION	Identificador del grupo, comunidad, lista de difusión o estados del usuario en el que se encuentra el contacto del siguiente campo. El valor se corresponde con el campo " Z_PK " de la tabla " ZCHATSESSION ", permitiendo vincular ambas tablas.
ZMEMBERJID	Identificador "jid" o "lid" de un contacto o del usuario de esta cuenta.

*Ilustración 108. Descripción de los campos de la tabla "**ZWAGROUPMEMBER**"*

5.3.6. ZWAGROUPMEMBERSCHANGE

Tabla que registra los cambios que se ha producido en los grupos.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor " 7 ", siendo el número de orden alfabético de la tabla en la base de datos.
ZCHANGETYPE	Tipo de cambio que se ha producido en el grupo: 4 : el miembro ha sido eliminado del grupo por un administrador. 5 : el miembro ha abandonado el grupo.
ZCHANGEDATE	Fecha en formato UTC OS X Epoch en el que se produjo el cambio.
ZGROUPJID	Identificador "jid" del grupo al que le afecta el cambio.
ZMEMBERJIDS	Identificador "jid" del usuario o del contacto que ha sufrido el cambio.

*Ilustración 109. Descripción de los campos de la tabla "**ZWAGROUPMEMBERSCHANGE**"*

5.3.7. ZWAMEDIAITEM

Tabla que registra información sobre los archivos (notas de voz, notas de vídeo, archivos de audio/vídeo, documentos, etc.) intercambiados entre el usuario y sus contactos, grupos...

No siempre se graban todos los campos, como por ejemplo la ruta o el nombre del archivo transmitido cuando no se ha descargado el archivo, o es de visualización única y ha sido eliminado.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "8", siendo el número de orden alfabético de la tabla en la base de datos.
ZFILESIZE	Tamaño del archivo transmitido en bytes.
ZMEDIAORIGIN	0: demás casos. 1: notas de voz o ubicación en tiempo real. 3: gif de la librería de la aplicación en Android. 4: gif de la librería de la aplicación en iOS.
ZMOVIEDURATION	Duración de los ficheros multimedia en segundos o páginas en documentos.
ZMESSAGE	Valor del campo "Z_PK" de la tabla "ZMESSAGE" en el cual se transmitió este archivo, que permite vincular ambas tablas.
ZLATITUDE	Latitud inicial cuando se transmite ubicación. Resolución horizontal (píxeles) en imágenes y vídeos.
ZLONGITUDE	Longitud inicial cuando se transmite ubicación. Resolución vertical (píxeles) en imágenes y vídeos.
ZMEDIAURLDATE	Fecha en la que se subió el archivo al servidor de WhatsApp y se generó la URL en formato UTC OS X Epoch. Fecha prevista para la finalización de la transmisión de la ubicación en tiempo real en formato UTC Unix Epoch (microsegundos), cuando se recibe la ubicación de un contacto.
ZAUTHORNAME	Nombre o título del archivo transmitido como documento. Fecha en la que se inició la transmisión de la ubicación en tiempo real en formato UTC Unix Epoch (microsegundos), cuando se recibe la ubicación de un contacto.

Campo	Descripción
ZMEDIALOCAL-PATH	Ruta parcial y nombre del archivo en el que se encuentra o se ha encontrado almacenado el archivo en este dispositivo.
ZMEDIAURL	URL en el que se encontraba el archivo transmitido. URL de un "lugar cercano" cuando se transmite a través de un mensaje de ubicación.
ZTITLE	Texto añadido al mensaje con el archivo transmitido. En mensajes eliminados "para todos" es el valor de identificación del mensaje previo a de ser eliminado, que se registró en el campo " ZSTANZAID " de la tabla " ZWAMES-SAGE ".
ZVCARDNAME	Cuando se ha transmitido una tarjeta de contacto, es el nombre del contacto. Si se ha transmitido un archivo, es el hash SHA256 del archivo codificado en Base64. Cuando el archivo se lo ha enviado el usuario de esta cuenta a sí mismo estará vacío. En caso de que se haya eliminado un mensaje "para todos", es el identificador "jid" del chat individual o grupal en el que se produjo el borrado. Cuando se transmite la ubicación de un "lugar cercano", es el nombre del lugar.
ZVCARDSTRING	Cuando se ha transmitido una tarjeta de contacto, es la información que contiene del contacto. Si se ha recibido ubicación en tiempo real, es la "latitud final;longitud final;tiempo en segundos que se ha compartido la ubicación". Cuando se trata de un archivo, es el tipo MIME. Ejemplo: image/jpeg; video/mp4, audio/ogg.... En caso de que se haya eliminado un mensaje "para todos" en un grupo, es el identificador "jid" del contacto que envió el mensaje, siempre que no haya sido el usuario de esta cuenta, caso en el que se encontrará vacío.
ZXMPPTHUMB-PATH	Ruta parcial en la que se encuentra almacenado la miniatura o thumbnail en el teléfono cuando se trata de la transmisión de una imagen, vídeo, gif o un pdf.
ZMEDIAKEY	Archivo protobuf con la llave de cifrado.
ZMETADATA*	Archivo protobuf con metadatos del fichero transmitido.

Ilustración 110. Descripción de los campos de la tabla "ZWAMEDIAITEM"

*ZMETADATA: almacena un archivo protobuf que, tras ser decodificado, presenta información de mensajes reenviados, citados o mensajes temporales conservados. Existen campos que son comunes para diferentes tipos de mensajes, pero también hay campos que son específicos por el tipo de mensaje. Primero se describen los campos comunes y posteriormente los específicos que determinan el tipo de mensaje. Que sean comunes únicamente indica que se pueden presentar en todo tipo de mensaje, pero lo más habitual es que solo se muestren unos pocos campos dependiendo de cada caso.

Campos comunes:

Campo	Campo	Descripción
4		URL parcial en la que se encuentra el archivo del mensaje.
5		Identificador del mensaje que ha sido citado.
6		identificador "jid" del emisor del mensaje que ha sido citado. Cuando el mensaje citado es el usuario de esta cuenta no se encontrará este campo.
29		Temporalidad aplicada al mensaje.
32	4	Fecha en la que se transmitió el mensaje que cita otro mensaje en formato UTC Unix Epoch (milisegundos)
33		Fecha en la que se envió el mensaje en formato UTC OS X Epoch.
35		Fecha en la que se cambió la temporalidad de los mensajes en el chat en formato UTC Unix Epoch (Segundos)
47	3	Resolución horizontal (píxeles) del thumbnail señalado en el campo "47-8".
	4	Resolución vertical (píxeles) del thumbnail señalado en el campo "47-8".
	6	Hash SHA256 del thumbnail señalado en el campo "47-8".
	8	Ruta parcial en el dispositivo en el que se encuentra el thumbnail del archivo pdf que se encuentra en el mensaje.

Ilustración 111. Archivo protobuf del campo "ZMETADATA" de la tabla "ZWAMEDIAITEM"

La existencia del campo indica el tipo de mensaje:

Campo	Descripción (tipo de mensaje específico)
17	Mensaje reenviado.
19	Mensaje que cita otro mensaje.
66	Mensaje temporal conservado.
74	Transcripción de nota de voz.
159	Opción de "Privacidad avanzada del chat".

Ilustración 112. Archivo protobuf del campo "ZMETADATA" de la tabla "ZWAMEDIAITEM"

5.3.8. ZWMESSAGE

Esta tabla es la columna vertebral de la aplicación. Contiene información primordial de los mensajes enviados, recibidos y mensajes del sistema, como son fechas de transmisión, contenido en texto, tipo de mensaje (texto, audio, archivo de vídeo, encuesta...), tipo de dispositivo que ha emitido el mensaje, etc.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "9", siendo el número de orden alfabético de la tabla en la base de datos.
ZCHILDMESSAGESREADCOUNT	Número de contactos que han leído el estado publicado por el usuario de esta cuenta.
ZFILTEREDRECIPIENTCOUNT	Número de contactos que han recibido el estado publicado por el usuario de esta cuenta.
ZGROUPEVENT-TYPE	Tipo de evento. Ejemplos de acciones que generan mensajes del sistema: 1: creación de un canal (que sigue el usuario o creado por éste). 2: "Los mensajes y las llamadas están cifradas de extremo a extremo. Nadie fuera de este chat, ni siquiera WhatsApp, puede leerlos ni escucharlos. Toca para obtener más información". Es un mensaje del sistema cuando se inicia un chat.

Campo	Descripción
ZGROUPEVENT-TYPE	3: "xxxxx salió del grupo". 7: "xxxx te eliminó del grupo." 8: "Creaste una lista de difusión". 10: "Ahora eres admin. del grupo.". Otro administrador ha asignado como administrador del grupo al usuario. 12: "Creaste este grupo" o xxxxx te añadió". Cuando se crea un grupo 18: "(Cambiaste o xxxxx cambió) los ajustes para que solo los administradores puedan editar las opciones de grupo." 19: "(Cambiaste o xxxxx cambió) los ajustes para que todos los miembros puedan editar las opciones de grupo" 20: (Cambiaste o xxxx cambió) los ajustes de este grupo para permitir que solo quienes lo administran puedan enviar mensajes al grupo". 23: "(Activaste o xxxx activó) los mensajes temporales. Los mensajes nuevos desaparecerán de este chat después de xx horas/días después de haber sido enviados, a menos que se use la opción para conservarlos." o "(Desactivaste o xxxx desactivó) los mensajes temporales. Se puede aplicar en chats individuales. 26: "(Se activaron, activaste o xxxx activó) los mensajes temporales. Los mensajes nuevos desaparecerán de este chat después de xx horas/días después de haber sido enviados, a menos que se use la opción para conservarlos.". Se puede aplicar en chat grupales. 33: "(Actualizaste o xxxx actualizó" la duración de los mensajes. Los mensajes nuevos desaparecerán de este chat después de xxxx horas/días después de haber sido enviados, a menos que se use la opción para conservarlos." 34: "bloqueaste a este contacto." 35: "desbloqueaste a este contacto." 36: "(Activaste o xxxx activó) la aprobación de los admin. para unirse a este grupo."

Campo	Descripción
ZGROUPEVENT-TYPE	42: "(Cambiaste o xxxx cambió) los ajustes de este grupo para permitir que solo quienes lo administran puedan añadir a otros miembros." 43: "(Usas una duración predeterminada para los mensajes temporales en chats nuevos o Se activaron los mensajes temporales). Los mensajes nuevos desaparecerán de este chat después de xx horas/días de haber sido enviados, a menos que se use la opción para conservarlos." o "Se activaron los mensajes temporales. Los 44: "xxxx usa una duración predeterminada para los mensajes temporales en chats nuevos. Los mensajes nuevos desaparecerán de este chat después de xx horas/días de haber sido enviados, a menos que se use la opción para conservarlos.". Se puede aplicar en chat individuales. 51: mensaje del sistema cuando se crea una comunidad. 58: "(Fijaste o xxxx fijó) un mensaje." 60: "(Añadiste o xxxxx te añadió) a un grupo en la comunidad "nombre de la comunidad". Se ha añadido a un grupo que pertenece a una comunidad.
ZISFROMME	Dirección del mensaje: 0: mensaje recibido por el usuario de esta cuenta. 1: mensaje enviado por el usuario de esta cuenta. Existe la excepción de los mensajes del sistema ("ZMESSAGE-TYPE" = "6" o "10"), todos los cuales tendrán siempre el valor "0". Parece contradictorio que todos los mensajes del sistema consten como recibidos, aunque al generarse todos los mensajes en el iPhone, el identificador del mensaje "ZSTANZAID" será el que corresponde a este tipo de dispositivos (20 caracteres hexadecimales, empezando por "3A")
ZMESSAGE-RRORSTATUS	Fecha prevista para la eliminación de este mensaje temporal, en formato UTC OS X Epoch. Cuando es un valor negativo, el mensaje se ha conservado. Reconvirtiendo el valor en positivo, era la fecha en la que estaba prevista su eliminación en formato UTC OS X Epoch. 0: mensaje no temporal.

Campo	Descripción
ZMESSAGESTATUS	Estado de la entrega/recepción en el que se encuentra el mensaje (ver apartado 8.3.2 Mensajes enviados y recibidos (iOS)): <u>Mensajes enviados:</u> 9 o 3: mensaje enviado no ha salido del dispositivo (falta de conexión). 1: mensaje enviado entregado al servidor. 6: mensaje entregado a su destinatario. 8: mensaje abierto en el chat del contacto (considerado "leído"). 5: nota de voz o mensaje de visualización única reproducido por el contacto. <u>Mensajes recibidos:</u> 6: mensaje recibido. 8: mensaje abierto por el usuario de esta cuenta. 4: nota de vídeo reproducida por el usuario de esta cuenta. 5: nota de voz o mensaje de visualización única reproducido por el usuario de esta cuenta.
ZMESSAGETYPE	Tipo de mensaje: 0: mensaje de texto. 1: imagen. 2: vídeo. 3: nota de voz o archivo de audio. 4: tarjeta de contacto. 5: ubicación en tiempo real o ubicación actual 6: mensaje de sistema. 7: enlace a una URL. 8: documento (pdf, docx, xlsx...). 10: mensaje del sistema. 11: gif. 14: mensaje individual o grupal eliminado para todos participantes. 15: sticker o avatar.

Campo	Descripción
ZMESSAGE TYPE	28: se ha cambiado la temporalidad de los mensajes en chat individual. 38: imagen de visualización única. 39: vídeo de visualización única. 46: encuesta. 53: nota de voz de visualización única. 54: nota de vídeo. 55: mensaje del sistema cuando se crea un canal. Cuando el usuario crea un canal o cuando empieza a seguir un canal: "Este canal ofrece mayor privacidad para tu perfil y número de teléfono", "Este canal es público y visible para cualquiera, incluido WhatsApp. Tu perfil y número de teléfono tienen más privacidad" "Se creó el canal "xxxx"". 58: feedback (positivo o negativo del desempeño del bot de Meta AI enviado por el usuario. 59: llamada, videollamada o chat de audio. 62: mensaje del sistema cuando el usuario crea un canal. "Para comenzar, escribe tu primera actualización e invita a las personas con tu enlace". 63: evento. 66: álbum multimedia (mensaje con varios archivos de imagen y/o vídeo). 68: mención de un contacto en el "Estado" del usuario de esta cuenta o viceversa. 73: mensaje del sistema por la activación o desactivación de la privacidad avanzada del chat individual.
ZSORT	Número de posición del mensaje en el chat al que pertenece. Si un mensaje es eliminado, su número de posición se mantendrá y por tanto quedarán saltos de posición entre mensajes.
ZSPOTLIGHTS-TATUS	Se desconoce la función de este campo, pero sus valores están asociados a diferentes tipos de mensajes: 2: mensajes enviados por los contactos a sus respectivos estados. 3: mensajes enviados por el usuario a su estado. 7: mensajes enviados por canales que sigue el usuario. 8: mensajes enviados por el usuario a sus canales. -32768: otros mensajes.

Campo	Descripción
ZSTARRED	Mensaje destacado por el usuario de esta cuenta: vacío : no destacado 0 : mensaje que no puede ser destacado (se encuentra eliminado, "ZMESSAGETYPE" = "14") 1 : mensaje destacado
ZCHATSESSION	Chat al que pertenece el mensaje. Se corresponde con el valor del campo " Z_PK " de la tabla " ZWCHATSESSION ", permitiendo vincular ambas tablas.
ZGROUPMEMBER	Contacto que envió el mensaje al grupo (si es el usuario de esta cuenta se encontrará vacío). El valor se corresponde con el campo " Z_PK " de la tabla " ZWAGROUPMEMBER ", permitiendo vincular ambas tablas.
ZLASTSESSION	Cuando es el último mensaje transmitido en el chat en base a la fecha del campo " ZMESSAGEDATE " muestra el mismo valor que el campo " ZCHATSESSION ". Si no es el último mensaje de este chat, el campo se encuentra vacío.
ZMEDIAITEM	El valor se corresponde con el campo " Z_PK " de la tabla " ZWAMEDIAITEM ", permitiendo vincular ambas tablas.
ZMESSAGEINFO	El valor se corresponde con el campo " Z_PK " de la tabla " ZWAMESSAGEINFO ", permitiendo vincular ambas tablas.
ZPARENTMESSAGE	En las difusiones, el valor corresponde con el número de mensaje "padre" en el campo " Z_PK " de esta tabla. Partiendo de la sesión de chat con el mensaje "padre", se puede identificar la difusión concreta a través de la cual se envió el mensaje a los contactos en la tabla " ZWACHATSESSION ".
ZMESSAGEDATE	Fecha de envío del mensaje por el usuario de esta cuenta o por el contacto en formato OS X Epoch. Fecha de inicio de llamada o videollamada en formato OS X Epoch.
ZSENTDATE	<u>Mensaje enviado</u> : fecha de envío del mensaje en formato OS X Epoch. <u>Mensaje recibido</u> : fecha de recepción del mensaje en este dispositivo en formato OS X Epoch. Vacío en llamadas/videollamadas, mensajes del sistema y cambios de temporalidad en chats individuales.

Campo	Descripción
ZFROMJID	Identificador "jid" o "lid" del contacto (chat individual) o del grupo emisor del mensaje cuando se recibe. En caso de ser enviado por el usuario se encuentra vacío.
ZMEDIASECTIONID	Registra el año y el mes en el que fue transmitido un archivo multimedia. Cuando se transmite un documento, además se le añade el prefijo "doc". Ejemplo: doc-2024-12 Cuando el usuario crea un evento, el valor es el texto "event-" junto con la fecha en la que se iniciará el evento en formato UTC Unix Epoch. Ejemplo: event-1725224400000 En cualquier otro caso se encuentra vacío.
ZPUSHNAME	Archivo protobuf codificado en Base64 con información del mensaje transmitido: Mensajes enviados: identificador "jid" del usuario y la fecha de envío en formato UTC Unix Epoch (segundos). Mensajes recibidos: fecha de recepción en formato UTC Unix Epoch (segundos). En algunos mensajes de visualización única el campo se encuentra vacío. En mensajes editados, conserva metadatos del mensaje original (ver apartado 9.1.1 <i>Mensajes editados</i>).
ZSTANZAID	El identificador del mensaje, que es una secuencia que varía desde 9 caracteres hexadecimales hasta 32. Se puede identificar el tipo de dispositivo que envió un mensaje dependiendo del número de caracteres y/o los caracteres por los que empiece el "ZSTANZAID": 18 caracteres hexadecimales: <u>se envió</u> a través de la versión de la aplicación para Windows o Wear OS. 20 caracteres hexadecimales, empezando por la secuencia: 3EBO <u>se envió</u> el mensaje a través de la versión WEB. 3A <u>se envió</u> el mensaje a través de versión de la aplicación para iOS, iPadOS o la versión para macOS. 5E <u>se envió</u> el mensaje a través de versión de la aplicación para iOS. 30 o 32 caracteres hexadecimales: <u>se envió</u> el mensaje a través de la versión para dispositivos Android.

Campo	Descripción
ZTEXT	Contenido del mensaje de texto (exclusivamente en mensajes de texto). No mostrará el texto de cualquier otro tipo de mensaje que tenga texto añadido (como imágenes, vídeos...), el cual se encontrará en el campo "ZTITLE" de la tabla "ZWAMEDIAITEM". En algunos mensajes del sistema (ZMESSAGE TYPE = "6" o "10") puede contener la siguiente información: Cuando se crea un grupo con temporalidad asignada a los mensajes o se modifica manualmente la temporalidad de los mensajes en un grupo ("ZGROUPEVENTTYPE" = "26") el campo registra la temporalidad aplicada en segundos. Si se suprime la temporalidad el campo se encontrará vacío. Identificador "jid" del usuario o contacto que ha realizado la acción que ha generado el mensaje del sistema (ejemplo: administrador de grupo que elimina a un miembro). Un archivo tipo json con información del suceso.
ZTOJID	Identificador único "jid" del contacto, grupo, etc., receptor del mensaje WhatsApp. Cuando es un mensaje publicado en el estado del usuario de esta cuenta es el valor del propio usuario: status@broadcast. Cuando el usuario de esta cuenta se envía un mensaje a sí mismo o es un mensaje del sistema (ZMESSAGE TYPE= 6 o 10), se muestra el identificador "jid" del propio usuario.

Ilustración 113. Descripción de los campos de la tabla **"ZWMESSAGE"**

5.3.9. ZWMESSAGEDATAITEM

Tabla que registra información sobre mensajes en los que se ha adjuntado un enlace a una URL. Esta URL puede dirigir a páginas web o puede ser enlace de llamada/videollamada, invitación para unirse a un canal de WhatsApp, etc.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).

Campo	Descripción
Z_ENT	Valor " 10 ", siendo el número de orden alfabético de la tabla en la base de datos.
ZMESSAGE	Valor que se corresponde con el del campo " Z_PK " de la tabla " ZWAMESSAGE " y permite determinar el mensaje en el que se envió el enlace.
ZDATE	Fecha de la transmisión del enlace en formato UTC OS X Epoch.
ZCHATJID	Valor que se corresponde con el del campo " Z_PK " de la tabla " ZWACHATSESSION " precedido del carácter " p " y permite determinar el identificador "jid" y nombre del contacto, grupo, canal o difusión en el que se transmitió el enlace.
ZCONTENT1	URL del enlace. Contiene el token cuando es una llamada/videollamada. Ejemplo: https://call.whatsapp.com/voice/nXVEf3rZZaJYAnzyxx-vuXN
ZMATCHEDTEXT	La misma URL que en el campo anterior.
ZSECTIONID	Año y mes de la transmisión del enlace.
ZSUMMARY	Resumen del contenido al que dirige el enlace. En la interfaz gráfica de la aplicación, dentro del mensaje, se muestra debajo del título del enlace (ZTITLE). Ejemplo: "Enlace de llamada de WhatsApp"
ZTHUMBNAIL-PATH	Ruta parcial en el sistema de archivos del dispositivo en el que se encuentra la miniatura o thumbnail que se muestra junto con el enlace.
ZTITLE	Título del enlace. Ejemplos: "Llamada de WhatsApp" o "Videollamada de WhatsApp".

*Ilustración 114. Descripción de los campos de la tabla
"ZWAMESSAGEDATAITEM"*

5.3.10. ZWAMESSAGEINFO

Tabla que registra información relevante sobre los mensajes transmitidos, principalmente enviados.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "11", siendo el número de orden alfabético de la tabla en la base de datos.
ZMESSAGE	Valor que se corresponde con el campo "Z_ENT" de la tabla "ZWAMESSAGE", permitiendo vincular ambas tablas y obtener el identificador del mensaje.
ZRECEIPTINFO*	Archivo de tipo protobuf con información del mensaje. En los mensajes del sistema y en la mayoría de los mensajes recibidos se encuentra vacío.

Ilustración 115. Descripción de los campos de la tabla "ZWAMESSAGEINFO"

*ZRECEIPTINFO: Tras ser decodificado se observan campos que pueden contener información de diferentes tipos mensajes. Lo más habitual es que solo se muestren unos pocos campos de los que se describen dependiendo del mensaje:

Campo	Campo		Descripción
2 Hay tantos campos 2 como receptores del mensaje	1		Número de teléfono del contacto que ha recibido el mensaje precedido del número "81" y finalizado con el carácter "f". Ejemplo: 81 34633456456f
	7 (sólo observado en mensajes publicados en el estado del usuario)		Nombre del contacto con el que está grabado en la agenda del usuario. Si se trata del mismo usuario, será referido como "Tú".
	9 Hay tantos campos 2-9 como dispositivos	1	Número de dispositivo al que se ha enviado el mensaje, pero no lo ha recibido
	10 Hay tantos campos 2-10 como dispositivos ³	1	Número de dispositivo que ha recibido el mensaje.
7 (reacción al mensaje)	1 (un contacto ha reaccionado) Hay tantos campos 7-1 como contactos reaccionen al mensaje.	1	Identificador del mensaje de reacción del contacto al mensaje.
		2	Identificador "jid" del contacto que ha reaccionado al mensaje.
		3	Emoji de reacción.
		4	Fecha en la que se produjo la reacción al mensaje en formato UTC Unix Epoch (milisegundos)

³ Excepto el dispositivo principal del usuario de esta cuenta, aunque lo reciba no se registra.

Campo	Campo		Descripción
7 (reacción al mensaje)	2 (el usuario de esta cuenta ha reaccionado)	1	Identificador del mensaje de reacción de este usuario al mensaje.
		2	Emoji de reacción.
		3	Fecha en la que se produjo la reacción al mensaje en formato UTC Unix Epoch (milisegundos)
	3 (un seguidor del canal ha reaccionado a un mensaje del canal) Hay tantos campos 7-3 como reacciones al mensaje del canal.	1	Emoji de reacción.
8 (encuesta)	2		Pregunta de la encuesta
	3 Hay tantos campos 8-3 como opciones de respuesta tenga la encuesta	1	Respuesta (opción de respuesta).
8 (encuesta)	4		Número de respuestas que se permite por participante: 0 : varias. 1 : una.

Campo	Campo		Descripción
8 (encuesta)	5 (respuesta del contacto) Hay tantos campos 8-5 como contactos hayan respondido a la encuesta	1 (Elección de respuesta) Hay tantos campos 8-5-1 como respuestas haya elegido el contacto	El valor que presenta la opción elegida por el usuario. El valor "0" es la primera respuesta posible, que se encuentra en primer el campo 8-3-1, el valor "1" se corresponde con el segundo campo 8-3-1. Así sucesivamente.
		2	Fecha de la respuesta en formato UTC Unix Epoch (milisegundos). Si hay más de una repuesta, corresponde a la última.
		4	Identificador "jid" del contacto que ha respondido en la encuesta
		5	Fecha de la respuesta en formato UTC Unix Epoch (milisegundos).
	6 (respuesta del usuario de esta cuenta)	1	El valor que presenta la opción elegida por el usuario. El valor "0" es la primera respuesta posible, que se encuentra en primer el campo 8-3-1, el valor "1" se corresponde con el segundo campo 8-3-1. Así sucesivamente.
		2	Fecha en formato UTC Unix Epoch (milisegundos).

Ilustración 116. Archivo protobuf del campo "ZRECEIPTINFO" de la tabla "ZWMESSAGEINFO"

5.3.11. ZWAPROFILEPICTUREITEM

Tabla que registra datos sobre las imágenes de perfil del usuario, contactos, grupos, comunidades y canales.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "12" , siendo el número de orden alfabético de la tabla en la base de datos.
ZREQUESTDATE	Fecha en formato UTC OS X Epoch en la que la aplicación ha consultado en sus servidores la imagen de perfil del contacto, grupo, comunidad o canal.
ZJID	Identificador único "jid" del contacto, grupo, etc., de WhatsApp.
ZPATH:	Ruta parcial en el sistema de archivos del dispositivo en la que se encuentra almacenada la imagen del perfil del contacto, grupo, comunidad o canal.
ZPICTUREID:	Fecha en el que se estableció la imagen de perfil: En contactos en formato UTC Unix Epoch (segundos). En grupos, comunidades y canales en formato UTC Unix Epoch (microsegundos).

*Ilustración 117. Descripción de los campos de la tabla
"ZWAPROFILEPICTUREITEM"*

5.3.12. ZWAPROFILEPUSHNAME

Tabla que registra el nombre que un contacto se ha autoasignado a su perfil y que es visible para los demás usuarios. Aunque el contacto no se encuentre en la agenda del usuario de esta cuenta, si es miembro de un grupo al que pertenece el usuario, se grabará en esta tabla.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).

Campo	Descripción
Z_ENT	Valor "13" , siendo el número de orden alfabético de la tabla en la base de datos.
ZJID	Identificador "jid" del contacto en WhatsApp.
ZPUSHNAME	Nombre que el contacto se ha autoasignado en su perfil (texto y/o emojis).

*Ilustración 118. Descripción de los campos de la tabla **"ZWAPROFILEPUSHNAME"***

5.3.13. ZWAVCARDMENTION

Tabla que registra información sobre la transmisión de tarjetas de contacto.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "14" , siendo el número de orden alfabético de la tabla en la base de datos.
ZISFROMME	Dirección del envío de la tarjeta de contacto: 0 : tarjeta recibida por el usuario de esta cuenta. 1 : tarjeta enviada por el usuario de esta cuenta.
ZMEDIAITEM	Valor que se corresponde con el campo "Z_ENT" de la tabla "ZWAMEDIAITEM" y permite vincular ambas tablas.
ZDATE	Fecha en el que el usuario de esta cuenta envió o recibió la tarjeta de un contacto en formato UTC OS X Epoch.
ZSENDERJID	Identificador "jid" del contacto que envió la tarjeta de contacto. Cuando la envía el usuario de esta cuenta este campo se encuentra vacío.
ZWHATSAPPID:	Número de teléfono almacenado en la tarjeta de contacto transmitida.

*Ilustración 119. Descripción de los campos de la tabla **"ZWAVCARDMENTION"***

5.4. Base de datos *ContactsV2.sqlite*

Es la base de datos que contiene la información de los contactos. No contiene información alguna de los grupos, difusiones, comunidades o canales.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/ContactsV2.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/ContactsV2.sqlite**

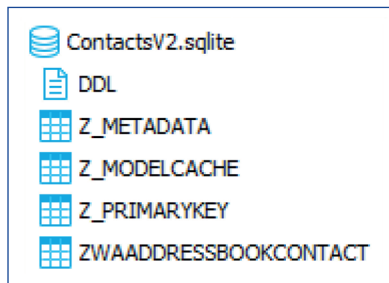


Ilustración 120. Tablas de la base de datos “ContactsV2.sqlite”

5.4.1. ZWAADDRESSBOOKCONTACT

Tabla que registra los contactos que se encuentran en la agenda de WhatsApp del usuario de esta cuenta.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor “1”, siendo el número de orden alfabético de la tabla en la base de datos.

Campo	Descripción
ZPHONESTATUS	Estado de la cuenta: 1 : contacto del usuario (se encuentra registrado en su agenda). 4 : no es contacto del usuario (no se encuentra registrado en su agenda).
ZSORT	Valor (generalmente múltiplo de mil) que indica el orden en el que se muestran los contactos en la agenda de WhatsApp. El orden numérico se corresponde con el orden alfabético del valor del campo "ZHIGHLIGHTEDNAME" , de tal modo que el primer contacto ordenado alfabéticamente tendrá el valor "1000", el segundo el valor "2000" y sucesivamente, pudiéndose dar valores como "2250" o "3500", que se posicionarán en el correspondiente orden numérico. No es un valor inmutable y la incorporación de nuevos contactos produce cambios de orden.
ZSOURCE	Fuente de la información del contacto: 0 : agenda del teléfono. 1 : WhatsApp
ZSPOTLIGHTS-TATUS	Estado del usuario de WhatsApp en la agenda del usuario de esta cuenta: 1 : contacto que se muestra en la agenda. -5 : miembro de WhatsApp que no se muestra en la agenda (no es un contacto almacenado del usuario de esta cuenta).
ZABOUTTIMES-TAMP	Fecha en la que el contacto estableció el texto y/o emojis en el campo "info." de su perfil en formato UTC OS X Epoch.
ZLASTUPDATED	Fecha de la última actualización de datos del contacto en formato UTC OS X Epoch.
ZABOUTTEXT	"info." establecido por el contacto en su perfil. Por defecto <i>"¡Hola! Estoy usando WhatsApp."</i> Solo puede ser un texto limitado y/o emojis.
ZFULLNAME	Nombre y apellidos del contacto tal y como se encuentra guardado en la agenda del usuario de esta cuenta.
ZGIVENNAME	Nombre del contacto tal y como se encuentra guardado en la agenda del usuario de esta cuenta.
ZHIGHLIGHTED-NAME	Texto que se muestra en la agenda para ordenarla. Será el Apellido del contacto y en caso de no tener grabado el campo apellido tomará el valor del campo "ZGIVENNAME" .

Campo	Descripción
ZLID	Identificador "lid" del contacto.
ZPHONENUM-BER	Número de teléfono de contacto.
ZPHONENUM-BERLABEL	Etiqueta asociada al número de teléfono (móvil, casa, trabajo, etc.).
ZSEARCH-TOKENLIST	Tokens por los que se puede buscar al contacto en la agenda (cada una de las palabras que forman el nombre y apellido del contacto)
ZSECTIONTITLE	Carácter por el que empieza y se puede localizar el apellido o nombre del contacto en la agenda. Se corresponde con la primera letra del campo " ZHIGHLIGHTEDNAME ". Ejemplo: R si el contacto se apellida Rodríguez.
ZWHATSAPPID	Identificador "jid" del contacto.

*Ilustración 121. Descripción de los campos de la tabla
"ZWAADDRESSBOOKCONTACT"*

5.5. Base de datos *DeviceAgents.sqlite*

Esta base de datos **almacenaba** información sobre los dispositivos vinculados al dispositivo principal. Desde las versiones de WhatsApp publicadas a mediados de 2025, solo registra información sobre el dispositivo principal, **sin incluir datos sobre los dispositivos vinculados**.

Si la instalación de la aplicación es anterior a la fecha indicada, puede que aún conserve información de vinculaciones previas, hasta el momento en que la aplicación dejó de registrar dichos datos (mediados de 2025).

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/DeviceAgents.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/DeviceAgents.sqlite**

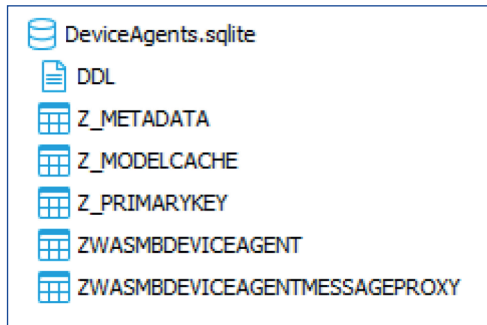


Ilustración 122. Tablas de la base de datos “**DeviceAgents.sqlite**”

5.5.1. ZWASMBDEVICEAGENT

Tabla que registra los dispositivos que se han vinculado con el dispositivo principal.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor “ 1 ”, siendo el número de orden alfabético de la tabla en la base de datos.
ZDEVICEID	Número de identificación de dispositivo vinculado. En cada ocasión que se vincula un dispositivo incrementa en una unidad, siendo el número “ 0 ” el dispositivo principal al cual se vinculan los demás. Cuando se desvincula el valor es “ -1 ”.
ZLASTMODIFIED-TIMESTAMP	Fecha de la vinculación del dispositivo en formato UTC Unix Epoch (segundos) o de desvinculación si el valor del campo “ ZDEVICEID ” es “ -1 ”

Campo	Descripción
ZAGENTID	UUID que identifica el dispositivo vinculado y determinado software. Si se vincula en más de una ocasión un mismo dispositivo, no se generará un nuevo registro de dispositivo, sino que se actualizará la información que contiene el registro existente. Ejemplo: Un ordenador con S.O. Windows en el que se ha vinculado la cuenta a través de WhatsApp Web en Edge, siempre tendrá el mismo UUID independientemente de las veces que se vincule y desvincule. Pero si en el mismo ordenador se vincula a través del navegador Firefox, se creará un nuevo UUID, debido al uso de otra aplicación para navegar.
ZNAME	Tipo de plataforma a través de la cual se ha vinculado la cuenta: "Android Phone": Dispositivo Android. "iPhone": Teléfono iPhone (distinto al iPhone de la cuenta principal) "macOS": Aplicación de escritorio para ordenadores Mac. De WhatsApp Web registra el "navegador (sistema operativo)". Ej: " Firefox (Windows) ", " Safari (macOS) " (tanto iMac como iPad).

*Ilustración 123. Descripción de los campos de la tabla
"ZWASMBDEVICEAGENT"*

5.6. Base de datos *emoji.sqlite*

Almacena todos los emojis de los que dispone el usuario. La tabla "**gms_es_content**" es donde se encuentran registrados los emojis.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/emoji.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUI>/emoji.sqlite**

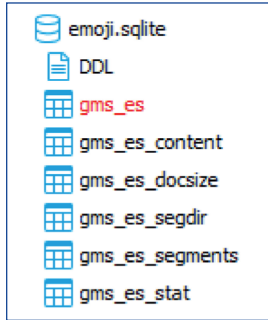


Diagrama de la base de datos emoji.sqlite. El diagrama muestra una lista de tablas dentro de un recuadro. Las tablas son: emoji.sqlite (representada por un icono de cilindro de base de datos), DDL (representada por un icono de documento), gms_es (representada por un icono de cuadrícula y resaltada en rojo), gms_es_content (representada por un icono de cuadrícula), gms_es_docsize (representada por un icono de cuadrícula), gms_es_segdir (representada por un icono de cuadrícula), gms_es_segments (representada por un icono de cuadrícula) y gms_es_stat (representada por un icono de cuadrícula).

emoji.sqlite
DDL
gms_es
gms_es_content
gms_es_docsize
gms_es_segdir
gms_es_segments
gms_es_stat

Ilustración 124. Tabla de la base de datos “emoji.sqlite”

5.7. Base de datos *ExtChatDatabase.sqlite*

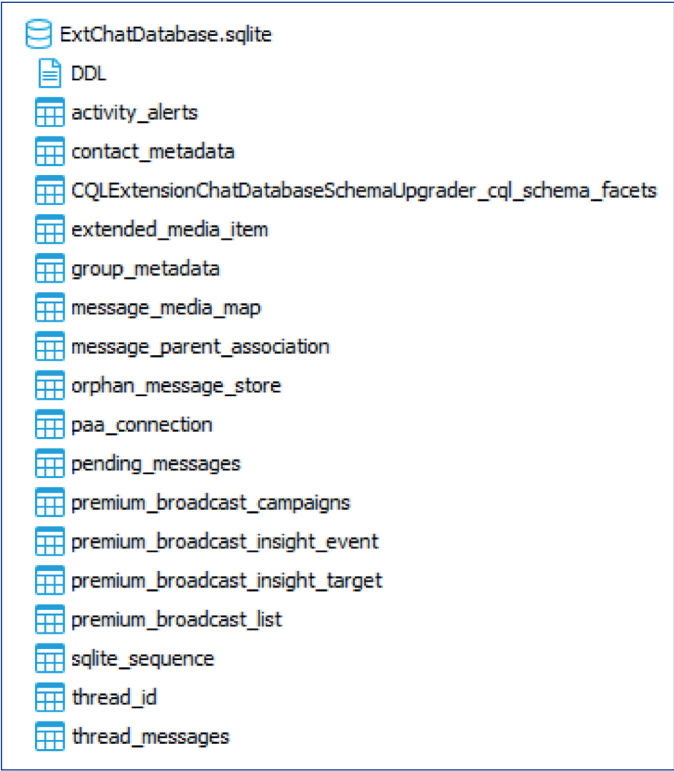
Base de datos que registra la relación entre los archivos enviados en un álbum y el mensaje del sistema que informa del envío del álbum. Posiblemente relacione otros archivos también, pero es un extremo que no se ha podido confirmar.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/ExtChatDB/ExtChatDatabase.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUI>/ExtChatDB/ExtChatDatabase.sqlite**



A screenshot of a database browser showing the structure of the ExtChatDatabase.sqlite database. The list includes the database file itself, a DDL file, and 20 tables: activity_alerts, contact_metadata, CQLExtensionChatDatabaseSchemaUpgrader_cql_schema_facets, extended_media_item, group_metadata, message_media_map, message_parent_association, orphan_message_store, paa_connection, pending_messages, premium_broadcast_campaigns, premium_broadcast_insight_event, premium_broadcast_insight_target, premium_broadcast_list, sqlite_sequence, thread_id, and thread_messages.

ExtChatDatabase.sqlite
DDL
activity_alerts
contact_metadata
CQLExtensionChatDatabaseSchemaUpgrader_cql_schema_facets
extended_media_item
group_metadata
message_media_map
message_parent_association
orphan_message_store
paa_connection
pending_messages
premium_broadcast_campaigns
premium_broadcast_insight_event
premium_broadcast_insight_target
premium_broadcast_list
sqlite_sequence
thread_id
thread_messages

Ilustración 125. Tabla de la base de datos “ExtChatDatabase.sqlite”

5.7.1. message_parent_association

Tabla que registra la información de los archivos multimedia que han sido enviados agrupados en un álbum. Se genera un registro por cada uno de los archivos enviados en una agrupación, compartiendo el mismo valor del campo “parent_stanza_id” todos los archivos que se han enviado juntos.

Campo	Descripción
stanza_id	Valor que se corresponde con el valor del campo “ZSTAN- ZOID” de la tabla “ZWMESSAGE” de la base de datos “ChatStorage.sqlite”, permitiendo identificar el mensaje de uno de los archivos transmitidos.

Campo	Descripción
parent_stanza_id	Valor que se corresponde con el valor del campo "ZSTAN- ZAID" de la tabla "ZWAMESSAGE" de la base de datos "ChatStorage.sqlite", permitiendo identificar el mensaje del sistema que informa de la transmisión de un álbum.
sort	Número de posición del mensaje en el chat al que perte- nece.
chat_jid	Identificador "lid" del chat en el que se ha transmitido el álbum.

*Ilustración 126. Descripción de los campos
de la tabla "message_parent_association"*

5.8. Base de datos *Labels.sqlite*

Base de datos que registra las etiquetas (labels) predefinidas por la aplicación ("No leídos", "Favoritos" y "Grupos") y las etiquetas creadas por el usuario, así como los contactos o grupos incluidos por el usuario en estas últimas etiquetas.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.
WhatsApp.shared/Labels.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUI>/
Labels.sqlite**

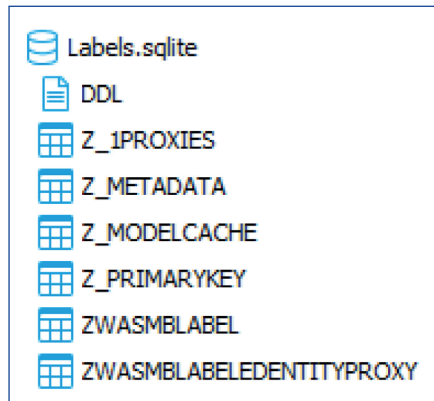


Ilustración 127. Tabla de la base de datos "**Labels.sqlite**"

5.9. Base de datos **LID.sqlite**

Base de datos que almacena los identificadores "lid" de participantes en chats relacionados con el usuario de esta cuenta. En las versiones más actuales de la aplicación (al menos desde la 2.25.32.77), únicamente se está haciendo uso de la tabla "**ZWAZACCOUNT**", pero también se van a describir las tablas "**ZWALIDPROPERTIES**" y "**ZWAPHONENUMBER-LIDPAIR**" para abarcar los casos en los que se analicen teléfonos con versiones antiguas de WhatsApp.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/LID.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/LID.sqlite**

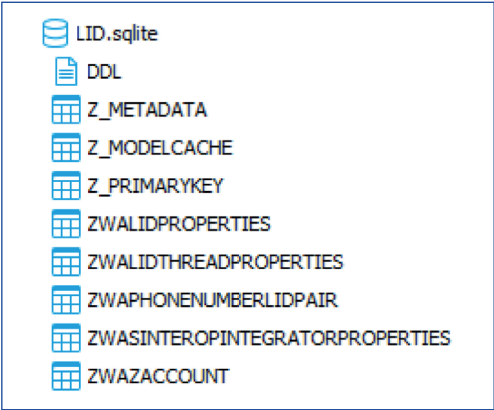


Diagrama de la estructura de la base de datos **LID.sqlite**. El diagrama muestra una jerarquía de archivos y tablas. El archivo principal es **LID.sqlite**, que contiene un archivo **DDL** y varias tablas: **Z_METADATA**, **Z_MODELCACHE**, **Z_PRIMARYKEY**, **ZWALIDPROPERTIES**, **ZWALIDTHREADPROPERTIES**, **ZWAPHONENUMBERLIDPAIR**, **ZWASINTEROPINTEGRATORPROPERTIES** y **ZWAZACCOUNT**.

Ilustración 128. Tabla de la base de datos “**LID.sqlite**”

5.9.1. ZWALIDPROPERTIES

Tabla actualmente en desuso que registraba el identificador “lid” de usuarios de WhatsApp que NO eran contactos del usuario de esta cuenta, pero mantenían algún tipo de relación, como pertenecer a la misma comunidad.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor “1”, siendo el número de orden alfabético de la tabla en la base de datos.
ZDISPLAYNAME	Número de teléfono parcial del “participante”. Está formado por el prefijo internacional y las dos últimas cifras del número de teléfono. Ej: “+34.....24”.
ZLID	Identificador “lid” del “participante”.

Ilustración 129. Descripción de los campos de la tabla “**ZWALIDPROPERTIES**”

5.9.2. ZWAPHONENUMBERLIDPAIR

Tabla actualmente es desuso, que registraba el identificador "lid" de cada contacto del usuario de esta cuenta y lo conectaba con su número de teléfono.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "3", siendo el número de orden alfabético de la tabla en la base de datos.
ZTIMESTAMP	Fecha de la grabación de este registro en esta base de datos en formato UTC OS X Epoch.
ZLID	Identificador "lid" del contacto.
ZPHONENUMBER	Número de teléfono del contacto con prefijo internacional.

*Ilustración 130. Descripción de los campos de la tabla
"ZWAPHONENUMBERLIDPAIR"*

5.9.3. ZWAZACCOUNT

Tabla que registra el identificador "lid" y el número de teléfono de cada participante en chats, grupos o comunidades en los que se encuentra el usuario de esta cuenta.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "5", siendo el número de orden alfabético de la tabla en la base de datos.
ZCREATEDAT	Fecha de la grabación de este registro en esta base de datos en formato UTC OS X Epoch.
ZDISPLAYNAME	Número de teléfono parcial del "participante". Está formado por el prefijo internacional y las dos últimas cifras del número de teléfono. Ej: "+34.....24".

Campo	Descripción
ZIDENTIFIER	Identificador "lid" del contacto.
ZPHONENUM- BER	Número de teléfono del contacto con prefijo internacional.

Ilustración 131. Descripción de los campos de la tabla "ZWAZACCOUNT"

5.10. Base de datos *Sticker.sqlite*

Almacena la información relacionada con los diferentes stickers de los que dispone el usuario.

Ruta en la que se encuentra la base de datos en la extracción de iTunes Backup:

- **/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/Sticker.sqlite**

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/Sticker.sqlite**

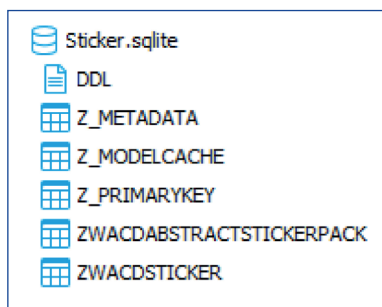


Ilustración 132. Tablas de la base de datos "Sticker.sqlite"

Bases de datos exclusivas de extracciones Full File System

5.11. Base de datos *AppState.sqlite*

Esta tabla no se encuentra por defecto cuando se instala la aplicación en el dispositivo, sino que se genera cuando se vincula el dispositivo principal con otro dispositivo secundario. Esta base de datos almacena información de acciones y cambios muy importantes producidos en el contenido de la aplicación, como borrado de chats, vaciado de chats o eliminaciones de mensajes por el usuario para sí mismo. Se expone la información de la tabla "**ZAPPSTATECONFIRMEDMUTATIONENTITY**", pero no se desarrolla el contenido de las tablas "**ZAPPSTATEENCRYPTIONKEYENTITY**" y "**ZAPPSTATEKEYVALUEENTITY**", debido a que en la primera no se ha podido relacionar la información que aporta y la segunda contiene datos redundantes de la tabla expuesta.

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/AppState/<GUID>/AppState.sqlite**

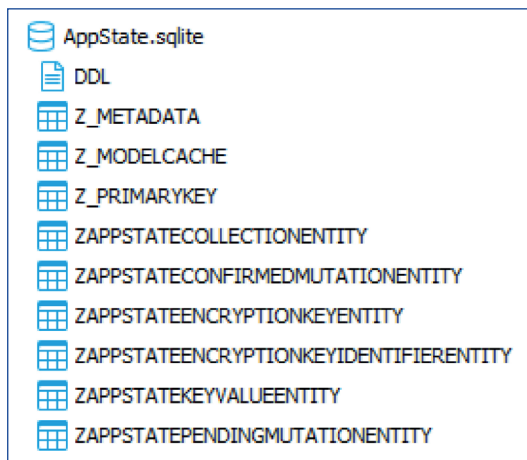


Ilustración 133. Tabla de la base de datos "*AppState.sqlite*"

5.11.1. ZAPPSTATECONFIRMEDMUTATIONENTITY

Tabla que registra cambios que se han producido en la aplicación, como puede ser la eliminación o vaciado de chats. Algunos de estos cambios pueden ser de gran interés durante un análisis forense.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "2", siendo el número de orden alfabético de la tabla en la base de datos.
ZACTIONNAME	Nombre de la acción registrada: clearChat : vaciado de un chat. contact : contacto que se encuentra en la agenda del usuario. deleteMessageForMe : eliminación de un mensaje por el usuario de esta cuenta, únicamente para él. deleteChat : eliminación de un chat. device_capabilities : dispositivos vinculados. lock : chat restringido. setting_chatLock : aplicar código para restringir y ocultar chat. star : mensaje destacado. status_privacy : privacidad de estados seleccionada por el usuario. setting_pushName : nombre autoasignado en la aplicación por el usuario
ZTARGETID	Identificador "jid" del chat sobre la que recae la acción. Cuando la acción es "deleteMessageForMe" o "star" también se le añade el identificador del mensaje.
ZINDEX	Archivo de tipo json con la información de los campos "ZACTIONNAME" y "ZTARGETID"
ZVALUE*	Archivo protobuf con la información relevante de la acción.

*Ilustración 134. Descripción de los campos de la tabla
"ZAPPSTATECONFIRMEDMUTATIONENTITY"*

* ZVALUE: Archivo protobuf que tras ser decodificado presenta información sobre eliminación de mensajes por y para el propio usuario, vaciado o eliminación de chats. En el vaciado de mensajes de un chat o la eliminación de un chat puede registrar el identificador del último o últimos mensajes:

Campo	Campo	Campo	Campo	Descripción
1				Fecha en la que se produjo la acción en formato UTC Unix Epoch (milisegundos)
18 (eliminación de mensaje para mí)		2		Fecha en el que se envió el mensaje eliminado en formato UTC Unix Epoch (segundos).
21 (vaciado de chat)	1	1		Fecha a partir de la cual se reseña en los campos "2X-1-3" los mensajes eliminados o vaciados, en formato UTC Unix Epoch (segundos)
		3 (último o últimos mensajes transmitidos en el chat)	1	1 Identificador "jid" del chat.
				2 Dirección del mensaje: 0 : mensaje recibido por el usuario. 1 : mensaje enviado por el usuario.
				3 Identificador "STANZAID" del mensaje
			2	Fecha de envío del mensaje en formato UTC Unix Epoch (segundos).
22 (eliminación de chat)				

Ilustración 135. Archivo protobuf del campo "ZVALUE" de la tabla "ZAPPSTATECONFIRMEDMUTATIONENTITY"

5.11.2. ZAPPSTATEENCRYPTIONKEYENTITY

Tabla cuya funcionalidad no se ha podido dilucidar pero que presumiblemente registra información sobre claves de cifrado de los dispositivos (principal y vinculados) del usuario de esta cuenta.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "3", siendo el número de orden alfabético de la tabla en la base de datos.
ZDEVICEID	Número de identificador del dispositivo vinculado. Ejemplo: 0 : dispositivo principal 15 : dispositivo vinculado número "15"
ZCREATIONDATE	Fecha de la grabación de este registro en esta base de datos en formato UTC OS X Epoch.
ZDATA	Valor de 32 bytes.
ZFINGERPRINT	Se desconoce su propósito.

*Ilustración 136. Descripción de los campos de la tabla
"ZAPPSTATEENCRYPTIONKEYENTITY"*

5.12. Base de datos Axolotl.sqlite

Esta base de datos almacena las claves públicas de los contactos. Todos los contactos con los que se haya intercambiado las claves públicas se encontrarán en esta base de datos, incluso cuando se borre el contacto de la agenda del dispositivo y/o de WhatsApp.

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/Axolotl.sqlite**

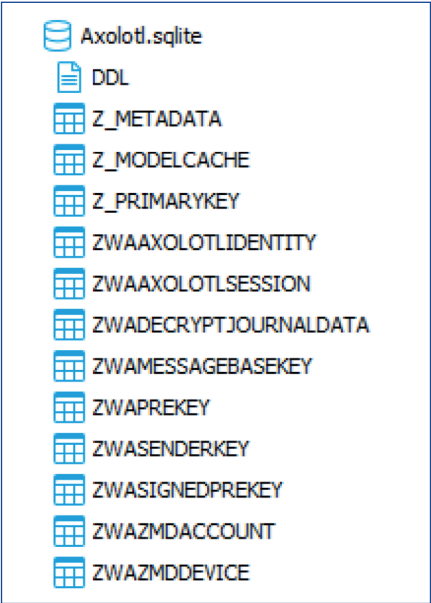


Ilustración 137. Tablas de la base de datos “Axolotl.sqlite”

5.12.1. ZWAAXOLOTLIDENTITY

Tabla que registra el intercambio de las claves públicas por los contactos.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor “1”, siendo el número de orden alfabético de la tabla en la base de datos.
ZDEVICEID	Número de identificación del dispositivo del contacto. El número de identificación siempre es “0” para el dispositivo principal y cualquier otro número es un dispositivo vinculado.
ZTIMESTAMP	Fecha de recepción o comprobación de la clave pública en formato UTC OS X Epoch.

Campo	Descripción
ZRECIPIENTJID	Número de cuenta "jid" del contacto que ha compartido la clave pública. Se corresponde con el campo "ZCONTACT-JID" de la tabla "ZWACHATSESSION" de la base de datos "ChatStorage.sqlite" .
ZKEYDATA	Clave pública compartida por el contacto.

*Ilustración 138. Descripción de los campos de la tabla **"ZWAAXOLOTLIDENTITY"***

5.12.2. ZWAAXOLOTLSESSION

Tabla que registra la fecha de la última interacción con las cuentas de los contactos.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "2" , siendo el número de orden alfabético de la tabla en la base de datos.
ZDEVICEID	Número de identificación del dispositivo del contacto. El número de identificación siempre es "0" para el dispositivo principal y cualquier otro número es un dispositivo vinculado.
ZTIMESTAMP	Fecha de la última interacción con el chat del contacto en formato UTC OS X Epoch. No tiene por qué ser la transmisión de un mensaje, sino una interacción automática de la aplicación como recabar información o comprobar la clave pública del contacto.
ZACCOUNTJIDS-TRING	Identificador "lid" del contacto con el que se ha iniciado una sesión de chat. Se corresponde con el campo "ZIDENTIFIER" de la tabla "ZWAZACCOUNT" de la base de datos "LID.sqlite" .
ZRECIPIENTJID	Identificador "jid" del contacto con el que se ha iniciado una sesión de chat. Se corresponde con el campo "ZCONTACTJID" de la tabla "ZWACHATSESSION" de la base de datos "ChatStorage.sqlite" .

*Ilustración 139. Descripción de los campos de la tabla **"ZWAAXOLOTLSESSION"***

5.13. Base de datos *ChatSearchV5f.sqlite*

Esta base de datos almacena e indexa características de los mensajes transmitidos que permiten al usuario la búsqueda de mensajes de su interés en la aplicación.

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/fts/ChatSearchV5f.sqlite**

En esta base de datos **no se registran** los siguientes tipos de mensajes: notas de vídeo, mensajes de visualización única (imágenes, vídeos y notas de voz), stickers, ubicación, mensajes de canales, notificaciones de llamadas/videollamadas o mensajes del cambio de la temporalidad de los mensajes.

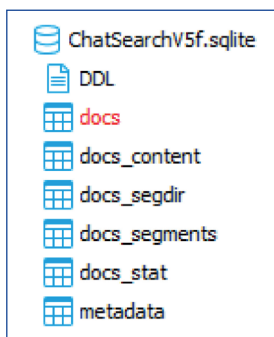


Ilustración 140. Tablas de la base de datos “ChatSearchV5f.sqlite”

5.13.1. docs_content

Tabla que registra el tipo de archivo y/o texto transmitido en los mensajes, así como los chats individuales o grupales en los que se ha compartido.

Campo	Descripción
docid	Número secuencial de creación del registro (establecido por la base de datos SQLite).
c0text	Características del mensaje transmitido por el que se puede buscar en la aplicación: En mensajes en el que haya texto (mensajes de texto, links, encuestas, texto añadido a archivos multimedia...) son las palabras que forman el mensaje o emojis, pero no están ordenadas ni se repiten palabras, aunque se encuentren en el mensaje original. En archivos son su extensión (mp4, jpg, opus...)
c1contact	Número de teléfono del contacto con el que se ha intercambiado el mensaje, con prefijo internacional, precedido del número "81" y finalizado con el carácter "f", codificado en Base64. Para la decodificación hay que eliminar previamente los caracteres finales "_0" y decodificar de Base64 a hexadecimal Ejemplo tras la decodificación: 8134633456456f
c2chat	Chat en el que se ha transmitido el mensaje, codificado en Base64 el cual se debe decodificar a hexadecimal. En un <i>chat individual</i>, el valor es el número de teléfono del contacto, con prefijo internacional, precedido del número "81" y finalizado con el carácter "f". En un <i>chat grupal</i>, el valor es el identificador "jid" del grupo sin el dominio, precedido del número "82".
c3documentType	Tipo de archivo por el que está indexado en la aplicación. Vacío: mensajes de texto o emojis. A: enlace. B: documento. C: imagen. D: vídeo. E: gif. F: audio. G: encuesta. H: evento.

Ilustración 141. Descripción de los campos de la tabla "docs_content"

5.13.2. metadata

Tabla que registra la fecha del intercambio de las claves públicas con el contacto concreto.

Campo	Descripción
docID	Número secuencial de creación del registro (establecido por la base de datos SQLite). Se corresponde con el valor del campo "docid" de la tabla "docs_content" , permitiendo vincular ambas tablas y determinar el mensaje al que le corresponde la fecha registrada en esta tabla.
date	Fecha de envío/recepción del mensaje en formato UTC OS X Epoch. Se corresponde con la fecha del campo "ZMESSAGEDATE" de la base de datos "ChatStorage.sqlite" .

Ilustración 142. Descripción de los campos de la tabla **"metadata"**

5.14. Base de datos **LocalKeyValue.sqlite**

Esta base de datos almacena información sobre elementos considerados clave, aunque en este estudio únicamente se desarrolla la información registrada sobre la vinculación de dispositivos (ver apartado 8.4 VINCULACIÓN DE DISPOSITIVOS).

Ruta en la que se encuentra la base de datos en la extracción FFS:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/LocalKeyValue.sqlite**

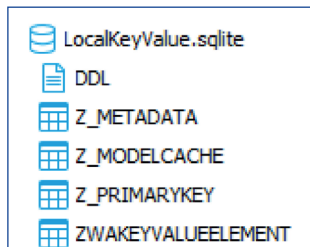


Ilustración 143. Tablas de la base de datos **"LocalKeyValue.sqlite"**

5.14.1. ZWAKEYVALUEELEMENT

Tabla que registra información sobre elementos clave, como por ejemplo la vinculación de dispositivos con el dispositivo principal.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
ZDATE	Fecha del registro en formato UTC OS X Epoch.
ZKEY	Elemento clave sobre el que se ha almacenado información en esta tabla. Ejemplos: Identificador del mensaje del elemento: 3ADCB1D-7196C8BC67907 Identificador "jid" del dispositivo vinculado con la fecha de vinculación en formato UTC Unix Epoch (segundos): 34642642164:31@s.whatsapp.net-2-1762698106
ZNAMESPACE	Tipo de información que se ha registrado sobre el elemento clave. Ejemplo: mud.c: información sobre la vinculación de un dispositivo.
ZVALUE	Información sobre el elemento clave, codificado en un archivo protobuf.

*Ilustración 144. Descripción de los campos de la tabla
"ZWAFINALLOCATIONRECIPIENT"*

5.15. Base de datos Location.sqlite

Esta base de datos que *puede registrar temporalmente* los mensajes de ubicación en tiempo real recibidos y enviados por el usuario de esta cuenta.

Ruta en la que se encuentra la base de datos en la extracción FFS:

- /private/var/mobile/Containers/Shared/AppGroup/<GUID>/Location.sqlite

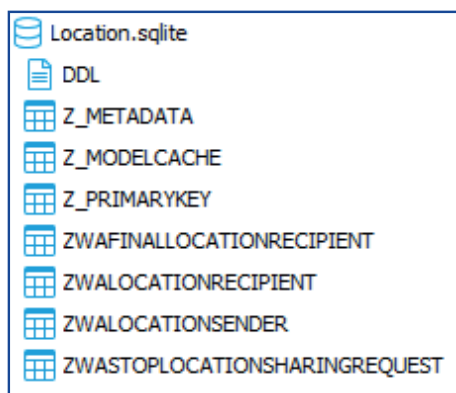


Ilustración 145. Tablas de la base de datos **"Location.sqlite"**

5.15.1. ZWAFINALLOCATIONRECIPIENT

Tabla que puede registrar temporalmente los mensajes de ubicación en tiempo real enviados por el usuario de esta cuenta.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "1" , siendo el número de orden alfabético de la tabla en la base de datos.
ZEXPIRATION	Fecha en la que finalizará automáticamente la transmisión de la ubicación en formato UTC OS X Epoch.
ZCHATJID	Identificador "jid" del contacto que ha recibido la ubicación en tiempo real.
ZJID	Identificador "lid" del contacto que ha recibido la ubicación en tiempo real.
ZMESSAGEID	Valor que se corresponde con el valor del campo "ZSTAN- ZAID" de la tabla "ZWAMESSAGE" de la base de datos "ChatStorage.sqlite" , permitiendo identificar el mensaje en el que fue transmitido la ubicación.

Ilustración 146. Descripción de los campos de la tabla **"ZWAFINALLOCATIONRECIPIENT"**

5.15.2. ZWALOCATIONSENDER

Tabla que puede registrar temporalmente los mensajes de ubicación en tiempo real enviados al usuario de esta cuenta.

Campo	Descripción
Z_PK	Número secuencial de creación del registro (establecido por la base de datos SQLite).
Z_ENT	Valor "3", siendo el número de orden alfabético de la tabla en la base de datos.
ZSEQUENCENUMBER	Fecha del inicio de la transmisión en formato UTC Unix Epoch (microsegundos) en ubicación en tiempo real.
ZCHAT	Identificador "jid" del contacto o grupo desde el que se ha transmitido la ubicación.
ZPARTICIPANT	Identificador "lid" del contacto que ha enviado la ubicación en tiempo real.

*Ilustración 147. Descripción de los campos de la tabla
"ZWALOCATIONSENDER"*

6. Archivos de interés de Whatsapp (Android)

En este capítulo se describen las principales rutas del sistema de archivos del dispositivo donde se localizan los directorios y los archivos cuyo análisis puede presentar un mayor interés, debido a que están directamente relacionados con el uso de la aplicación:

6.1. Directorio `/data/data/com.whatsapp/files`

Está ubicado en una zona protegida o restringida del sistema de archivos, a la que un usuario sin privilegios no puede acceder directamente. Para evadir esta limitación, es necesario contar con permisos de administrador, bien por tratarse de un teléfono "rooteado" o porque se ha explotado alguna vulnerabilidad del dispositivo.

Entre los archivos de interés que se encuentran en este directorio están la clave de cifrado de las bases de datos, archivos compartidos a través de la aplicación, logs del uso de la aplicación, información sobre la versión instalada de WhatsApp, preferencias del usuario, etc.

También contiene otros archivos de menor relevancia forense, como son las imágenes de perfil de los contactos y grupos (carpeta Avatars), stickers e imágenes de avatares, cuya información no se va a ampliar en este análisis.

A continuación, se describen los archivos, carpetas y subdirectorios más relevantes de este directorio:

6.1.1. /data/data/com.whatsapp/files/

En la raíz de este directorio podemos localizar la clave de cifrado que utiliza la aplicación para cifrar los posibles backups (copias de seguridad) generados. La aplicación utiliza la clave criptográfica denominada "**key**" para cifrar con "crypt14" y la clave denominada "**encrypted_backup.key**" en el caso que esté cifrado con "crypt15". Pueden darse varias situaciones: que no se encuentre ninguna clave, que solo esté presente una o que existan ambas.

6.1.2. /data/data/com.whatsapp/files/.Shared/

Carpeta que puede contener algunos de los últimos archivos multimedia enviados por el usuario de esta cuenta. Los archivos que se han almacenado en este subdirectorio se mantienen por un tiempo indeterminado (desde horas a días) y posteriormente son eliminados por la aplicación. En las pruebas realizadas, se ha observado que puede almacenar imágenes, notas de voz y stickers enviados. Pueden proceder incluso de mensajes eliminados o de visualización única tanto reproducidos como no reproducidos.

6.1.3. /data/data/com.whatsapp/files/.Trash/

Puede albergar temporalmente algún archivo que se corresponda con un elemento enviado como thumbnail, vídeo o nota de vídeo. En las

pruebas realizadas, los archivos son visualmente idénticos a los enviados, pero no tienen el mismo hash; por tanto, no se puede asegurar con certeza que pertenezcan a un mensaje concreto.

6.1.4. /data/data/com.whatsapp/files/decompressed/libs.spo/.superpack_version

Almacena información sobre la versión instalada de WhatsApp en el dispositivo.

6.1.5. /data/data/com.whatsapp/files/Logs/

Esta carpeta contiene los archivos de registro de los “logs” de la aplicación WhatsApp, los cuales contienen información de alto valor forense, aunque presentan una importante limitación temporal: solo se conservan los últimos 4 o 5 días.

Los registros se generan con fecha/hora local basándose en la zona horaria del dispositivo, a diferencia de las bases de datos que se basan en horario UTC.

Existe un archivo en texto plano denominado **whatsapp.log** que registra los logs del día actual. Además, en esta carpeta deberían coexistir 4 archivos comprimidos con los logs de los últimos 4 días con la siguiente nomenclatura:

- **whatsapp-AAAA-MM-DD.1.log.gz**⁴

Dado que se trata de archivos en texto plano y a su gran extensión, la forma más básica de localizar la información requerida es mediante búsquedas de palabras clave con un editor de texto como puede ser Notepad++.

4. AAAA es el año, MM es el mes, DD es el día.

Muchos de los datos registrados corresponden a valores presentes en las bases de datos ya descritas. Por ello, puede ser necesario consultar el significado de esos valores para interpretar correctamente los registros.

Asimismo, las marcas de tiempo están codificadas en fecha UTC Unix Epoch (milisegundos) y los identificadores "jid" de los contactos del chat con los que se mantienen las comunicaciones únicamente son mostrados con las últimas cuatro cifras del número de teléfono:

remoteChatJid=2255@s.whatsapp.net

Cuando se trata de grupos, comunidades, etc., se muestra el identificador "jid" completo:

remoteChatJid=363167962076426@g.us

Son innumerables las interacciones que la aplicación registra en estos logs. A continuación, se mostrarán varios ejemplos, aunque hay registros que por ser de interés para análisis específicos se mostrarán en los apartados del presente informe creados para tal extremo.

Cuando *se envía un mensaje* (**isFrom_me=true**), es posible localizar el valor de **"key_id"** (identificador del mensaje), el número de registro **"row_id"** (que se corresponde con el campo **"_id"** de la tabla **"message"**) y los últimos cuatro dígitos de la cuenta **"jid"** (**chatJid=8364@s.whatsapp.net**) a la que se ha remitido —si se trata de un contacto— o el identificador completo en el resto de los casos.

Para determinar el tipo de mensaje enviado, pueden encontrarse registros con nombres como **"mediaType=2"** o **"...write/type=43"**, que podrían inducir a pensar que representan el valor del campo **"message_type"**. Sin embargo, el dato correcto se obtiene de los registros que contienen el texto **"...messagenotification/new=fmsg/status:0/type:3/..."** o **"overallMediaType=3"**, en los cuales el valor de **"type"** se corresponde efectivamente con el campo **"message_type"** de la tabla **"message"** (en este caso, **"3"**).

Cuando el mensaje transmitido incluye un archivo, el registro puede contener el nombre con el que se almacena en el dispositivo (el vídeo **VID-20251127-WA0005**), su tamaño en bytes (**overallMediaSize=392538**) y los distintos estados por los que pasa durante el proceso de envío y entrega (en este caso, el último estado registrado es **"status=13"**).

A continuación, se incluyen los registros más significativos de un envío, omitiéndose otros de menor interés para simplificar la visualización (al igual que en el resto de los ejemplos):

```
2025-11-27 16:43:57.402 LL_I W [2:main] MediaTranscodeService/onMessageChanged for message:Key(id=AC927E3B2B4E985C8337777E9667EA9E, isFromMe=true, chatJid=8364@s.whatsapp.net) : status = 1
: in progress = false : size = 0
2025-11-27 16:43:57.420 LL_I W [94:AsyncCommitThread] MainMessageStore/insertMainMessageRow/
inserted/updated rowId=4977 key=Key(id=AC927E3B2B4E985C8337777E9667EA9E, isFromMe=true,
chatJid=8364@s.whatsapp.net) chatRowId=null
2025-11-27 16:44:00.444 LL_I W [966:WhatsApp Worker #495] BaseMediaFileUtils/readablefilename VID-
20251127-WA0005
2025-11-27 16:44:00.491 LL_I W [931:WhatsApp Worker #489] MediaJobEventBuilder/postWamMediaU-
pload2Event WamMediaUpload2 {batchSize=1, connectionType=1, estimatedBandwidth=154.3000030517578,
estimatedBandwidthV2=182.5, fileHeight=850, fileWidth=474, httpProtocolVersionType=0, isViewOnce=false,
mediaId=4050966546371856422, messageKeyHash=DTica0i53H4YXty+OH/Uk/19iNW+HbQMCueww2sBkAU=,
networkStack=4, originalSize=1531230, overallAttemptCount=0, overallConnBlockFetchT=1, overallConnection-
Class=pop, overallCumT=3081, overallCumUserVisibleT=3081, overallDomain=157.240.5.60, overallIsFinal=true,
overallIsForward=false, overallIsManual=true, overallMediaKeyReuse=1, overallMediaSize=392538 0, overall-
MediaType=3, overallMmsVersion=4, overallOptimisticFlag=0, overallQueueT=5048066, overallRetryCount=0,
overallT=3081, overallTranscodeT=1784, overallUploadMode=1, overallUploadOrigin=2, overallUploadResult=1,
overallUserVisibleT=3081, uploadBytesTransferred=392554.0, uploadConnectT=2, uploadHttpCode=200,
uploadIsReuse=true, uploadIsStreaming=false, uploadNetworkT=1078, uploadSource=2, videoQualitySetting=0, }
2025-11-27 16:57:17.044 LL_I W [2:main] MediaTranscodeService/onMessageChanged for message:Key(id=AC927E3B2B4E985C8337777E9667EA9E, isFromMe=true, chatJid=8364@s.whatsapp.net) : status = 13
: in progress = false : size = 0
```

Cuando *se recibe un mensaje*, la forma de registrar el tipo de mensaje es similar a la del envío. Los valores **"key_id"** (identificador del mensaje) y **"row_id"** (que se corresponde con el campo **"_id"** de la tabla **"message"**) se mantienen, pero el campo **"isFrom_me"** adquiere el valor **false**.

Del mismo modo, el campo que representa el tipo de mensaje (**"message_type"**) puede generar confusión. No debe atenderse a valores como **"mediaType=2"** o **"...write/type=43"**, que podrían llevar a error, sino a los registros que incluyen el texto **"...messagenotification/new=fmsg/status:0/type:3/..."**, donde el valor de **"type"** se corresponde realmente con el campo **"message_type"** de la tabla **"message"** (en este caso, **"3"**).

Cuando el mensaje recibido contiene un archivo, se registran también el tamaño del archivo en KB, los últimos cuatro caracteres del **hash SHA-256** codificado en **Base64** (dato exclusivo de los mensajes recibidos) y el nombre con el que se ha almacenado en el dispositivo tras su descarga (el vídeo **VID-20251125-WA0006**):

```
2025-11-25 20:41:26.378 LL_I W [781:SignalExecutor] MainMessageStore/insertMainMessageRow/inserted/updated rowId=4974 key=Key(id=3A9DA558CFB8E2A271B8, isFromMe=false, chatJid=8364@s.whatsapp.net) chatRowId=null
2025-11-25 20:41:26.531 LL_I W [169:Notifications] messagenotification/ new=fmsg/status:0/type:3/rmt-src:null Key(id=3A9DA558CFB8E2A271B8, isFromMe=false, chatJid=8364@s.whatsapp.net) isNotificationSilent=false
2025-11-25 20:41:38.374 LL_I W [934:WhatsApp Worker #176] MediaDownloadManager/start manual download Key(id=3A9DA558CFB8E2A271B8, isFromMe=false, chatJid=8364@s.whatsapp.net), message.mediaHash=*****uBQ=
2025-11-25 20:41:38.374 LL_I W [934:WhatsApp Worker #176] MediaDownload/call; priority=-1; mediaSize:780KB; mediaType=2
2025-11-25 20:41:39.279 LL_I W [934:WhatsApp Worker #176] BaseMediaFileUtils/readablefilename VID-20251125-WA0006
```

Salida del usuario de un grupo: el "jid" parcial 2387@s.whatsapp.net es el usuario de esta cuenta, y el grupo es el "jid" 363371851860189@g.us:

```
2025-11-25 19:17:44.604 LL_I W [335:WhatsApp Worker #114] BaseNotificationHandler/handleAndAckNotification handlerType=209 id=2511361855 type=w.gp2 t=1737832664 retry=null offline=null
2025-11-25 19:17:44.605 LL_I W [335:WhatsApp Worker #114] groupmgr/onGroupRemoveUsers StanzaMetadata(id=2511361855, remoteChatJid=363371851860189@g.us, participantUserJid=2387@s.whatsapp.net, loggableStanzaId=48, stanzaAckCallback=X.8y7@df7bdda)jids:[2387@s.whatsapp.net]/removedBy:2387@s.whatsapp.net
2025-11-25 19:17:44.605 LL_E W [335:WhatsApp Worker #114] WaJidMapRepository/setJidOrderedMapping fail; messageStoreManager.isReady:true
2025-11-25 19:17:44.606 LL_I W [335:WhatsApp Worker #114] groupmgr/onGroupRemoveUsers/me leaving
2025-11-25 19:17:44.606 LL_I W [335:WhatsApp Worker #114] groupmgr/onLeaveGroup/[363371851860189@g.us]
2025-11-25 19:17:44.608 LL_I W [335:WhatsApp Worker #114] groupmgr/onLeaveGroup/starting to remove from groupjid = 363371851860189@g.us
```

Estado de la batería con el nivel de carga, estado de salud o si está cargando:

```
2025-11-16 20:42:01.227 LL_I M [911:AsyncTask #3] HoURLyCronAction; battery BatteryState{health=good, level=51, plugged=0, scale=100, percent=51.0}
```

Inicio de generación de copia de seguridad:

```
2025-11-15 02:05:11.295 LL_I W [680:AsyncTask #1] backupMessages/timer/start
2025-11-15 02:05:11.297 LL_I W [680:AsyncTask #1] BackupMessagesAction/backupMessages; intent=Intent { act=com.whatsapp.action.BACKUP_MESSAGES flg=0x10 cmp=com.whatsapp/.AlarmService }
2025-01-15 02:05:11.302 LL_I W [680:AsyncTask #1] BackupMessagesAction/backupMessages starting message backup
```

Estado de conexión del teléfono a la red móvil de datos y/o a Wi-Fi:

```
2025-11-25 15:46:36.181 LL_I W [147:MessageHandler Connectivity Handler] network/info  
[type: MOBILE], state: DISCONNECTED/DISCONNECTED, reason: (unspecified), extra: (none), failover: false,  
available: true, roaming: false], type: 0, subtype: 0  
[type: WIFI], state: CONNECTED/CONNECTED, reason: (unspecified), extra: , failover: false, available: true,  
roaming: false], type: 1, subtype: -1
```

6.1.6. /data/data/com.whatsapp/files/ViewOnce/

Contiene temporalmente los archivos de visualización única recibidos. Cuando son visualizados, se eliminan inmediatamente. En caso de no ser visualizados, la aplicación los borra automáticamente a los **14 días** desde su recepción.

6.2. Directorio /data/data/com.whatsapp/shared_prefs/

En este directorio se encuentran los archivos de configuración del usuario de la aplicación. Son más de cincuenta archivos en formato "xml". Aunque todos los archivos pueden contener información relevante según el contexto de la investigación, los de mayor interés forense son los que gestionan parámetros de seguridad, autenticación y copias de seguridad.

6.2.1. backup_prefs.xml

Almacena información referente a las copias de seguridad generadas a través de la aplicación. Los parámetros y valores que registra se explicarán en el apartado *8.7 COPIAS DE SEGURIDAD / BACKUPS*.

6.2.2. com.whatsapp_preferences.xml

Entre los datos que registra, el más importante es la activación del doble factor de autenticación en la cuenta.

Nombre y valor del parámetro	Significado de los valores
 long name = two_factor_auth_nag_time value = 1736492591291	Fecha en formato UTC Unix Epoch (milisegundos) de la activación del doble factor de autenticación en la cuenta.

Ilustración 148. Archivo **com.whatsapp_preferences.xml**

6.2.3. com.whatsapp_preferences_light.xml

Almacena las opciones de privacidad, descarga automatizada de archivos y generación de copias de seguridad en Google Drive.

De acuerdo con la estructura del presente análisis, se ha optado por mostrar cada grupo de opciones en su apartado correspondiente: las opciones relativas a las descargas en el apartado 8.6 *DESCARGA DE ARCHIVOS RECIBIDOS*, las referentes a las copias de seguridad en Google Drive en el apartado 8.7.1 *Copia de seguridad en Google Drive (Android)* y las de los chats restringidos en el apartado 8.5 *RESTRINGIR UN CHAT*. A continuación, se muestran varias entre las muchas opciones registradas en este archivo "xml".

Nombre y valor del parámetro	Significado de los valores
 long name = last_read_conversation_time value = 1736703899627	Fecha en formato UTC Unix Epoch (milisegundos) de la última conversación leída.
 int name = privacy_status value = 1	Opción de privacidad: info. Quién puede ver los datos de la sección "info." (por defecto la info. del usuario es "¡Hola! Estoy usando WhatsApp". 0: Todos. 1: Mis contactos. 2: Nadie. 3: Mis contactos, excepto... (contacto/s seleccionado/s).

Nombre y valor del parámetro	Significado de los valores
 boolean <code>name = media_quality_has_send_hd_media</code> <code>value = true</code>	Se envía por defecto en calidad HD los archivos multimedia: true: activado. false: desactivado.
 int <code>name = privacy_groupadd</code> <code>value = 3</code>	Opción de privacidad, "Quién puede añadirme a los grupos": 0: Todos. 1: Mis contactos. 3: Mis contactos, excepto... (contacto/s seleccionado/s).
 int <code>name = privacy_online</code> <code>value = 0</code>	Opción de privacidad, "Quién puede ver cuándo estoy en línea": 0: Todos. 4: Igual que la hora de últ. vez (igual que la opción seleccionada en "privacy_last_seen", expuesta un poco más adelante).
 string = ¡Hola! Estoy usando WhatsApp. <code>name = my_current_status</code>	Info. del perfil del usuario.
 int <code>name = privacy_last_seen</code> <code>value = 3</code>	Opción de privacidad, "Quién puede ver mi hora de últ. vez": 0: Todos. 1: Mis contactos. 2: Nadie. 3: Mis contactos, excepto... (contacto/s seleccionado/s).
 boolean <code>name = read_receipts_enabled</code> <code>value = false</code>	Opción de privacidad, "Confirmaciones de lectura". true: activado. false: desactivado.
 int <code>name = delete_chat_count</code> <code>value = 26</code>	Número de chats eliminados por el usuario.
 long <code>name = db_last_all_migrations_attempt_timestamp</code> <code>value = 1703642776318</code>	Fecha en formato UTC Unix Epoch (milisegundos) del último intento de creación de una copia de seguridad en el propio dispositivo (en local).

Ilustración 149. Archivo **com.whatsapp.preferences_light.xml**

6.2.4 disappearing_mode_prefs.xml

Contiene la información de las preferencias del usuario en la asignación de temporalidad a los mensajes de los nuevos chats.

Nombre y valor del parámetro	Significado de los valores
 long name = disappearing_mode_timestamp value = 1693289894000	Fecha en formato UTC Unix Epoch (milisegundos) en el que se le aplicó la temporalidad a los mensajes de los nuevos chats.
 int name = disappearing_mode_duration_int value = 7776000	Tiempo asignado en segundos de la duración de los mensajes de los nuevos chats antes de ser eliminados, 0 (temporalidad desactivada), 86400 (24 horas), 604800 (7 días) o 7776000 (90 días).

Ilustración 150. Archivo **disappearing_mode_prefs.xml**

6.2.5. reg_prefs.xml

Contiene la información del registro de la cuenta de WhatsApp. Hasta principios del año 2025, la mayoría de estos datos se encontraban en el archivo "com.whatsapp_preferences_light.xml", presentando en el apartado 6.2.3.

Nombre y valor del parámetro	Significado de los valores
 long name = registration_success_time_ms value = 1735236700953	Fecha en formato UTC Unix Epoch (milisegundos) del registro exitoso de la cuenta de usuario en el dispositivo.
 string = 346 [REDACTED] name = registration_jid	Número de teléfono con el que se registró la cuenta "jid".
 string = 888888 name = 2fa	Segundo factor de autenticación. El string es el código utilizado.

Ilustración 151. Archivo **reg_prefs.xml**

6.2.6. register_phone_prefs.xml

Contiene la información el número de teléfono registrado en la cuenta. Hasta mediados de diciembre de 2024, este archivo se denominaba "registration.phonenumberentry.RegisterPhone.xml".

Nombre y valor del parámetro	Significado de los valores
 <pre>string = 34 name = com.whatsapp.registration.RegisterPhone.input_country_code</pre>	Código telefónico internacional del país del usuario.
 <pre>string = 6 name = com.whatsapp.registration.RegisterPhone.phone_number</pre>	Número de teléfono con el que se registró la cuenta.

Ilustración 152. Archivo **registration.phonenumberentry.RegisterPhone.xml**

6.2.7. startup_prefs.xml

Contiene, entre otros, los datos del bloqueo de la aplicación por huella, la versión instalada de WhatsApp y el nombre autoasignado por el usuario de la cuenta.

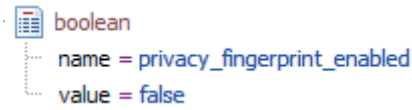
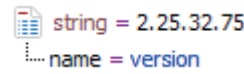
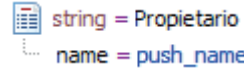
Nombre y valor del parámetro	Significado de los valores
 <pre>boolean name = privacy_fingerprint_enabled value = false</pre>	Opción de privacidad, "Bloquear con huella dactilar" la aplicación. true: activado. false: desactivado.
 <pre>string = 2.25.32.75 name = version</pre>	Versión de la aplicación WhatsApp instalada en el dispositivo.
 <pre>string = Propietario name = push_name</pre>	Nombre de usuario que se ha asignado a sí mismo y que será mostrado al resto de usuarios de la aplicación que no lo tengan grabado en su agenda. El usuario de esta cuenta se ha auto-nombrado como "Propietario".

Ilustración 153. Archivo **startup_prefs.xml**

6.3. Directorio /data/media/0/Android/media/com.whatsapp/WhatsApp/

Es un directorio donde se almacenan la mayoría de los archivos multimedia transmitidos y las copias de seguridad locales de la aplicación.

El usuario puede acceder a este directorio desde cualquier aplicación de exploración de archivos del teléfono, pudiendo copiar, modificar o borrar los archivos almacenados. Sin embargo, las carpetas que comienzan por un punto (.), como son ".Shared", ".Links" y ".Statuses", permanecen ocultas al usuario.

6.3.1. /data/media/0/Android/media/com.whatsapp/WhatsApp/.Shared/

Subdirectorio que almacena temporalmente, algunas imágenes de links, vídeos parciales enviados o recibidos, thumbnails de archivos transmitidos, imágenes de perfil y notas de voz pendientes de envío por falta de conexión.

6.3.2. /data/media/0/Android/media/com.whatsapp/WhatsApp/Backups/

En esta ubicación se guardan copias de seguridad cifradas de las bases de datos de la aplicación que se exponen más abajo y que se actualizan todos los días. Pueden estar cifradas con "crypt14" o si el usuario selecciona en la aplicación el cifrado de extremo a extremo de las copias de seguridad, se cifrará con "crypt15":

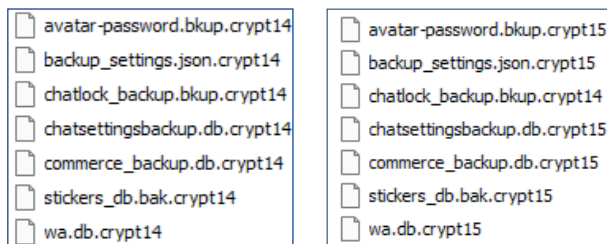


Ilustración 154. Muestra de las copias de las bases de datos con los tipos de cifrados posibles.

6.3.3. /data/media/0/Android/media/com.whatsapp/WhatsApp/Databases/

En este subdirectorio se almacenan varias copias de seguridad de la principal base de datos de WhatsApp: **"msgstore.db"**.

Dada la importancia que tienen estas copias de seguridad, su descripción y análisis se ha expuesto en el apartado 8.7.2 *Copia de seguridad local (Android)*.

6.3.4. /data/media/0/Android/media/com.whatsapp/WhatsApp/Media/

Es un subdirectorio que contiene carpetas con los archivos que han sido transmitidos o han sido generados a través de la aplicación.

El modo en el que se organizan depende de los siguientes parámetros:

1º. Por el tipo de archivo;

Las carpetas se organizan por categorías: imágenes asociadas a los links (.Links) transmitidos, estados del usuario y de sus contactos que actualmente están publicados (.Statuses), Gifs, archivos de audio, documentos, imágenes, stickers, vídeos, notas de vídeo y notas de voz. Se prevé que cuando se implemente en el bot de Meta AI la capacidad de generar archivos multimedia, estos se almacenarán en la carpeta AI Media o WhatsApp AI Media.

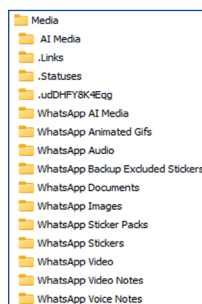


Ilustración 155. Directorios para almacenamiento de archivos

2º. Por tipo de origen (recibido/enviado);

Los archivos **recibidos** se graban en la raíz de la carpeta de cada tipo de archivo (por ejemplo, *Audio*, *Imágenes*, *Videos*, etc.) y los archivos **enviados** en sus respectivas subcarpetas "**Sent**", salvo las notas de voz y de vídeo, que no siguen esta convención (explicada en el punto 3º).

Tampoco siguen esta norma los archivos recibidos en un chat que tenga activada alguna de las opciones: "**Mensajes temporales**", "**Privacidad avanzada del chat**", "**Restringir chat**" o desactivada la "**Visibilidad de archivos multimedia**". En estos casos, se almacenan en la subcarpeta "**Private**", con la particularidad de que no se muestran en la galería del dispositivo.

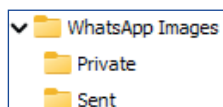


Ilustración 156. Subdirectorios para archivos temporales (Private) y enviados (Sent) de la carpeta de imágenes.

3º. Las notas de voz y notas de vídeo;

Las notas, tanto recibidas como las enviadas, se guardan en subcarpetas que la aplicación genera cada uno o varios días (no se ha podido determinar la frecuencia de creación). A estas carpetas se les asigna un nombre con el año actual seguido de una numeración incremental:

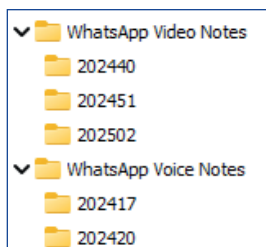


Ilustración 157. Subdirectorios para notas de vídeo y notas de voz

7. Archivos de interés de Whatsapp (iOS)

Los ficheros de configuración, la actividad del usuario y los archivos transmitidos a través de la aplicación siempre son de interés para cualquier investigación.

Al igual que se ha señalado en el *CAPÍTULO 5: BASES DE DATOS DE WHATSAPP (iOS)*, existen diferencias significativas en la cantidad de archivos obtenidos al efectuar una extracción Full File System (FFS) o un iTunes Backup, por lo que siempre que sea posible, resulta preferible efectuar una extracción Full File System (FFS).

Para facilitar la comprensión de este capítulo, primero se describen los archivos de cada directorio que pueden obtenerse en ambos tipos de extracción y posteriormente los archivos que son exclusivos de una extracción FFS.

SUBDIRECTORIOS COMUNES EN AMBOS TIPOS DE EXTRACCIONES

7.1. Directorio “Shared”

Entre los diferentes archivos que se encuentran en las carpetas de este directorio, se almacenan archivos multimedia transmitidos, ficheros de

configuración de la aplicación, imágenes de perfiles, etc. En una extracción FFS se obtienen además dos bases de datos (AppState.sqlite y ChatSearchV5f.sqlite), explicadas en su correspondiente apartado de bases de datos de WhatsApp (iOS), y archivos con registros de logs.

La ruta cuando se analiza una extracción de tipo iTunes Backup es:

- **/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/**

La ruta cuando se analiza una extracción de tipo FFS es:

- **/private/var/mobile/Containers/Shared/AppGroup/<GUID>/**

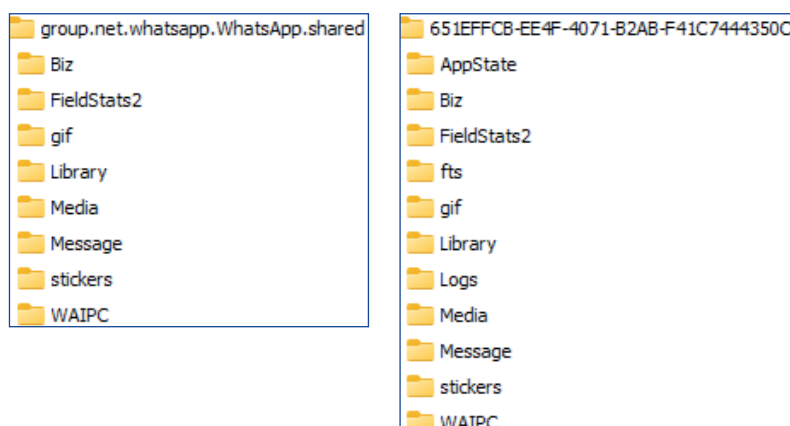


Ilustración 158. Subdirectorios de una Extracción iTunes Backup (izq.) y FFS (dcha.)

Los subdirectorios más relevantes se describen a continuación:

7.1.1. /gif/

En este subdirectorio se almacenan los GIF generados por el usuario de la cuenta.

7.1.2. /Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist

En este subdirectorio únicamente se encuentra un archivo de tipo "plist" que registra las preferencias de configuración del usuario.

Las opciones de estas preferencias que se ajustan al contenido de alguno de los apartados que se desarrollan más adelante se describen en dichos apartados, para que se comprenda mejor su efecto en la aplicación.

En la siguiente ilustración se presentan varias de las opciones registradas en este archivo "plist":

Nombre y valor del parámetro	Significado de los valores
 <code>lidd = "23004364980348:0@lidd"</code>	Identificador "lid" de este dispositivo.
 <code>abp.pnonem = bplist000....]clientVersion[refreshDate22.25.32.77</code>  <code><Dictionary></code>  <code>clientVersion = "2.25.32.77"</code>  <code>refreshDate = 17/12/2025 20:12:03</code>	Archivo "bplist" con la versión de la aplicación instalada actualmente.
 <code>CurrentStatusText = "Descansando cuando se puede"</code>	Estado actual (info.) del usuario de esta cuenta.
 <code>OwnJabberID = "34[REDACTED]@s.whatsapp.net"</code>	Identificador "jid" del usuario de esta cuenta.
 <code>FullName = "Usuario iOS"</code>	Nombre que se ha asignado el propio usuario de esta cuenta en la aplicación.
 <code>se3 = "26.2"</code>	Versión del sistema operativo iOS instalado en el dispositivo.
 <code>lid = "23004364980348@lidd"</code>	Identificador "lid" del usuario de esta cuenta.
 <code>gen47 = True</code>	Se guarda en Fotos (las imágenes y vídeos transmitidos): True: cierto. False: falso.

Ilustración 159. Archivo **group.net.whatsapp.WhatsApp.shared.plist**

7.1.3. /Media/Profile/

Este es el destino donde se almacenan las imágenes de los perfiles de contactos, grupos, comunidades y canales.

7.1.4. /Message/Media/

Contiene un subdirectorio nombrado por el identificador "jid" de cada contacto, grupo o canal con el que el usuario de esta cuenta ha intercambiado archivos.

En cada subdirectorio se generan otros subdirectorios (cuyos nombres son números crecientes) dentro de los cuales se almacenan las imágenes, vídeos, audios, notas de voz, notas de vídeo y documentos transmitidos.

También se crea temporalmente un subdirectorio por cada contacto (dominio "@status") y/o usuario de esta cuenta (status@broadcast) cuando ha publicado alguna imagen, vídeo o nota de voz en su estado, donde almacena temporalmente los archivos compartidos. El subdirectorio normalmente se borra cuando se vacía debido a la eliminación automática de los estados a las 24 horas de publicarlos. No obstante, se ha comprobado que las miniaturas pueden permanecer más tiempo (horas) y que los archivos de estados no se eliminan mientras no se abra la aplicación.

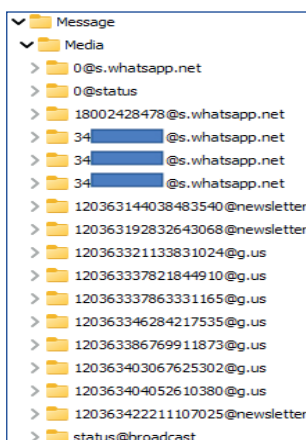


Ilustración 160. Subdirectorios para almacenar archivos transmitidos

7.1.5. /stickers/

Dentro de este subdirectorio hay diferentes carpetas con los stickers que puede enviar el usuario.

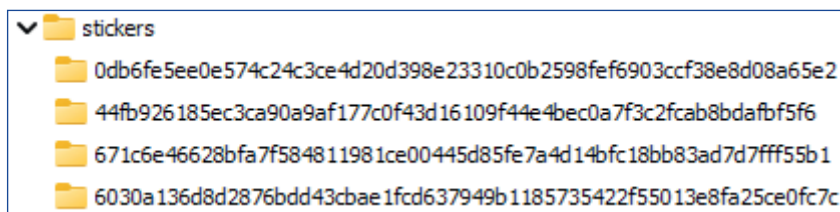


Ilustración 161. Subdirectorio de almacenamiento de stickers

SUBDIRECTORIOS EXCLUSIVOS DE UNA EXTRACCIÓN FULL FILE SYSTEM

7.1.6. /AppState/<GUID>/AppState.sqlite

La base de datos “**AppState.sqlite**” registra cambios de la aplicación, como por ejemplo, agregar contactos, eliminación de mensajes temporales, etc. Al tratarse de una base de datos, se expuso en el apartado 5.11 BASE DE DATOS AppState.sqlite.

7.1.7. /Logs/WhatsApp_2/

Esta carpeta contiene los archivos de registro de “logs” de la aplicación WhatsApp, los cuales almacenan información de su uso y presentan una limitación temporal importante, conservando los últimos 3 a 7 días, dependiendo del uso de la aplicación.

Los registros se graban con hora local basándose en la **zona horaria del dispositivo**.

Es habitual que se generen varios archivos para registrar un día completo, y todos ellos tienen el formato en texto plano.

La nomenclatura es importante porque el nombre del archivo es el único lugar que almacena la fecha completa del log. Estos ficheros son nombrados por su fecha y hora local (hasta milisegundos) de creación, y su numeración secuencial de creación. Cada vez que se genera un archivo de este tipo se incrementa en una unidad la numeración. Ejemplo:

- whatsapp-2025-11-30-00-03-4491-WhatsApp-100.log

Este log inició su grabación el día 30/11/2025 a las 00:03:44 horas. El número de orden de grabación de este log es el número 100. El siguiente archivo log que se genere será el número 101.

Name	Created (Canary)
 whatsapp-2025-11-27-06-19-41-1024-WhatsApp-90.log	27/11/2025 06:19:41
 whatsapp-2025-11-27-16-43-39-4365-ServiceExtension-12-launch.log	27/11/2025 16:43:39
 whatsapp-2025-11-27-16-57-18-1024-WhatsApp-91.log	27/11/2025 16:57:18
 whatsapp-2025-11-27-17-01-38-1024-WhatsApp-92.log	27/11/2025 17:01:38
 whatsapp-2025-11-27-17-04-29-1024-WhatsApp-93.log	27/11/2025 17:04:29
 whatsapp-2025-11-27-17-16-07-4491-WhatsApp-94-launch.log	27/11/2025 17:16:07
 whatsapp-2025-11-28-15-12-27-4491-WhatsApp-95.log	28/11/2025 15:12:27
 whatsapp-2025-11-28-20-54-29-4491-WhatsApp-96.log	28/11/2025 20:54:29
 whatsapp-2025-11-29-21-45-16-4491-WhatsApp-97.log	29/11/2025 21:45:16
 whatsapp-2025-11-30-00-17-08-4491-WhatsApp-98.log	30/11/2025 00:17:08
 whatsapp-2025-11-30-00-26-37-4491-WhatsApp-99.log	30/11/2025 00:26:37
 whatsapp-2025-11-30-13-00-03-4491-WhatsApp-100.log	30/11/2025 13:00:03
 whatsapp-2025-11-30-16-04-38-312-ServiceExtension-13-launch.log	30/11/2025 16:04:38
 whatsapp-2025-11-30-16-04-44-282-WhatsApp-101-launch.log	30/11/2025 16:04:44
 whatsapp-2025-11-30-17-57-02-634-ShareExtension-1-launch.log	30/11/2025 17:57:02
 whatsapp-2025-11-30-20-59-55-282-WhatsApp-102.log	30/11/2025 20:59:55
 whatsapp-2025-11-30-21-05-28-282-WhatsApp-103.log	30/11/2025 21:05:28
 whatsapp-2025-11-30-21-07-27-282-WhatsApp-104.log	30/11/2025 21:07:27

Ilustración 162. Archivos de logs

Dado que son archivos en texto plano y de gran extensión, la forma más básica de localizar la información requerida es mediante búsquedas de palabras clave con un editor de texto como puede ser Notepad++.

En la versión de iOS, la información se genera y almacena de una manera menos estructurada y con menor valor analítico que los registros de la versión de Android. No obstante, dependiendo de la investigación, la información que revelan puede resultar de interés.

En general, la aplicación evita que se graben los identificadores "jid" completos tanto de los contactos como de los grupos, mostrando únicamente las últimas cuatro cifras junto con el dominio. Ejemplo:

- Contactos: *****0111@s.whatsapp.net
- Grupos: *****5096@g.us

En ocasiones puede facilitar el identificador completo, como cuando se envía una nota de voz o cuando se sale de un grupo.

A continuación, se muestran los registros más significativos que se almacenan en los logs, omitiendo líneas que no aportan información de interés y únicamente extenderían el informe:

La primera información que registra cualquier fichero de logs son datos del sistema y dispositivo como son el modelo de iPhone, versión del S.O., versión de WhatsApp o el "jid" parcial del usuario:

```
Device: iPhone SE (2nd generation) | System: iOS 17.5.1 (21F90) | WhatsApp version: 2.25.32.77 | Build number: 626917689 | Hash: 8e62128972a | PID: 365 | JID: <*****5824:0@s.whatsapp.net> | launchID: 09DC14B3-F4E8-4D5C-B2BB-920F4C9AD593
```

Cuando se envía o recibe un mensaje, se genera un log con la hora local del teléfono, el identificador "jid" parcial del contacto o del grupo y el identificador del mensaje. Dependiendo del tipo de mensaje, proporcionará datos del archivo que adjunta, como el tipo y el tamaño en bytes:

```
09:06:54.379 [ 8172] [main-thread ] [F] LL_E streaming-keycache//read-pjpeg-object/scan_sidecar/file hash is nil  
09:06:54.380 [ 8172] [main-thread ] [F] LL_A media-uploader//regular-upload/opt-upload/success  
09:06:54.380 [ 8172] [main-thread ] [F] LL_A media-uploader//completed-with-result/encHash/nAx5T70b-VUuOGcchYOwy7NQVPHC7-E0A36ETc1Cctyg=  
09:06:54.380 [ 8172] [main-thread ] [F] LL_A media-uploader//completed-with-result/~*****0111@s.whatsapp.net>_3AA15B79816040C36C57_1_0/enc-hash/nAx5T70bVUuOGcchYOwy7NQVPHC7-E0A36ETc1Cctyg=/file-size/727120
```

En notas de voz puede indicar el directorio en el que se almacena, que contiene el identificador "jid" del contacto con el que se ha mantenido la conversación:

```
09:07:24.320 [ 8172] [main-thread ] [F] LL_A chatsession/<*****0111@s.whatsapp.net>/counter/4
09:07:24.323 [ 8172] [main-thread ] [F] LL_A message-sender//send/audio/3465500111@s.whatsapp.net
3AAE36148ADEA28E0D35_1_0/is-ptt: 1
09:07:24.406 [ 8172] [main-thread ] [F] LL_A interruption/pause/ /private/var/mobile/Containers/Shared/AppGroup/651EFFCB-EE4F-4071-B2AB-F41C7444350C/PTT/3465500111@s.whatsapp.net.opus]
```

En los archivos de visualización única registra esta característica como "ViewOnce":

```
09:07:55.475 [ 8172] [main-thread ] [F] LL_E streaming-keycache//read-pjpeg-object/scan_sidecar/file
hash is nil
09:07:55.475 [ 8172] [main-thread ] [F] LL_A media-uploader//completed-with-result/<*****0111@s.whatsapp.net>
3A440441ED0AFDD90CB0_1_0/enc-hash/F2_JAF8RaNK-cB1WI8P2xOEoctxxqt1sm6Nm-p7l1ty0=/file-size/795090
09:07:55.476 [ 8172] [main-thread ] [F] LL_A message//dropping-sidecar-for-type: ViewOnceImage
```

También puede quedar registrado un pequeño resumen de la transmisión del mensaje, con el identificador "jid" del contacto con el que se mantiene la conversación, el identificador "ZSTANZAID" del mensaje, o los dispositivos (incluidos los vinculados) a los que se ha enviado el mensaje:

```
09:07:55.481 [ 8172] [main-thread ] [F] LL_A messaging/request: OutboxItemEncryptionRequest {
LL_A chat_jid: <*****0111@s.whatsapp.net>,
LL_A stanza_id: 3A440441ED0AFDD90CB0,
LL_A recipients (5): [<*****5824:9@s.whatsapp.net>: v7, <*****5824:7@s.whatsapp.net>: v6,
<*****0111:0@s.whatsapp.net>: v2, <*****5824:6@s.whatsapp.net>: v5, <*****5824:1@s.whatsapp.net>: v2]
LL_A }
```

Nivel de la batería (1 = 100%):

```
13:16:43.130 [ 8172] [main-thread ] [F] LL_A app//battery level 0.450000
```

7.2. Directorio “Data”

La ruta cuando se analiza una extracción de tipo iTunes Backup es:

- **/private/var/mobile/Applications/net.whatsapp.WhatsApp/Library/**

La ruta cuando se analiza una extracción de tipo FFS es:

- **/private/var/mobile/Containers/Data/Application/<GUID>/Library/**

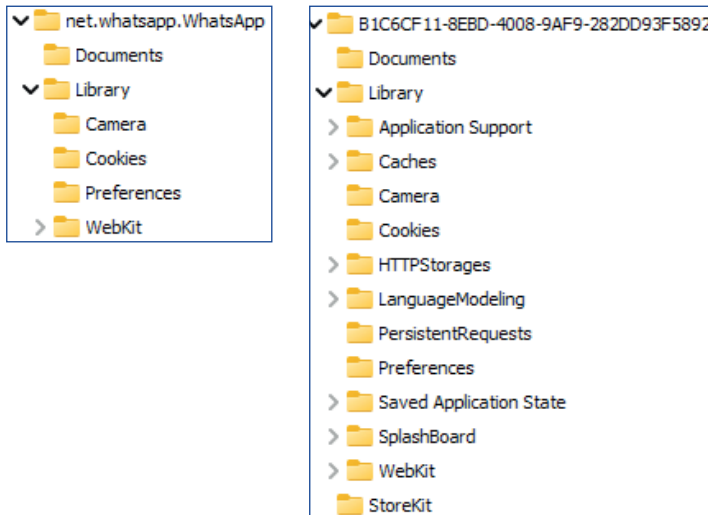


Ilustración 163. Subdirectorio **Library** de una extracción iTunes Backup (izq.) y FFS (dcha.)

SUBDIRECTORIO COMÚN EN AMBOS TIPOS DE EXTRACCIONES

7.2.1. /Camera/

Este subdirectorio almacena (durante unos pocos días) las notas de vídeo creadas por el usuario de esta cuenta.

Son las versiones originales, previas a la compresión que se produce cuando son enviadas. Aunque se trata de notas que se han enviado, en las pruebas no ha sido posible vincularlas con el mensaje enviado y por tanto se desconoce el destinatario de la nota de vídeo. Las notas permanecen durante unos pocos días, incluso cuando los mensajes en los que se enviaron sus correspondientes versiones comprimidas sean eliminados por el usuario de esta cuenta.

SUBDIRECTORIOS EXCLUSIVOS DE UNA EXTRACCIÓN FULL FILE SYSTEM

7.2.2. /Caches/

Es un subdirectorio en el que se graban miniaturas de imágenes, vídeos y notas de vídeo enviados, así como algunas notas de vídeo eliminadas.

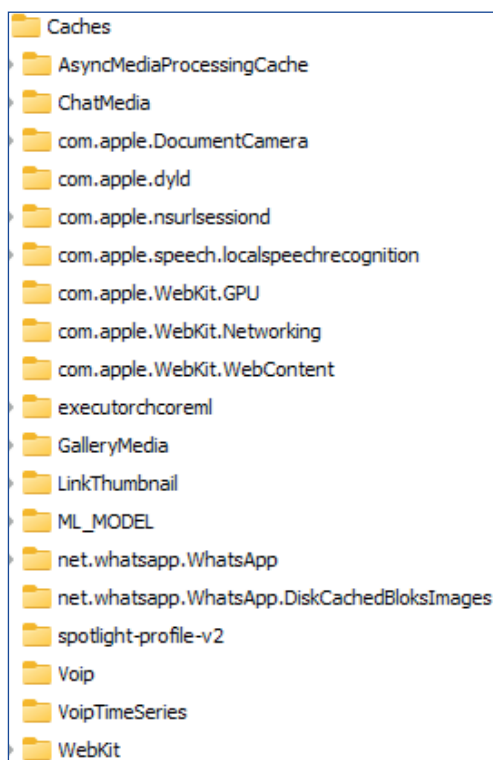


Ilustración 164. Subdirectorio **Caches**

- **/AsyncMediaProcessingCache/**: contiene vídeos y notas de vídeos que han sido enviados por el usuario de esta cuenta.
- **/ChatMedia/**: se almacenan imágenes (jpg) que se han generado de fotogramas de vídeos o de notas de vídeo, imagen previsualizada de archivos "pdf" o de mapas de ubicaciones compartidas. En ocasiones pueden permanecer incluso cuando se elimina el archivo que originó la imagen.

Los archivos se almacenan en subcarpetas que tienen como nombre el "jid" del chat en el que se transmitieron los archivos multimedia:

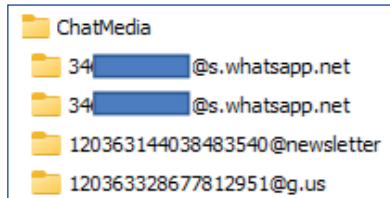


Ilustración 165. Subcarpetas de **ChatMedia**

El nombre del archivo hace referencia al mensaje en el que se ha transmitido el archivo del que se ha generado la imagen, cuando se trata de un fotograma de un vídeo o de una nota de vídeo. Se inicia con el identificador "jid" del contacto, grupo o canal en el que se ha transmitido el archivo, seguido de la identificación del mensaje (**ZSTANZAID**), y únicamente en el caso de los grupos termina con el identificador "jid" del emisor del mensaje:

Chat individual: 34677572337@s.whatsapp.net_321AA683DCE6BE26939334491789477C_0_0.jpg

Chat grupal: 120363328677812951@g.us_26D1E955477C5712460000DC3621C5B4_0_34633572288@s.whatsapp.net.jpg

Canal: 120363144038483540@newsletter_3A18D9254B2E01517EA2_0_0.jpg

- **/GalleryMedia/**: contiene miniaturas o thumbnails en formato "jpg" de imágenes, vídeos y notas de vídeo transmitidos. Se pueden generar días o meses después de que se enviaran los archivos de donde proceden; posiblemente se generen cuando el usuario abre la galería de la aplicación, pero es un extremo que no se ha podido corroborar. El nombre del archivo se corresponde con el archivo transmitido que representa, pero no hay que confundir

esta miniatura con la que se genera cuando se envía o recibe un archivo. La miniatura descrita en este apartado es de mayor resolución que la miniatura que se genera en la transmisión de un archivo, añadiendo que esta última se almacena en la misma ruta del teléfono que el archivo transmitido y tiene extensión ".thumb".

- **/LinkThumbnail/**: almacena las miniaturas generadas cuando se comparte un enlace (link) por la aplicación en un chat.
- **/spotlight-profile-v2/**: contiene imágenes de perfil de contactos, grupos, comunidades y canales.

7.2.3. /SplashBoard/

Contiene capturas de pantalla de la aplicación en formato "ktx". Puede mostrar capturas de chats concretos con los mensajes transmitidos.

8. Análisis de características y funcionalidades de interés (Android – iOS)

Este capítulo se centra en el análisis propiamente dicho de la aplicación. Desde la grabación de contactos o grupos en las bases de datos hasta la vinculación de dispositivos, la confirmación de lectura de mensajes y las diferentes opciones de descarga de archivos, así como otras particularidades de WhatsApp.

8.1. Usuarios, grupos, listas de difusión, comunidades y canales

Es evidente que cualquier herramienta de análisis forense de telefonía es capaz de interpretar los datos y relacionar el identificador "jid" de un usuario, su número de teléfono y el nombre grabado en la agenda de contactos, no siendo necesario profundizar en las bases de datos para este fin. Sin embargo, cuando se requiere un análisis en profundidad, es recomendable explorar las diferentes bases de datos y tablas para interconectar la mayor cantidad de información posible y determinar el origen de los resultados.

A continuación, se explicará cómo se almacena la información de los usuarios, grupos, difusiones, comunidades y canales, tanto en las bases de datos de Android como la de iOS:

8.1.1. Contactos

Todos los contactos que el usuario de la cuenta tiene grabados en la agenda del teléfono serán transferidos automáticamente a la aplicación WhatsApp, pero previamente hay que explicar cómo se registran e identifican los usuarios en la aplicación.

Cuando un usuario se registra en la aplicación WhatsApp, ésta le asigna identificadores para permitirle comunicarse con los demás usuarios. La aplicación adjudica los identificadores denominados "jid" (Jabber Identifier) y "lid". El identificador "jid" aporta una mayor funcionalidad y es significativamente más importante, pues determina la identidad del usuario en la mayoría de las comunicaciones.

Aunque los identificadores "jid" y "lid" ya se han descrito en los apartados 1.1.1 *JID* y 1.1.2 *LID*, en esta sección se repasa su significado.

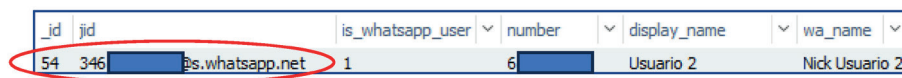
El identificador "jid" de un usuario está compuesto por el prefijo internacional, el número de teléfono del usuario y el dominio (@s.whatsapp.net). La aplicación también asigna un identificador "jid" a los grupos, difusiones, comunidades y canales, aunque su numeración y los dominios que utilizan son completamente diferentes, como se explicará más adelante. Gracias al identificador "jid", es posible relacionar los mensajes con los usuarios que los han transmitido.

Por otro lado, el identificador "lid" sirve para ocultar el número de teléfono del usuario y enlazar al usuario en las comunicaciones salvaguardando su privacidad. Aunque pudiera parecer una solución para mantener la privacidad del usuario, lo cierto es que actualmente se utiliza en pocos tipos de comunicación, como por ejemplo en los canales. El identificador "lid" está formado por 10 dígitos y el dominio (@lid). La

aplicación no asigna un identificador "lid" a los grupos, difusiones, comunidades ni canales.

Android

Retomando la forma en que la aplicación almacena la información de un contacto, cuando se graba en la agenda del teléfono, se crea un registro en la tabla "**wa_contacts**" de la base de datos "**wa.db**". En dicha tabla, los valores más representativos son los registrados en el campo "**jid**", donde está guardado el identificador "jid" del contacto; el valor del campo "**display name**", en el que constará el nombre con el que figura grabado en la agenda de contactos y el campo "**wa_name**", donde se registra el nombre que el contacto se ha autoasignado en la aplicación. Hay otros campos, como la condición de usuario de WhatsApp, el estado, o diversas marcas de tiempo, que según la investigación podrían ser igualmente de interés.



_id	jid	is_whatsapp_user	number	display_name	wa_name
54	346 [redacted]@s.whatsapp.net	1	6 [redacted]	Usuario 2	Nick Usuario 2

Ilustración 166. Tabla "**wa_contacts**"

En la base de datos "**msgstore.db**" existen dos tablas relacionadas con los usuarios. Por un lado, la tabla "**jid**" que, como cabe suponer, registra los *Jabber Identifier* de los contactos, grupos, difusiones, comunidades y canales; además los identificadores "jid" de los dispositivos vinculados de los contactos y del propio usuario (ver apartado 8.4 VINCULACIÓN DE DISPOSITIVOS) y los identificadores "lid" del usuario, contactos y dispositivos vinculados a todos ellos. Por otro lado, figura la tabla "**chat**", que registra la información de la actividad del chat en la que participa el usuario de esta cuenta con otros contactos, grupos, entre otros.

Para poder relacionar los identificadores “jid” y “lid” de un usuario o contacto, es necesario consultar la tabla “**jid_map**”, ya que no son numeraciones que están vinculadas en la tabla “**jid**”.

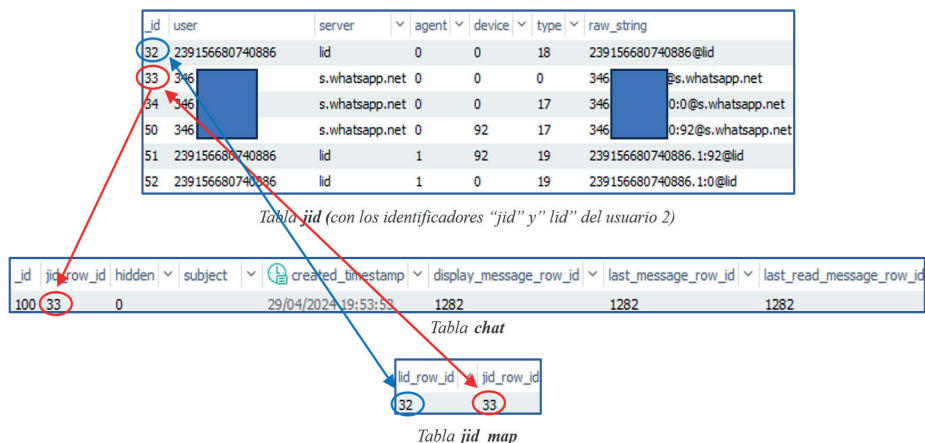


Ilustración 167. Relación entre tablas de los identificadores “jid” y “lid”

Por otro lado, la base de datos “**axolotl.db**”, registra las sesiones de comunicaciones cifradas con los contactos, siendo de gran valor las tablas “**identities**” y “**sessions**”, que registran datos de las claves de cifrado, sesiones con los distintos dispositivos de los contactos, etc. La fecha del primer mensaje intercambiado entre el contacto y el usuario de esta cuenta, desde la instalación de la aplicación en este dispositivo queda registrada en el campo “**timestamp**” de la tabla “**sessions**”. Tal como se observa en la imagen de la tabla “**identities**”, las llaves públicas tanto de la cuenta “jid” como la de la cuenta “lid” de un contacto concreto son idénticas, puesto que se trata del mismo individuo.

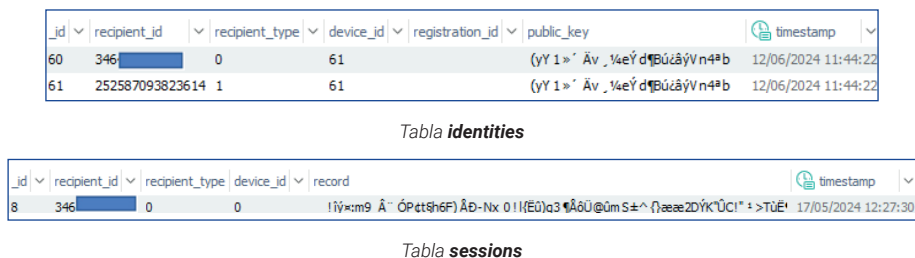


Ilustración 168. Tablas de la base de datos “axolotl.db”

Eliminación de un contacto:

Cuando el usuario elimina un contacto de WhatsApp permanecen pocos rastros de sus interacciones. La propia eliminación queda registrada en el fichero que almacena los logs de la actividad de la aplicación denominado "whatsapp.log". Como se explicó en apartados anteriores, solo se almacenan los registros de los últimos 4 días y únicamente aporta las últimas cuatro cifras de su identificador "jid":

Eliminación del contacto de la agenda del teléfono:

```
2024-07-30 07:48:11.791 LL_I W [204:High Pri Worker #4] unisyncprotocolhelper/parseDeviceData v2
user=2595@s.whatsapp.net
2024-07-30 07:48:11.792 LL_I W [204:High Pri Worker #4] unisyncprotocolhelper/parseDeviceData v2 index
list=2595@s.whatsapp.net; ts=1721920200; expectedTs=0
2024-07-30 07:48:11.793 LL_I W [204:High Pri Worker #4] UniSyncProtocolHelper/handleSyncResult si-
d=sync_sid_delta_78be712a-da4e-4ee2-b14d-3df9033ba90a querySync=false
2024-07-30 07:48:11.793 LL_I W [204:High Pri Worker #4] sync/result sid=sync_sid_delta_78be712a-da4e-
4ee2-b14d-3df9033ba90a index=0 users_count=3 version=1722322090962447 contact=[success=true]
status=[success=true] business=[success=true] devices=[success=true] disappearing_mode=[success=
true] lid=[success=true]
2024-07-30 07:48:11.802 LL_I W [193:sync] ContactManager/logContacts dbinfo/manager/deleteCon-
tacts/del/count 1
2024-07-30 07:48:11.806 LL_I W [193:sync] ContactManagerDatabase/onContactUnlinkedFromPhonebook
individualContactCount = 7
2024-07-30 07:48:11.817 LL_I W [193:sync] ContactManager/delete 0 status of UserJid 2595@s.whatsa-
pp.net deleted.
2024-07-30 07:48:11.831 LL_I W [193:sync] ContactManagerDatabase/onContactsAddedOrUpdated indivi-
dualContactCount = 7
```

Aunque se elimine un contacto y el chat asociado, es posible determinar que dicho chat ha existido y la fecha del primer intercambio de mensajes entre ambos, a partir del momento en que se activó la cuenta en este dispositivo. Estas acciones no eliminan los datos de las tablas **"identities"** y **"sessions"** de la base de datos **"axolotl.db"**.

iOS

La aplicación WhatsApp en iOS puede generar una agenda propia de contactos. Dicha agenda almacena los datos principales en la tabla **"ZWAADDRESSBOOKCONTACT"** de la base de datos **"ContactsV2.sqlite"**, que contiene información sobre el nombre y apellidos del contacto, así como los identificadores "jid" y "lid".

ZFULLNAME	ZGIVENNAME	ZLID	ZWHATSAPPID
Usuario 1	Usuario 1	148846453755945@lid	34[redacted]@s.whatsapp.net

Ilustración 169. Tabla "ZWAADDRESSBOOKCONTACT"

No obstante, se ha observado en distintos modelos de iPhone, versiones de iOS y de WhatsApp en los que no se genera esta base de datos, no hallando el motivo de este comportamiento. Aun así, a partir de la base de datos "**ChatStorage.sqlite**" en combinación con la base de datos "**LID.sqlite**" se puede obtener toda la información necesaria de un contacto.

En la tabla "**ZWCHATSESSION**" de la base de datos "**ChatStorage.sqlite**" se registran todos los chats en los que participa el usuario de esta cuenta, permitiendo localizar los mensajes intercambiados registrados en la tabla "**ZWMESSAGE**", al vincularlos con la sesión de chat del contacto:

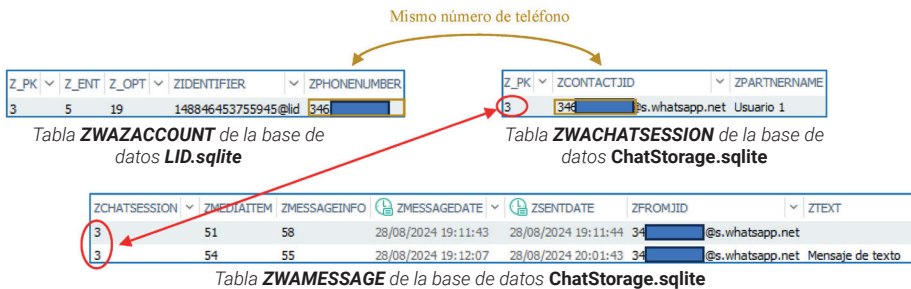


Ilustración 170. Relación entre tablas de la base de datos "LID.sqlite" y "ChatStorage.sqlite"

Eliminación de un contacto:

Tras la eliminación de un contacto pueden quedar vestigios en alguno de los logs que contiene la aplicación, como el identificador "jid" parcial del contacto (4 últimas cifras del número de teléfono). Estos logs se nombran con sus fechas de creación y se localizan en la ruta /private/var/mobile/Containers/Shared/AppGroup/<GUID>/Logs/WhatsApp_2/. La aplicación mantiene los archivos con logs por un periodo corto, aproximadamente entre 3 y 7 días.

Eliminación del contacto de la agenda del teléfono:

```
13:01:55.313 [ 354016] [NSManaged...5520] [B] LL_A contacts//reload/will-delete count=[1]
13:01:55.313 [ 354016] [NSManaged...5520] [B] LL_A contacts//reload/delete-contact id=[44736292-C327-41DE-B09D-5339AB9CC471:ABPerson] waid=[*****0111@s.whatsapp.net>]
```

Aunque se elimine un contacto y el chat asociado, es posible determinar que dicho chat ha existido y la fecha del primer intercambio de mensajes entre ambos, a partir del momento en que se activó la cuenta en este dispositivo. Estas acciones no eliminan los datos de las tablas **"ZWAAXOLOTLIDENTITY"** y **"ZWAAXOLOTLSESSION"** de la base de datos **"axolotl.db"**.

8.1.2. Grupos

Los grupos son una de las entidades cuya identificación ha variado con el tiempo. Existe una fecha crucial en la cual WhatsApp cambió completamente la forma de identificar internamente los grupos.

- a) Antes de mitad de noviembre de 2021: la aplicación generaba el identificador "jid" del grupo con el número de teléfono con prefijo internacional del usuario creador del grupo y la fecha en la que se creó el grupo en formato UTC Unix Epoch (segundos) seguido del nombre del dominio (@g.us). Ejemplo:

34612123123 - 1419072734@g.us → El grupo fue creado por el usuario del teléfono +34 612123123 el día 20 de diciembre de 2014 a las 18:43:49 UTC.

id	jid	display_name
3	34[REDACTED]-1419072734@g.us	Los Tres Mosqueteros

Ilustración 171. Tabla **"wa_contacts"** de la base de datos **"wa.db"** (Android)

- b) A partir de mitad de noviembre de 2021, la aplicación WhatsApp cambia la forma en la que genera el identificador de los chats grupales. El nombre estará formado por 18 dígitos junto con el nombre del dominio para grupos (@g.us).

Z_PK	ZCONTACTJID	ZPARTNERNAME
11	120363328792612948@g.us	Grupo iOS 1

Ilustración 172. Tabla **"ZWCHATSESSION"** de la base de datos **"ChatStorage.sqlite"** (iOS)

Android

Para localizar a todos los participantes de un grupo (válido para los antiguos y los nuevos formatos) es preciso apoyarse en varias tablas de la base de datos **"msgstore.db"**. Conviene no confundir el campo **"jid"** de la tabla **"wa_contacts"**, con la tabla **"jid"** de la base de datos **"msgstore.db"**.

Como ejemplo práctico, queremos localizar a los contactos que conforman el "Grupo restringido" y cuyo identificador "jid" hemos determinado a partir de la tabla **"wa_contacts"** de la base de datos **"wa.db"** que es 120363405612146253@g.us. Estos datos también se podrían obtener enlazando las tablas **"chat"** y **"jid"** de la base de datos **"msgstore.db"**.

_id	jid	is_whatsapp_user	display_name
594	120363405612146253@g.us	1	Grupo restringido

Ilustración 173. Tabla **"wa_contacts"** de la base de datos **"wa.db"**

A continuación, utilizamos las tablas **"jid"** y **"group_participant_user"** de la base de datos **"msgstore.db"**. Aunque la descripción del proceso pueda parecer compleja, el hecho es que a partir de la tabla **"jid"** se obtiene el número de fila (registro) en que se encuentra el grupo, el cual se utiliza en la tabla **"group_participant_user"** para localizar los registros de los miembros del grupo. Con estos registros se vuelve al punto de partida, la tabla **"jid"**, donde se determinan los identificadores "lid" o "jid" de los miembros del grupo.

Hasta mediados del año 2025, los participantes se referenciaban por su identificador "jid", y a partir de dicha fecha se empezó a registrar por su identificador "lid". Como se ha reiterado durante el estudio, el identificador "jid" es el que permite determinar el número de teléfono del participante, pero el hecho de que actualmente se registre el identificador "lid" añade un par de pasos en el análisis para localizar los identificadores "jid" de los participantes en el grupo.

Así, partiendo de la base de datos **"msgstore.db"**, primero nos dirigimos a la tabla **"jid"**, y el campo **"raw_string"** es la identificación asignada por WhatsApp al grupo. En la misma fila se encuentra el campo **"_id"**, que permite localizar todos los contactos integrantes del grupo. El valor de este campo **"_id"** se debe buscar en el campo **"group_jid_row_id"** de la tabla **"group_participant_user"**.

Por cada contacto integrante del grupo existirá una fila con el mismo **"group_jid_row_id"** con un valor único registrado en el campo **"user_jid_row_id"** excepto el usuario de la cuenta analizada que puede tener dos registros

Si estamos en un grupo antiguo, el valor del campo **"user_jid_row_id"** que se corresponde con el campo **"_id"** de la tabla **"jid"**. En esta última tabla, en el campo **"user"** figura el registro del teléfono móvil del participante con el prefijo internacional.

Si el grupo es más moderno (como el del ejemplo), el valor obtenido de la tabla **"jid"** tras el paso anterior es el identificador **"lid"** de los miembros del grupo (el del usuario de la cuenta, y los contactos 148846453755945@lid y 222359768326203@lid). Con estos datos hay que obtener las correspondencias entre los identificadores **"lid"** y **"jid"** de los contactos en la tabla **"jid_map"**, para volver a consultar la tabla **"jid"**:

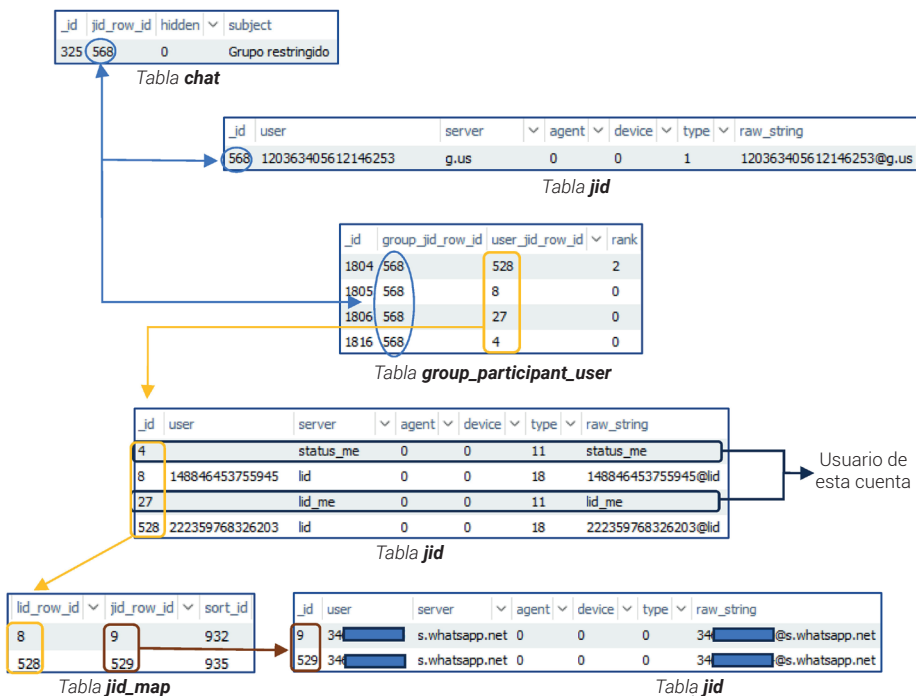


Ilustración 174. Relación entre tablas para determinar los miembros de un grupo

En cualquier caso, estos son ejemplos de la forma en la que se puede relacionar la identificación del grupo y el nombre del grupo con sus miembros, pero dependiendo de la información de la que se parta se puede utilizar multitud de caminos para obtener los datos deseados.

Para determinar el nombre de los contactos se debe consultar la tabla **"wa_contacts"** de la base de datos **"wa.db"** y contrastarlos con los identificadores **"jid"** de los miembros del grupo.

iOS

Los grupos se localizan en la tabla **"ZWACHATSESSION"** de la base de datos **"ChatStorage.sqlite"**. Los grupos presentan el valor **"1"** en el campo **"ZSESSIONTYPE"**.

El número de sesión de chat vincula el grupo con sus participantes. De este modo, el campo **"Z_PK"** de la tabla **"ZWACHATSESSION"** se corresponde con el campo **"ZCHATSESSION"** de la tabla **"ZWAGROUPMEMBER"**. En esta última tabla se almacenan los identificadores **"lid"** de todos los miembros del grupo y también el identificador **"jid"** del usuario de esta cuenta.

Z_PK	Z_SESSIONTYPE	ZCONTACTJID	ZPARTNERNAME
54	1	120363406422734383@g.us	Grupo citaciones

Tabla **ZWACHATSESSION**

Z_PK	Z_ENT	Z_OPT	ZCONTACTABID	ZISACTIVE	ZISADMIN	ZCHATSESSION	ZMEMBERJID
126	6	1	0	0	0	54	34[REDACTED]@s.whatsapp.net
127	6	1	0	1	1	54	148846453755945@lid
128	6	1	0	1	0	54	262074978558186@lid

Tabla **ZWAGROUPMEMBER**

Ilustración 175. Relación entre tablas para determinar los miembros de un grupo

Para obtener los nombres e identificadores **"jid"** de los miembros del grupo a partir de su **"lid"**, puede consultarse las tablas **"ZWACHATSESSION"** de la base de datos **"ChatStorage.sqlite"**, **"ZWAZACCOUNT"** de

la base de datos **"LID.sqlite"** y **"ZWAADDRESSBOOKCONTACT"** de la base de datos **"ContactsV2.sqlite"**. Por otro lado, la información del grupo (creador, fecha de creación, descripción, etc.) es posible ampliarla gracias a la tabla **"ZWAGROUPINFO"**.

8.1.3. Difusiones

La difusión, también llamada "Lista de difusión", es una funcionalidad que permite al usuario enviar el mismo mensaje a varios contactos a la vez.

Si se recibe un mensaje de una difusión, se registra exactamente igual que cuando se recibe un mensaje de un contacto individual, de hecho, el contacto no distinguirá que el mensaje procede de una difusión. Para saber que se trata de un mensaje de una difusión es necesario analizar la base de datos de la cuenta del usuario que creó la difusión y envió el mensaje, o al menos la base de datos de dos usuarios que hayan recibido el mensaje de la difusión, ya que ambos tendrían un mensaje con el mismo identificador de mensaje (**"key_id"** en Android o **"ZSTANZAID"** en iOS).

Android

El identificador "jid" de la difusión se genera con el valor de la fecha en la que se creó en formato UTC Unix Epoch (segundos), seguido del nombre del dominio (@broadcast). Este identificador puede localizarse en el campo **"jid"** de la tabla **"wa_contacts"** de la base de datos **"wa.db"**. El campo **"display_name"** almacena el nombre que ha asignado el usuario a la difusión.

_id	jid	display_name
292	1737883368@broadcast	Difusión para afiliados

Ilustración 176. Tabla **"wa_contacts"**

El modo en el que la aplicación registra a los participantes de una difusión es el mismo que el de un grupo, tal y como se ha mostrado anteriormente. Por ello, se omite la repetición del proceso.

Cuando el usuario envía un mensaje a la difusión, se graban los siguientes registros en la tabla **"message"** de la base de datos **"msgstore.db"**:

- Todos los mensajes generados para los participantes de una difusión, a partir del mensaje enviado por el usuario, comparten la misma **"key_id"**, que identifica el mensaje de manera única, ya que se trata del mismo contenido enviado a todos los contactos agregados a la difusión.
- Se crea un registro consecutivo para cada contacto al que se envía el mensaje. El campo **"chat_row_id"**, vinculado con la tabla **"chat"**, permite determinar el chat de cada contacto. A continuación, desde la tabla **"chat"**, se obtiene el registro de la tabla **"jid"** para identificar finalmente a los contactos añadidos a la difusión y a la difusión en sí misma mediante su identificador **"jid"**.

La difusión también se puede establecer a partir del campo **"sender_jid_row_id"**, que registra el valor que permite vincularlo directamente con la tabla **"jid"** y así obtener el identificador **"jid"** de la difusión.

- El último de los registros creados en la tabla **"message"** corresponde con el de la propia difusión. En este ejemplo es el del campo **"_id" = "3241"**.
- El campo **"broadcast"** registra el valor **"1"**, indicando que son mensajes de una difusión.

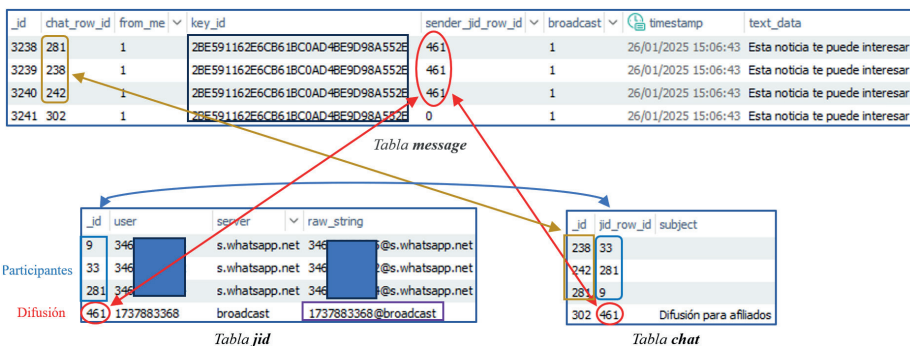


Ilustración 177. Relación entre tablas para determinar los participantes de una difusión del usuario

iOS

Las difusiones se localizan en la tabla **"ZWACHATSESSION"** de la base de datos **"ChatStorage.sqlite"**, y son reconocibles porque todas presentan el valor **"2"** en el campo **"ZSESSIONTYPE"**. Aunque ese valor se asigna tanto a difusiones como a "estados" del usuario, es fácilmente diferenciable por el identificador "jid". En los "estados" del usuario de la cuenta analizada el valor del campo **"ZCONTACTJID"** siempre es "status@broadcast", mientras que en las difusiones son la fecha de creación en formato UTC Unix Epoch (segundos) junto al dominio "@broadcast".

Partiendo del número de sesión de chat (campo **"Z-PK"**) que se corresponde con el valor del campo **"ZCHATSESSION"** de la tabla **"ZWAGROUPMEMBER"**, se localiza a todos los contactos incluidos en la difusión:

Z_PK	ZSESSIONTYPE	ZCONTACTJID	ZPARTNERNAME
9	2	1724967684@broadcast	Lista de difusión

Tabla **ZWACHATSESSION**

Z_PK	Z_ENT	Z_OPT	ZCONTACTABID	ZISACTIVE	ZISADMIN	ZCHATSESSION	ZMEMBERJID
9	6	1	0	1	0	9	346 [redacted]@s.whatsapp.net
10	6	1	0	1	0	9	346 [redacted]@s.whatsapp.net

Tabla **ZWAGROUPMEMBER**

Ilustración 178. Relación entre tablas para determinar los participantes de una difusión del usuario.

Al igual que en Android, cuando se envía un mensaje en una difusión, se generan tantos mensajes como contactos estén agregados. Todos los mensajes generados tienen el mismo identificador de mensaje (campo **"ZSTANZAID"**). Pero la versión de iOS presenta varias peculiaridades, como la falta de información del emisor del mensaje en la tabla **"ZWAGROUPMEMBER"**, si bien por definición el usuario de esta cuenta es siempre el emisor del mensaje en una difusión creada por él mismo. Otra diferencia es que el "status" de los mensajes enviados, aunque hayan sido recibidos por los destinatarios se registran con el valor **"1"**, que generalmente indica que se ha entregado al servidor únicamente. Teniendo la referencia de la sesión de chat (campo **"Z_PK"** de la tabla

"**ZWCHATSESSION**"), que en este caso es "9", se obtiene el número de mensaje (campo "**Z_PK**" de la tabla "**ZWMESSAGE**") que es el mensaje padre de los enviados a los contactos pertenecientes a la difusión (campo "**ZPARENTMESSAGE**" de la tabla "**ZWMESSAGE**"):

Z_PK	ZMESSAGESTATUS	ZCHATSESSION	ZPARENTMESSAGE	ZSTANZAID	ZMESSAGEDATE	ZTEXT	ZTO.JID
269	6	9		3A3D97F7B10D6EAA0FDB	23/09/2024 7:31:27	Otro mensaje al listado	1724967684@broadcast
270	1		269	3A3D97F7B10D6EAA0FDB	23/09/2024 7:31:27	Otro mensaje al listado	34...@s.whatsapp.net
271	1	3	269	3A3D97F7B10D6EAA0FDB	23/09/2024 7:31:27	Otro mensaje al listado	34...@s.whatsapp.net

*Ilustración 179. Tabla "**ZWMESSAGE**"*

8.1.4. Comunidades

Cuando se crea una comunidad, la aplicación genera dos identificadores "jid" únicos para esa comunidad, a diferencia de los contactos individuales, grupos, difusiones o canales que reciben un único "jid" que los identifica. Esto se debe a que uno de ellos es propiamente dicho el identificador de la comunidad, y el otro corresponde al grupo "Avisos", que administra el creador de la comunidad. En este grupo "Avisos", únicamente los administradores de la comunidad pueden enviar mensajes para que los reciban todos los miembros. El grupo "Avisos" presenta en las versiones de la aplicación para ambos sistemas operativos la particularidad de que el nombre asignado automáticamente al grupo por la aplicación ("Avisos") no se encuentra en ninguna base de datos ni archivos de configuración, debiendo deducir cuál es su identificador "jid".

Además, cuando se crea una comunidad se genera otro grupo denominado "General" en el que inicialmente sólo se encuentra el creador de la comunidad como administrador y al que posteriormente todos los miembros de la comunidad pueden unirse libremente. Este grupo "General" está incluido en la comunidad, siendo como cualquier otro grupo que, de forma predeterminada, todos los integrantes pueden enviar mensajes.

Android

Los identificadores de las comunidades siguen las mismas reglas que los de los grupos. Están formados por 18 dígitos junto con el nombre del dominio "@g.us". Estos datos se pueden verificar en la tabla "**wa_contacts**" de la base de datos "**wa.db**", en el campo "**jid**", mientras que el campo "**display_name**" registra el nombre de la comunidad. La única diferencia notable en esta tabla entre un grupo y una comunidad es que la comunidad tendrá dos registros con diferentes identificadores "jid" pero un único valor en el campo "**display_name**" para ambos registros, mientras que un grupo solo tendrá un registro:

jid	display_name
120363320123164021@g.us	Comunidad De Amigos
120363301493900890@g.us	Comunidad De Amigos

Ilustración 180. Tabla "**wa_contacts**"

Un identificador "jid" es utilizado por la aplicación para relacionar los grupos que conforman la comunidad y el otro es el identificador "jid" del grupo "Avisos". En el grupo "Avisos" están incluidos todos los miembros de la comunidad, pero como meros espectadores, pues solo los administradores pueden enviar mensajes. En este ejemplo, 120363301493900890@g.us es el que relaciona los diferentes grupos y 120363320123164021@g.us es el identificador del grupo "Avisos". Como se indicó anteriormente, cuando se crea la comunidad también se genera un grupo "General" que pertenece a ella.

Todas estas relaciones y vinculaciones entre comunidad y grupos quedan registradas en la tabla "**group_relationship**" de la base de datos "**wa.db**". Si la comunidad está formada por más de un grupo, existirán tantas filas con el mismo identificador de la comunidad como grupos estén agregados (en este caso 2 grupos), además del grupo "Avisos" y grupo "General":

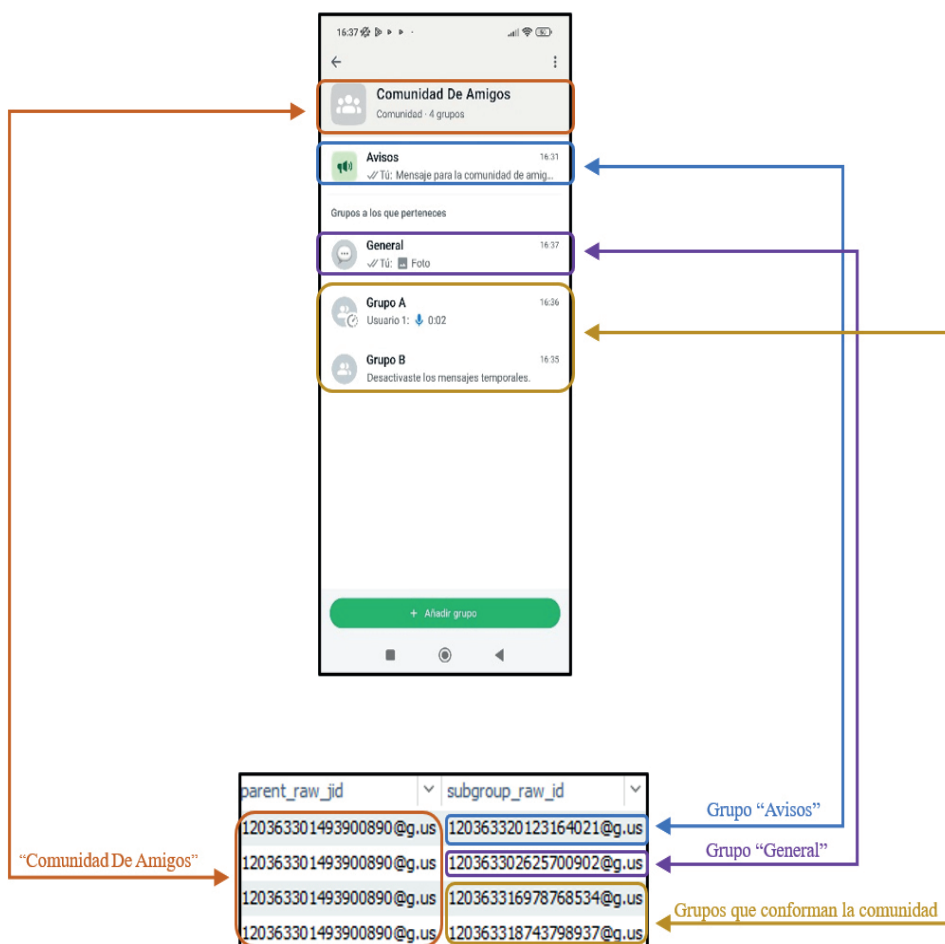


Tabla **group_relationship** (wa.db)

Ilustración 181. Presentación en la interfaz gráfica de la comunidad en la aplicación y base de datos que contiene dicha info.

Partiendo de los identificadores "jid" de los grupos y de la comunidad, obtenidos de la tabla "**group_relationship**" (wa.db), se pueden localizar en la tabla "**jid**" de la base de datos "**msgstore.db**" las filas o registros en los que se encuentran todos estos identificadores "jid". Utilizando la numeración de la fila (campo "**_id**") se obtiene la información de los nombres de los grupos en la tabla "**chat**". Hay que reseñar que la aplicación no asigna ningún nombre al grupo "Avisos" en las bases de datos, por ello, siempre hay que deducir que el chat que no tiene nombre, entre

los que conforman la comunidad, es el grupo "Avisos". En este caso la fila 180 de la tabla "**chat**":

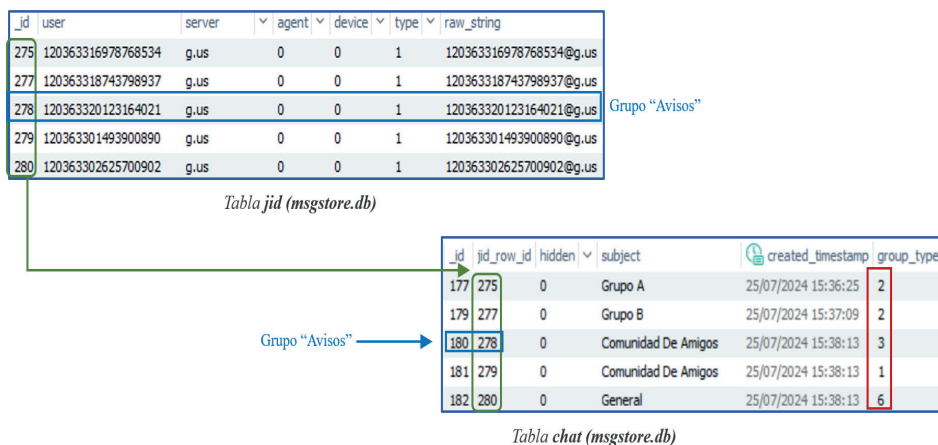


Ilustración 182. Relación entre los identificadores "jid" de una comunidad y sus grupos con sus nombres.

Parte de esta información se puede corroborar con los datos registrados en el campo "**group_type**" de la tabla "**chat**". El valor "**1**" hace referencia a comunidades, el "**2**" a grupos que forman parte de una comunidad, el "**3**" a grupos "Avisos" de las comunidades y "**6**" a grupos "General" de las comunidades.

Las comunidades relacionan a sus miembros por su identificador "lid", que como se ha explicado en el apartado 1.1.2 *LID*, oculta el número de teléfono del usuario con el que creó su cuenta. Para determinar los miembros que forman la comunidad, es necesario tomar el número de registro (campo "**_id**") del identificador "jid" del grupo "Avisos" en la tabla "**jid**". En este ejemplo, dicho número es 278, como se muestra en la ilustración anterior. Con este valor, se obtienen los registros en la tabla "**group_participant_user**" y, al vincularlos con la tabla "**jid**", se obtienen los identificadores "lid" de todos los participantes:

_id	group_jid_row_id	user_jid_row_id	rank	pending	add_timestamp
953	279	4	2	0	25/07/2024 15:38:14
961	278	126	0	0	25/07/2024 15:39:32
962	278	13	0	0	25/07/2024 15:39:13
963	278	62	0	0	25/07/2024 15:39:32
964	278	32	0	0	25/07/2024 15:39:13
965	278	8	1	0	25/07/2024 15:39:13
966	278	27	2	0	25/07/2024 15:38:14
967	278	205	0	0	31/07/2024 6:20:48

_id	user	server	agent	device	type	raw_string
4	status_me		0	0	11	status_me
8	148846453755945	lid	0	0	18	148846453755945@lid
13	242493903896807	lid	0	0	18	242493903896807@lid
27	lid_me		0	0	11	lid_me
32	239156680740886	lid	0	0	18	239156680740886@lid
62	252587093823614	lid	0	0	18	252587093823614@lid
126	45878941360338	lid	0	0	18	45878941360338@lid
205	204101308694769	lid	0	0	18	204101308694769@lid

1. El usuario sea el creador y administrador de la comunidad:

Todos los grupos añadidos a la comunidad son grupos en los que participa este usuario, y todos los contactos añadidos son contactos de su agenda. Por esta razón constan en las bases de datos todos los números de teléfono de los participantes en la comunidad. Esto facilita mucho la identificación de estos miembros, ya que se puede vincular el identificador "lid" con el identificador "jid" (número de teléfono) por medio de la tabla **"jid_map"**.

_id	user	server	agent	device	type	raw_string
8	148846453755945	lid	0	0	18	148846453755945@lid
9	3469	s.whatsapp.net	0	0	0	3469@s.whatsapp.net
13	242493903896807	lid	0	0	18	242493903896807@lid
14	3464	s.whatsapp.net	0	0	0	3464@s.whatsapp.net
32	239156680740886	lid	0	0	18	239156680740886@lid
62	252587093823614	lid	0	0	18	252587093823614@lid
63	3464	s.whatsapp.net	0	0	0	3464@s.whatsapp.net
125	3468	s.whatsapp.net	0	0	0	3468@s.whatsapp.net
126	45878941360338	lid	0	0	18	45878941360338@lid
204	3460	s.whatsapp.net	0	0	0	3460@s.whatsapp.net
205	204101308694769	lid	0	0	18	204101308694769@lid

_id	group_jid_row_id	user_jid_row_id
8	9	
13	14	
62	63	
126	125	
205	204	

Ilustración 183. Relación de identificadores "lid" y "jid" de los participantes de una comunidad

2. El usuario forma parte de la comunidad (no es propietario ni administrador):

El administrador ha incluido en la comunidad un grupo al que pertenece el usuario, o lo ha añadido individualmente. En este caso, el usuario dispondrá de los identificadores "jid" de sus contactos y de los miembros de los grupos a los que pertenece. En los supuestos en que se añada un participante que no sea contacto del usuario o un grupo al que no pertenezca el usuario, solo contará con el identificador "lid".

La única información que se podrá obtener a partir del identificador "lid" y tras consultar la tabla **"lid_display_name"**, será el prefijo internacional y las dos últimas cifras del teléfono del participante. En las tablas

que se han mostrado más arriba, se puede observar que la fila 32 de la tabla **"jid"** corresponde a un identificador "lid" que no tiene aparejado un identificador "jid" en la tabla **"jid_map"**. Esto se debe a que no se trata de un contacto ni un miembro de un grupo del usuario de esta cuenta y por motivos de privacidad la aplicación almacena en la tabla **"lid_display_name"** la información parcial del teléfono:

lid_row_id	display_name
32	+34.....92

Ilustración 184. Tabla **"lid_display_name"**

iOS

Se ha explicado en el apartado de Android, los diferentes identificadores que se generan con la creación de una comunidad, por lo que si es necesario se remite a consultarlo. En iOS el registro de los datos es en general más sencillo, aunque hay datos almacenados en archivos protobuf que deben decodificarse.

Inicialmente se puede detectar la existencia de una comunidad por el valor **"4"** en el campo **"ZSESSIONTYPE"** de la tabla **"ZWACHATSESSION"**. Cuando se crea una comunidad se genera automáticamente el grupo "Avisos", que permite al administrador de la comunidad enviar mensajes a todos los miembros. Es fácil conectar la comunidad con su grupo "Avisos" porque coinciden en el valor del campo **"ZPARTNERNAME"**. Aunque en el dispositivo se muestra como grupo "Avisos", en la base de datos se almacena con el nombre de la comunidad, pero indicando con el valor **"1"** en el campo **"ZSESSIONTYPE"** de que se trata de un grupo. A partir de los datos adquiridos en la tabla **"ZWACHATSESSION"**, se pueden vincular con la tabla **"ZWAGROUPINFO"** y **"ZWAGROUPMEMBER"**, obteniendo la información de su fecha de creación y la identificación de todos los miembros de la comunidad. Por motivos de privacidad, la aplicación almacena la identificación "lid" de los miembros de la comunidad que no son contactos del usuario de esta cuenta, en lugar del identificador "jid".

Z_PK	ZSESSIONTYPE	ZGROUPINFO	ZCONTACTJID	ZPARTNERNAME
58	1	43	120363320123164021@g.us	Comunidad De Amigos
59	4	44	120363301493900890@g.us	Comunidad De Amigos

Tabla ZWACHATSESSION

Z_PK	Z_ENT	Z_OPT	ZSTATE	ZCHATSESSION	ZCREATIONDATE	ZSUBJECTTIMESTAMP	ZCREATORJID
43	5	6	0	58	25/07/2024 15:38:13	25/07/2024 15:38:13	262074978558186@lid
44	5	2	0	59	25/07/2024 15:38:13	25/07/2024 15:38:13	262074978558186@lid

Tabla ZWAGROUPINFO

Z_PK	Z_ENT	Z_OPT	ZCONTACTABID	ZISACTIVE	ZISADMIN	ZCHATSESSION	ZMEMBERJID
142	6	1	0	1	0	58	242493903896807@lid
143	6	1	0	1	0	58	45878941360338@lid
144	6	1	0	0	0	58	346-@s.whatsapp.net
145	6	1	0	1	0	58	204101308694769@lid
146	6	2	0	1	1	58	262074978558186@lid
147	6	1	0	1	0	58	239156680740886@lid
148	6	1	0	1	0	58	222359768326203@lid
149	6	1	0	1	1	58	148846453755945@lid
150	6	2	0	1	1	59	262074978558186@lid
151	6	2	0	1	1	59	148846453755945@lid

Tabla ZWAGROUPMEMBER

Ilustración 185. Relación de identificadores "lid" y "jid" de los participantes de una comunidad

Partiendo de nuevo de los valores de la tabla **"ZWACHATSESSION"**, con el número de sesión de chat (campo **"Z-PK"**) se localiza el primer mensaje registrado en la tabla **"ZWAMESSAGE"** que recibe el grupo **"Avisos"**, que es de la propia comunidad y que contiene en el campo **"ZTEXT"** un archivo JSON con la información de configuración de la comunidad. En el caso de la comunidad, el campo **"ZLASTMESSAGETEXT"** de la tabla **"ZWACHATSESSION"**, almacena codificado en Base64 un archivo protobuf con la información de todos los grupos que forman parte de la comunidad:

Francisco Arenaz Benito

Análisis de características y funcionalidades de interés (Android – iOS)

Z_PK	ZSESSIONTYPE	ZGROUPINFO	ZCONTACTJID	ZLASTMESSAGETEXT	ZPARTNERNAME
58	1	43	120363320123164021@g.us	UhsKFzEyMDM2MzMyMDQ5MzkxMDg5MEBnLnV...	Comunidad De Amigos
59	4	44	120363301493900890@g.us	UgkFzEyMDM2MzMyMDEyMzE2NDYyMUBnLnVz...	Comunidad De Amigos

Tabla ZWCHATSESSION

Z_PK	ZCHATSESSION	ZMESSAGEDATE	ZTEXT
795	58	17/12/2025 23:03:30	{\"author\":\"262074978558186@lid\", \"is_parent_group_general_chat\":false, \"is_initially_empty\":false,

Tabla ZWMESSAGE

```

<Object>
  S author = "262074978558186@lid"
  B is_parent_group_general_chat = False
  B is_initially_empty = False
  O subject
  S parent_group_jid = "120363301493900890@g.us"
  O context_group
  B show_membership_string = False
  B is_hidden_sub_group = False
  B is_open_group = False
  S parent_group_name = "Comunidad De Amigos"
  B auto_add_disabled = True
  I reason = 4
  B should_use_identity_header = False
  
```

Archivo
JSON

Archivo protobuf codificado en Base64
decodificado con Protobuf Decoder

Result						
Byte Range	Field Number	Type	Content			
0-58	10	protobuf	Byte Range	Field Number	Type	Content
			0-25	1	string	120363320123164021@g.us
			25-46	2	string	Comunidad De Amigos
			46-52	3	varint	As uint: 1721921893 As sint: -860960947
			52-54	4	varint	As uint: 1 As sint: -1
			54-56	7	varint	As uint: 0 As sint: 0
58-110	10	protobuf	Byte Range	Field Number	Type	Content
			0-25	1	string	120363302625700902@g.us
			25-34	2	string	General
			34-40	3	varint	As uint: 1721921893 As sint: -860960947
			40-42	6	varint	As uint: 1 As sint: -1
			42-44	7	varint	As uint: 3 As sint: -2
			44-46	8	varint	As uint: 0 As sint: 0
			46-48	9	varint	As uint: 0 As sint: 0
			48-50	11	varint	As uint: 0 As sint: 0

Grupo "Avisos"

Grupo "General"

110-162	10	protobuf	Byte Range	Field Number	Type	Content	Grupo "Grupo A"
			0-25	1	string	120363316978768534@gus	
			25-34	2	string	Grupo A	
			34-40	3	varint	As uint: 1721921785 As sint: -860960893	
			40-42	6	varint	As uint: 0 As sint: 0	
			42-44	7	varint	As uint: 5 As sint: -3	
			44-46	8	varint	As uint: 0 As sint: 0	
			46-48	9	varint	As uint: 0 As sint: 0	
48-50	11	varint	As uint: 0 As sint: 0				
162-214	10	protobuf	Byte Range	Field Number	Type	Content	Grupo "Grupo B"
			0-25	1	string	120363318743798937@gus	
			25-34	2	string	Grupo B	
			34-40	3	varint	As uint: 1721921829 As sint: -860960915	
			40-42	6	varint	As uint: 0 As sint: 0	
			42-44	7	varint	As uint: 3 As sint: -2	
			44-46	8	varint	As uint: 0 As sint: 0	
			46-48	9	varint	As uint: 0 As sint: 0	
48-50	11	varint	As uint: 0 As sint: 0				

214-252	12	string	374DEE99-1CBA-47CF-93CC-9E519CD7BA88			
252-255	19	varint	As uint: 2 As sint: 1			
255-262	20	varint	As uint: 1727122720 As sint: 863561360			
262-265	33	varint	As uint: 1 As sint: -1			
265-272	44	varint	As uint: 1727122720 As sint: 863561360			
272-279	62	varint	As uint: 1727122838 As sint: 863561419			

Ilustración 186. Archivo protobuf del campo “ZLASTMESSAGETEXT”

8.1.5. Canales

Al igual que en los grupos y las comunidades, los canales tienen un identificador “jid” que se asigna cuando se crean. Está formado por 18 dígitos junto con el nombre del dominio para canales (@newsletter). En los canales solo los administradores pueden enviar mensajes y los

seguidores únicamente pueden reaccionar a los mensajes del administrador y votar en las encuestas. El propietario del canal puede proponer a otro contacto o seguidor ser administrador y de igual forma puede ceder la propiedad del canal a otro administrador.

Android

Relacionando las tablas **"jid"** y **"chat"** de la base de datos **"msgstore.db"** se obtiene la información de los canales que el usuario sigue y/o administra. La tabla **"jid"** registra todo canal con el que el usuario ha tenido contacto, y por ello, pueden almacenar multitud de canales que la aplicación ha sugerido al usuario para que los siga, aunque no lo haya hecho. Solo cuando el canal está administrado o seguido por el usuario de la cuenta presenta registro en la tabla **"chat"**.

_id	user	server	agent	device	type	raw_string
197	120363144038483540	newsletter	0	0	21	120363144038483540@newsletter
198	120363169046208812	newsletter	0	0	21	120363169046208812@newsletter

Tabla **jid**

_id	jid_row_id	hidden	subject	created_timestamp	sort_timestamp
86	197	1	WhatsApp	07/07/2023 16:21:35	22/12/2023 16:00:12
87	198	1	LOS40	03/10/2023 10:49:50	26/12/2023 16:32:29

Tabla **chat**

Ilustración 187. Relación entre el identificador "jid" de un canal y su nombre

Las tablas más significativas para el estudio de un canal, además de las expuestas previamente, son **"message"** que contiene los mensajes transmitidos por los canales entre otros, **"newsletter_message"** que registra los identificadores de los mensajes transmitidos en los canales y la cantidad de visualizaciones que ha tenido el mensaje de un canal que sigue o administra el usuario, y **"newsletter_subscribers"** que graba los identificadores "lid" de los suscriptores a los canales administrados por el usuario.

iOS

Los canales se registran con el valor "5" en el campo "ZSESSIONTYPE" de la tabla "ZWCHATSESSION", cuya información puede ampliarse con los datos de la tabla "ZWAGROUPINFO":

Z_PK	ZSESSIONTYPE	ZGROUPINFO	ZLASTMESSAGE	ZCONTACTIDENTIFIER	ZCONTACTJID	ZPARTNERNAME
18	5	9	23/09/2024 20:47:44	23/09/2024 20:39:06	120363321516136658@newsletter	Canal de usuario iOS
19	5	10	07/10/2024 16:01:37	07/07/2023 16:21:35	120363144038483540@newsletter	WhatsApp

Tabla ZWCHATSESSION

Z_PK	ZPICTUREID
9	+CkEKEDE3MjcxMjQwMzMyMTM0ODgaLUNhbmFsIHhcmEgaGFibGFyIGRIIGNvc2FzIGRIIHdoYXRzYXBwIGVuiElvcxIISABQ...
10	+Cn0KEDE2ODk2NTM4Mzk0NTA2NigaaVdoYXRzOXBw4oCZcvBvZmZpY2lhbCBiaGFubmVsljBGB2xsb3cnZm9yIG91cB5YXRj...

Tabla ZWAGROUPINFO

Ilustración 188. Registro en los canales en las tablas de la base de datos "ChatStorage.sqlite"

El campo "ZPICTUREID" de la tabla "ZWAGROUPINFO", contiene un archivo protobuf codificado en Base64 con información del canal. Para la correcta interpretación de la información contenida en el campo referido, debe eliminarse el carácter "+" y decodificar la información de Base64 a hexadecimal (protobuf) y posteriormente decodificar el archivo protobuf.

Una vez decodificado, la información más relevante es la siguiente:

Campo	Campo	Descripción
1	1	Fecha en la que se describió el canal en formato UTC Unix Epoch (milisegundos).
	3	Descripción del canal.
20		Número de seguidores del canal.
30	1	Identificador "lid" de un seguidor que ha interactuado con canal (habrá tantos campos como seguidores, siempre que el usuario de esta cuenta sea el administrador).

Ilustración 189. Archivo protobuf del campo "ZPICTUREID" de la tabla "ZWAGROUPINFO"

En el caso de que el canal esté administrado por el usuario de esta cuenta y el seguidor sea un contacto de la agenda de éste, gracias al campo "30-1" (identificador "lid" del seguidor) podrá vincularse con su número de teléfono e identificarlo con la tabla **"ZWAADDRESSBOOK-CONTACT"** de la base de datos **"ContactsV2.sqlite"** o través de la tabla **"ZWAZACCOUNT"** de la base de datos **"LID.sqlite"**

ZFULLNAME	ZGIVENNAME	ZHIGHLIGHTEDNAME	ZLID	ZPHONENUMBER
Usuario 1	Usuario 1	Usuario 1	148846453755945@lid	+34 [REDACTED]
Usuario Android	Usuario	Android	262074978558186@lid	+34 [REDACTED]

Ilustración 190. Tabla **"ZWAADDRESSBOOKCONTACT"** de la base de datos **"ContactsV2.sqlite"**

ZIDENTIFIER	ZPHONENUMBER
262074978558186@lid	34 [REDACTED]
148846453755945@lid	34 [REDACTED]

Ilustración 191. Tabla **"ZWAZACCOUNT"** de la base de datos **"LID.sqlite"**

8.2. Nomenclatura de archivos transmitidos por Whatsapp

La nomenclatura específica para los distintos archivos por parte de la aplicación solo se presenta en su versión de Android.

Android

Cuando un archivo es enviado o recibido por medio de la aplicación, ésta le asigna un prefijo diferenciador según el tipo de archivo, fecha de grabación en el dispositivo y una numeración creciente en un mismo día. Será el dispositivo el que asigne el nombre al archivo, por lo que cuando se transmite entre dos usuarios no tiene por qué coincidir en ambos dispositivos, y de hecho habitualmente no lo tienen.

El inicio del nombre asignado consiste en tres letras que hacen referencia al tipo de archivo enviado o recibido:

- **VID:** archivos de vídeo (incluidos los GIFs).

- **IMG**: archivos de imagen.
- **AUD**: archivos de audio.
- **PTT**: nota de voz.
- **PTV**: nota de vídeo.
- **STK**: stickers.
- **DOC**: los documentos son una excepción. La aplicación emplea esta nomenclatura en los archivos enviados como documentos (ya sean documentos propiamente dicho como pdf, texto, hoja de cálculo, etc. o archivos multimedia como vídeos, audios, fotografías...), pero los archivos recibidos en este dispositivo, que hayan sido transmitidos como documentos por el otro contacto, conservarán su nombre original y por tanto la aplicación no le asignará ningún nombre nuevo.

El siguiente dato que se añade es la fecha en formato año-mes-día del dispositivo.

El final del nombre incluye el acrónimo de WhatsApp (WA) seguido de la numeración secuencial de archivo transmitido, comenzando por 0000 e incrementado en una unidad en el siguiente archivo. La numeración se reinicia cada día, empezando de nuevo por 0000, siguiendo por 0001, 0002... siendo indiferente el tipo de archivo y si ha sido enviado o recibido.

Ejemplos:

- Se envía una imagen el día 27 de octubre de 2025 y es el primer archivo que se ha grabado en el sistema de archivos del usuario:
IMG-20251027-WA0000
- El segundo archivo grabado es un archivo de audio que hemos recibido:
AUD-20251027-WA0001
- Así irá aumentando secuencialmente durante todo el día y se reiniciaría a WA0000 a las 00:00 horas del día siguiente.

Pero toda regla tiene sus excepciones, que conviene aclarar:

Los mensajes de “visualización única” *recibidos*, tanto las imágenes y vídeos como las notas de voz tienen su propia nomenclatura, iniciando por IMG (imagen), VID (vídeos) o AUD (notas de voz), seguidos por ocho caracteres y la extensión del tipo de archivo. No es muy probable que en un análisis de un dispositivo localicemos un archivo de este tipo, ya que tras su reproducción es eliminado automáticamente por la aplicación. En el caso de que se hayan descargado en el dispositivo y que el usuario no los haya abierto, se encontrarán en el directorio **/data/data/com.whatsapp/files/ViewOnce** o similar.

Ejemplos de nombres de archivos:

- **IMG-lqn09qmy.jpg** (imagen de visualización única)
- **VID-lqmzz7hh.mp4** (vídeo de visualización única)
- **AUD-lqn05ag5k.opus** (nota de voz de visualización única)

Por otro lado, las imágenes, vídeos y notas de voz publicadas en los “Estados” por contactos del usuario son almacenados en la ruta **.../Media/.Statuses/** y son nombrados con 32 caracteres hexadecimales, hasta que tras 24 horas son eliminados de dicha ubicación. Los publicados por el propio usuario mantienen la nomenclatura habitual y se graban en los subdirectorios para cada tipo de archivo que son enviados (**.../sent/**).

Full path	Modified (GMT+0)
/data/media/0/Android/media/com.whatsapp/WhatsApp/Media/.Statuses/c02085ab12b247d8bc500dbc156b3268.mp4	14/01/2025 15:53:23
/data/media/0/Android/media/com.whatsapp/WhatsApp/Media/.Statuses/48e4db9f6b864ce2a6a92e19caef72d1.mp4	14/01/2025 15:53:22
/data/media/0/Android/media/com.whatsapp/WhatsApp/Media/.Statuses/25bc9f18a2e146d4b81ac6b94a60631e.mp4	14/01/2025 15:53:23

Ilustración 192. Ruta y nombre de archivos publicados por contactos del usuario en sus “Estados” (Explorador de archivos)

iOS

En la versión para sistema operativo iOS, WhatsApp asigna a los archivos generados o transmitidos un “UUID⁵” formado por una secuencia de 32 valores hexadecimales divididos en 5 grupos separados por guiones (8-4-4-4-12 valores) seguido por la extensión del archivo.

5. universally unique identifier o identificador único universal.

Como excepción a esta regla se encuentran los documentos. Al igual que en la versión de Android, los archivos recibidos transmitidos como documentos se almacenan conservando su nombre original. También constituyen una excepción los archivos escaneados a través de WhatsApp, a los cuales la aplicación asigna el nombre:

- WhatsApp Scan AAAA-MM-DD at hh.mm.ss.pdf⁶

8.3. Confirmación de recepción y lectura de mensajes

En la interfaz gráfica de la aplicación, las confirmaciones de lectura se muestran junto a los mensajes que se envían, y cada una de ellas indica la siguiente información:

- ✓ El mensaje se envió correctamente.
- ✓✓ El mensaje se entregó correctamente en el teléfono principal o los dispositivos vinculados del destinatario incluso si el teléfono principal se encuentra apagado. En los chats grupales, el segundo tic aparecerá cuando todos los participantes del grupo hayan recibido el mensaje.
- ✓✓ El destinatario o destinatarios han leído el mensaje.



Ilustración 193. Diferentes estados de confirmación de lectura de los mensajes en iOS (similar en Android)

6. En el que AAAA es año, MM mes, DD día, hh horas, mm minutos y ss segundos en el que se escaneó el documento.

El usuario puede seleccionar en Ajustes>Privacidad>Confirmaciones de lectura, que se confirme o no la lectura de los mensajes. Si se selecciona que no se confirme la lectura de los mensajes recibidos tampoco se recibirá confirmaciones de lectura de los mensajes enviados a los contactos. En el caso de chats de grupo, esta opción no tiene efecto, ya que siempre se confirmará la lectura de los mensajes.

La información que se puede obtener de la confirmación de lectura de un mensaje, de la reproducción de notas de voz/vídeo o mensajes de visualización única, dependerá directamente de esta opción y del modo en el que esté configurado tanto en la cuenta del usuario del dispositivo analizado como en la del otro participante en el chat. Si uno de los dos usuarios tiene desactivada la confirmación de lectura, afectará a ambos.

Lógicamente, los desarrolladores de la aplicación han decidido que prevalezca la opción de privacidad más restrictiva, aplicándola de forma recíproca entre los usuarios. Esto implica que, si el Usuario X desactiva la confirmación de lectura, ninguno de sus contactos recibirá confirmaciones de lectura de los mensajes que él reciba. Pero el Usuario X tampoco obtendrá confirmaciones de lectura de los mensajes que envíe al resto de contactos, independientemente de la configuración de lectura que hayan dispuesto los demás.

Si la confirmación de lectura está activa en los dos participantes de un chat, la aplicación interpreta o considera “leídos” los mensajes, simplemente por la acción de que el *usuario abra el chat* en el que se encuentran. Se puede dar la circunstancia de que se reciba un archivo (fotografía, vídeo, audio, documento...) y ni siquiera haya descargado el archivo recibido, pero al haber abierto el chat, la aplicación confirmará y notificará su lectura, aunque el archivo no se encuentre en el dispositivo.

Por ello, aunque la opción se denomine “confirmación de lectura”, en realidad indica únicamente que el contacto ha abierto el chat donde se encuentran los mensajes. *En ningún caso significa que haya descargado las notas de vídeo, archivos multimedia (imagen, vídeo, audio) o*

documentos, ni que los haya reproducido. Las notas de voz se descargan automáticamente, independientemente de la configuración de la cuenta.

Por lo tanto, cuando se trata de un mensaje recibido en el dispositivo analizado, debe confirmarse además la descarga de los ficheros recibidos en la base de datos correspondiente según el sistema operativo. Para asegurar que el usuario ha tenido posibilidad de visualizar el archivo (descargado), en Android habría que consultar la tabla "**message_media**" de la base de datos "**msgstore.db**" y en iOS la tabla "**ZWAMEDIAITEM**" de la base de datos "**ChatStorage.sqlite**".

8.3.1. Mensajes enviados y recibidos (Android)

Para el análisis de la configuración de la confirmación de lectura, se deberá examinar el archivo "**com.whatsapp_preferences_light.xml**":

Nombre y valor del parámetro	Significado de los valores
 boolean name = read_receipts_enabled value = true	Confirmación de lectura: True: activada. False: desactivada

*Ilustración 194. Archivo **com.whatsapp_preferences_light.xml***

La activación o desactivación de la confirmación de lectura tiene un efecto directo en qué fechas se graban o no en la base de datos "**msgstore.db**". Para aclarar la relación que tienen las distintas tablas en la información que registran sobre la entrega, lectura y reproducción de mensajes se va a exponer una relación visual entre las distintas tablas. Las tablas están relacionadas por fila (campo "**_id**") de la tabla "**message**" del mensaje que analizaremos:

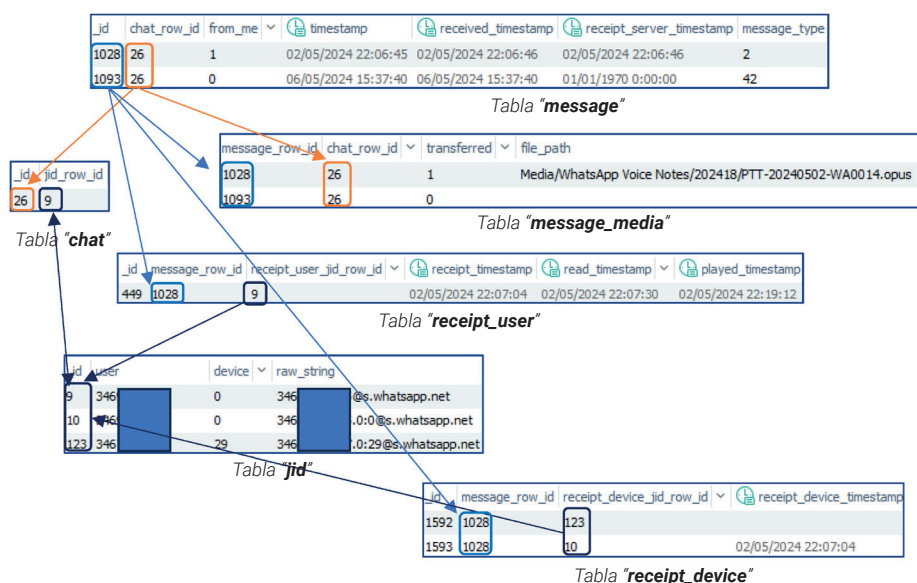


Ilustración 195. Relación entre tablas en la recepción de mensajes

1. El mensaje de la fila 1028 (tabla "**message**"), es una nota de voz (message_type="2"); el nombre del archivo empieza por "PTT" (tabla "**message_media**"), y enviada por el usuario de esta cuenta (from_me="1"). Ha sido recibido, abierto y reproducido (tabla "**receipt_user**") por el usuario registrado en la fila 9 de la tabla "**jid**", cuyo dispositivo principal (0:0) está registrado en la fila 10 de la tabla "**jid**". La nota de voz también se ha enviado al dispositivo vinculado número 29 que está registrado en la fila 123 de la tabla "**jid**", pero en el momento del envío no se estaba en línea y no lo recibió (sin fecha en el campo "**receipt_device_timestamp**" de la tabla "**receipt_device**").
2. El mensaje de la fila 1093 (tabla "**message**"), es una imagen de visualización única recibida por el usuario de esta cuenta (from_me="0"). No ha sido descargado por el usuario (transferred="0") y por ello no aparece en la tabla "**message_media**" la ruta en la que se debería haber grabado. Es importante comprobar este último extremo, porque si lo hubiese descargado y no apareciera la ruta significaría que el usuario lo habría visualizado, tras lo cual la aplicación la habría borrado automáticamente. Al ser un mensaje recibido en esta cuenta, no se registra información en las tablas "**receipt_user**" y "**receipt_device**".

- a) **ENVIADO**: cuando es un mensaje enviado, la aplicación almacena la información en el campo "**status**" de la tabla "**message**" de forma secuencial. Dependiendo de si en el chat se encuentra activa o no la confirmación de lectura para ambos participantes, la secuencia se detendrá en un valor u otro:



*Ilustración 196. Valores del campo "**status**" de la tabla "**message**" de mensajes enviados*

Independientemente de la configuración de la confirmación de lectura, todos los **mensajes del sistema y llamadas/videollamadas** ("message_type" = "7" y "90"), se registran en el campo "**status**" con el valor "**6**". Además, los mensajes del sistema siempre son grabados como mensajes enviados.

Entre las tablas que se van a exponer, las diferencias que existen cuando hay o no confirmación de lectura son en la tabla "**message**", explicado en el párrafo anterior, y en la tabla "**receipt_user**" que, cuando está activa la confirmación de lectura, registra la fecha de "lectura" de los mensajes y la fecha reproducción notas de voz/vídeo y mensajes de visualización única:

Tabla MESSAGE:

timestamp: fecha de inicio del envío del mensaje en formato UTC Unix Epoch (milisegundos)

received_timestamp: fecha del envío del mensaje tras el tiempo de procesamiento para el envío del mensaje, generalmente unos pocos segundos después del valor del campo "**timestamp**".

Toma el valor "**0**" cuando es un mensaje de texto, tarjeta de contacto, una encuesta, un registro de llamada, mensaje de cambio de temporalidad o un mensaje del sistema.

receipt_server_timestamp: fecha de la recepción del mensaje en el servidor de la aplicación en formato UTC Unix Epoch (milisegundos). Se muestra en el mensaje un tic gris ✓. Si se trata de un envío desde otro dispositivo vinculado a esta cuenta o un mensaje del sistema el valor será "-1".

Tabla RECEIPT_DEVICE:

receipt_device_jid_row_id: fila de la tabla "jid" vinculando ambas tablas. Indica los dispositivos receptores del mensaje, también los vinculados.

receipt_device_timestamp: fecha de recepción del mensaje por el contacto en formato UTC Unix Epoch (milisegundos). Se muestra en el mensaje doble tic gris ✍.

Tabla RECEIPT_USER:

message_row_id: fila de la tabla "message", vinculando ambas tablas.

receipt_user_jid_row_id: fila de la tabla "jid" del contacto que ha recibido el mensaje enviado.

receipt_timestamp: fecha en la que el contacto ha recibido el mensaje en su dispositivo en formato UTC Unix Epoch (milisegundos). Se muestra en el mensaje doble tic gris ✍. Es la misma fecha que el campo "**receipt_device_timestamp**" de la tabla "**receipt_device**".

read_timestamp: fecha en la que se ha abierto el chat del mensaje por el contacto en formato UTC Unix Epoch (milisegundos). Se muestra en el mensaje doble tic azul ✍. La confirmación de lectura debe estar activada en ambos usuarios.

played_timestamp: fecha en la que se ha reproducido el mensaje por el contacto en formato UTC Unix Epoch (milisegundos), en notas de voz/vídeo y en mensajes de visualización única. Se muestra en el mensaje doble tic azul ✍. La confirmación de lectura debe estar activada en ambos usuarios.

- b) RECIBIDO:** cuando es un mensaje recibido, no existen diferencias en los valores registrados por la aplicación, esté o no activa la confirmación de lectura. Esto resulta lógico, ya que solo implica

acciones del propio usuario y no vulnera la privacidad del contacto emisor del mensaje:

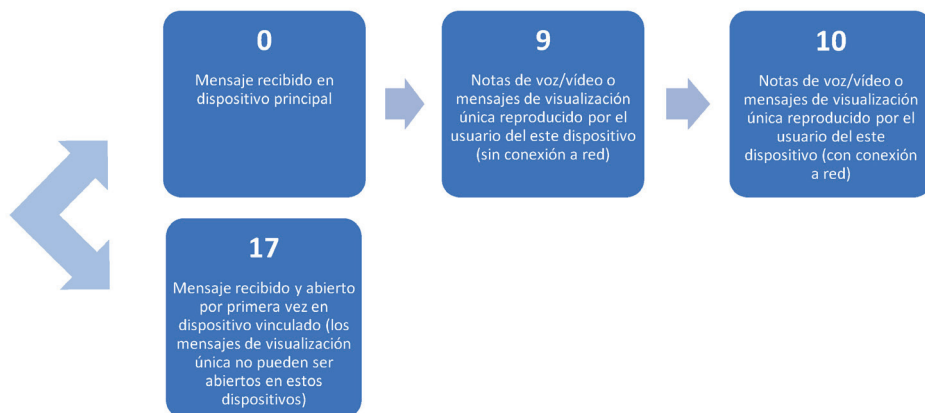


Ilustración 197. Valores del campo **"status"** de la tabla **"message"** de mensajes recibidos

Las **llamadas/videollamadas** ("message_type" = "90") se registran con valor en el campo **"status"** de **"6"**.

En los mensajes recibidos la tabla **"message"** registra marcas de tiempo del envío y recepción del mensaje, pero las tablas **"receipt_device"** y **"receipt user"** no contienen información de la recepción, lectura o reproducción de mensajes:

Tabla MESSAGE:

timestamp: fecha de envío del mensaje desde el dispositivo emisor en formato UTC Unix Epoch (milisegundos).

received_timestamp: fecha de recepción del mensaje en el dispositivo analizado en formato UTC Unix Epoch (milisegundos).

Toma el valor **"0"** en registros de llamada.

receipt_server_timestamp: el valor es **"-1"**.

Si el usuario de esta cuenta tiene desactivadas las "Confirmaciones de lectura", las notas de voz, notas de vídeo y mensajes de visualización única (archivo de imagen, archivo de vídeo o nota de voz) recibidos en esta cuenta y reproducidos por el usuario, se registrarán en la tabla **"played_self_receipt"**.

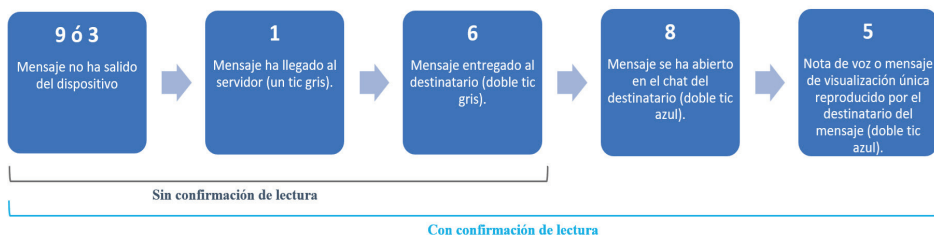
8.3.2. Mensajes enviados y recibidos (iOS)

En iOS se debe consultar el archivo de configuración "**group.net.whatsapp.WhatsApp.shared.plist**" para confirmar si se encuentra establecida la confirmación de lectura:

Nombre y valor del parámetro	Significado de los valores
 ReadReceiptsOff = False	Confirmación de lectura: True: activada. False: desactivada

*Ilustración 198. Opciones de confirmación de lectura en el archivo "**group.net.whatsapp.WhatsApp.shared.plist**"*

- a) **ENVIADO:** cuando se trata de un mensaje enviado, la forma en la que la aplicación almacena la información en el campo "**ZMESSAGESTATUS**" de la tabla "**ZWAMESSAGE**" es secuencial. Dependiendo del estado de la opción de la confirmación de lectura en el chat para los dos participantes, la secuencia se detendrá en un valor u otro. Además de los valores que adoptan en la secuencia, hay otra diferencia significativa respecto a la versión de Android, y es que el último valor no registra la reproducción de las notas de vídeo:



*Ilustración 199. Valores del campo "**ZMESSAGESTATUS**" de la tabla "**ZWAMESSAGE**" de mensajes enviados*

En las difusiones, como se ha explicado anteriormente, se registran 2 tipos de mensajes en la tabla "**ZWAMESSAGE**", el de la propia difusión y el mensaje enviado a cada uno de los integrantes en la difusión. El mensaje de la difusión sigue la misma secuencia

que se ha descrito arriba, teniendo en consideración que todos los miembros de la difusión deben tener confirmación de lectura para se aplique esta opción al mensaje. El mensaje enviado a cada uno de los participantes en la difusión siempre se le asigna el valor "1" al campo "ZMESSAGESTATUS".

Independientemente de la configuración de la confirmación de lectura, los **mensajes de cambio de temporalidad del chat, llamadas/videollamadas** ("message_type" = "28" o "59"), se registran con valor en el campo "ZMESSAGESTATUS" de "0".

- b) **RECIBIDO:** cuando es un mensaje recibido, no hay diferencia alguna en los valores que graba la aplicación si la confirmación de lectura se encuentra activa o no. Es lógico que se registre de igual modo, ya que únicamente implica a las acciones del propio usuario y no invade la privacidad del contacto emisor del mensaje:



Ilustración 200. Valores del campo "ZMESSAGESTATUS" de la tabla "ZWAMESSAGE" en mensajes recibidos

Los **mensajes del sistema, del cambio de temporalidad del chat, llamadas/videollamadas o mensaje de creación de canal por el usuario** ("message_type" = "6", "10", "28", "59" o "62"), se registran con valor en el campo "ZMESSAGESTATUS" de "0". Además, los mensajes del sistema siempre son grabados como mensajes recibidos.

8.4. Vinculación de dispositivos

La aplicación permite vincular hasta **4 dispositivos** al teléfono principal. Los dispositivos vinculados pueden ser teléfonos y tabletas (Android, iOS, iPadOS y KaiOS), ordenadores (navegador web o aplicación de escritorio para Windows o macOS), smartwatches (Wear OS) y gafas VR Oculus. Los dispositivos vinculados únicamente pueden acceder a los mensajes transmitidos en el **último año** y cada dispositivo se conecta a WhatsApp de forma independiente mediante cifrado de extremo a extremo.

Aunque se encuentre apagado el dispositivo principal o sin conexión, los dispositivos vinculados funcionarán con normalidad con la aplicación; no obstante, si en **14 días** no se vuelve a conectar el dispositivo principal, los dispositivos vinculados se desconectarán automáticamente. Cuentan con todas las funcionalidades, salvo la recepción y emisión de archivos de visualización única, crear difusiones y ver ubicación en tiempo real.

Cuando el dispositivo principal se vuelve a conectar a la red, sus bases de datos se actualizan automáticamente con los cambios que se hayan producido en los dispositivos vinculados en cuanto al envío, recepción, lectura o eliminación de mensajes, pero si se han descargado archivos en los dispositivos vinculados, no se replicarán en el dispositivo principal y viceversa.

Para numerar los dispositivos, la aplicación utiliza los identificadores "jid" y "lid" de la cuenta y les añade el número asignado al dispositivo. En todos los sistemas operativos el registro de los dispositivos es secuencial, de modo, que el dispositivo principal siempre tendrá la numeración "0". Posteriormente se incrementa en una unidad cada vez que un dispositivo se vincula (1, 2, 3, etc.). La aplicación conserva la numeración de los dispositivos de una cuenta y continúa incrementando en sucesivas vinculaciones y desvinculaciones, aun cuando se desinstale la aplicación y se vuelva a instalar en el mismo u otro teléfono.

Los identificadores "jid" de los dispositivos vinculados se obtienen de las bases de datos "**companion_devices.db**" en Android y "**LocalKeyValue**."

sqlite" en iOS, teniendo que analizar diferentes bases de datos para obtener los identificadores "lid" con los que se corresponden.

Cada vez que un usuario vincula su cuenta a la aplicación en el navegador (WhatsApp Web), se registrará como tal. Por ello puede llegar a observarse dispositivos vinculados con numeración alta debido a que el usuario habitualmente vincule y desvincule la cuenta de un ordenador. Cuando un mismo dispositivo se vincula y desvincula en varias ocasiones, se le asigna un nuevo número en cada una de ellas. Ejemplo:

Identificador jid	Identificador lid	Dispositivo
34655123123.0@s.whatsapp.net	218476530688052.1.0@lid	Dispositivo principal, su numeración es "0"
34655123123.0:5@s.whatsapp.net	218476530688052.1.5@lid	5º dispositivo vinculado
34655123123.0:8@s.whatsapp.net	218476530688052.1.8@lid	8º dispositivo vinculado

Ilustración 201. Ejemplo hipotético de identificadores de dispositivos en sistemas Android.

Identificador jid	Identificador lid	Dispositivo
34655123123:0@whatsapp.net	218476530688052:0@lid	Dispositivo principal, su numeración es "0"
34655123123:5@whatsapp.net	218476530688052:5@lid	5º dispositivo vinculado
34655123123:8@whatsapp.net	218476530688052:8@lid	8º dispositivo vinculado

Ilustración 202. Ejemplo hipotético de identificadores de dispositivos en sistemas iOS.

En este caso hay dos dispositivos vinculados y los dispositivos que se vincularon cronológicamente en 1º, 2º, 3º, 4º, 6º y 7º lugar, se encuentran actualmente desvinculados.

El análisis de un dispositivo vinculado presenta ciertas particularidades. La numeración de los registros en las bases de datos cambia totalmente respecto a las del dispositivo principal. La información registrada en las diferentes tablas de las bases de datos de ambos dispositivos es la misma, pero se localizan en filas cuya numeración es distinta. Esto es debido a que la grabación en las bases de datos de los mensajes

depende de las sincronizaciones. Es habitual que si el dispositivo no está conectado a red cuando recibe o envía los mensajes, en el momento que se conecte y se sincronicen los mensajes, éstos generalmente se graban en bloques pertenecientes a un mismo chat y no por la fecha en la se transmitieron. Este es el motivo de las divergencias que pueden presentarse entre las bases de datos de distintos dispositivos de una misma cuenta.

Android

Para poder determinar los dispositivos que se encuentran actualmente vinculados con el dispositivo principal hay que consultar la tabla "**devices**" de la base de datos "**companion_devices.db**". En dicha tabla se verifica el sistema operativo del dispositivo y la aplicación o navegador web utilizado por el dispositivo vinculado.

También se puede obtener información más limitada de los dispositivos vinculados a través de la tabla "**jid**" de la base de datos "**msgstore.db**". Dicha tabla registra todos los dispositivos vinculados con el propio dispositivo principal, así como los dispositivos vinculados de otros contactos con los que se haya tenido comunicación. En esta tabla no se graba si un dispositivo vinculado (propio) continúa en la actualidad vinculado o no, hecho que se comprobará en la tabla "**devices**".

Las bases de datos no son la única fuente de información que se puede consultar. Aunque mucho más limitada temporalmente, la vinculación también se registra en los "logs" de la aplicación, indicando el tipo de sistema operativo, navegador web/aplicación, fecha de activación UTC Unix Epoch (milisegundos), entre otros datos:

```
2025-01-25 12:29:58.503 LL_J W [207:High Pri Worker #14] HistorySyncManager/startMessageHistorySync for Device jid: 2237:38@s.whatsapp.net, Platform type: CHROME, Device OS: Windows, Last active: 1737808202753, Login time: 1737808202753, Logout time: 0, ADV Key Index: 1, full sync required: false, Place Name: null, History sync config info: fullSyncDaysLimit: null, fullSyncSizeMbLimit: null, storageQuotaMb: 449513, inlineInitialHistSyncPayloadEnabled: true, recentSyncDaysLimit: null, supportCallLogHistory: false, supportBotUserAgentChatHistory: true, supportCagReactionsAndPolls: true, supportRecentSyncChunkMessageCountTuning: true, supportHostedGroupMsg: true, supportBizHostedMsg: true, Nickname: null
```

Para establecer desde qué dispositivo se ha enviado un mensaje, tanto enviados desde la cuenta analizada como los recibidos (enviados por contactos), es necesario saber la fila (campo “_id”) del mensaje de interés de la tabla “**message**”. Este valor permite enlazar el mensaje con el número de dispositivo a través de la tabla “**message_details**” y la tabla “**jid**”.

Cuando el usuario de esta cuenta envía un mensaje desde un dispositivo vinculado, es posible obtener información sobre dicho dispositivo en la base de datos “**companion_devices.db**”, siempre que el dispositivo siga vinculado o se haya recuperado la información tras su desvinculación (archivo WAL):



*Ilustración 203. Relación de las tablas de la base de datos “**msgstore.db**” con la base de datos “**companion_devices.db**”*

También es posible determinar el número de dispositivo de un contacto que ha recibido un mensaje enviado por el usuario de esta cuenta (puede ser más de un dispositivo). Iniciando el análisis desde la fila (campo “_id”) del mensaje que es de interés en la tabla “**message**”, se vincula con la tabla “**receipt_device**” la cual dirige hacia la tabla “**jid**”, donde se obtiene la identificación del dispositivo vinculado con el identificador “**jid**” del contacto. Para conocer el tipo exacto de dispositivo que lo recibió sería necesario acceder a las bases de datos del teléfono del contacto. En el siguiente ejemplo, el dispositivo vinculado del contacto número “6” recibió el mensaje:

_id	key_id	from_me	timestamp	received_timestamp	message_type	text_data
2121	F403AB7904AC693CC843C9513ECAAC96	1	02/10/2024 11:26:36	1727868399466	3	Mensaje de 5 segundos

Tabla **message**

_id	message_row_id	receipt_device_id_row_id	receipt_device_timestamp
2942	2121	304	02/10/2024 11:26:40

Tabla **receipt_device**

_id	user	server	agent	device	type	raw_string
304	346	s.whatsapp.net	6	17	346	1.016@s.whatsapp.net

Tabla **jid**

Número de dispositivo

Ilustración 204. Relación de tablas para la identificación del dispositivo receptor del mensaje.

Cuando un mensaje es recibido por el usuario de la cuenta analizada, se abre antes en un dispositivo vinculado antes que en el principal, el campo “**status**” de la tabla “**message**” registrará el valor “**17**”.

Recuperación de datos de vinculación:

La base de datos “**companion_devices.db**” únicamente guarda la información de los dispositivos actualmente vinculados, pero dispone del archivo **WAL**, que puede almacenar algunos de los últimos dispositivos desvinculados. De tal forma que, entre los datos recuperables, en ocasiones está la fecha en la que se desvinculó (logout_time).

_id	device_id	device_os	platform_type	last_active	login_time	logout_time
2	346	.0:28@s.whatsapp.net	Mac OS	5	07/04/2024 23:47:46	07/04/2024 14:06:25
3	346	.0:29@s.whatsapp.net	Windows	6	08/04/2024 16:57:45	08/04/2024 16:57:45
1	346	.0:27@s.whatsapp.net	iOS	1	07/04/2024 14:04:09	10/03/2024 21:26:47

Dispositivo desvinculado

Dispositivos actualmente vinculados

Ilustración 205. Tabla **devices** de la base de datos **companion_devices.db**. Registro recuperado del archivo WAL (amarillo)

La posibilidad de recuperación del registro de una vinculación depende del tiempo transcurrido desde su desvinculación y la cantidad de dispositivos vinculados y desvinculados posteriormente. En el ejemplo arriba expuesto, el dispositivo vinculado número 27 (“_id” = “1”) es el único registro eliminado y recuperado. Fue desvinculado a las 16:55 horas del día 08/04/2024 (UTC).

iOS

Hasta mediados del año 2025, la información referente a los dispositivos vinculados se almacenaba en la tabla **"ZWASMBDEVICEAGENT"** de la base de datos **"DeviceAgents.sqlite"** (ver apartado 5.5 *BASE DE DATOS DeviceAgents.sqlite*).

En la última versión analizada de iOS 2.25.32.77, se han identificado dos ubicaciones en las que la aplicación almacena información relacionada con la vinculación de dispositivos, si bien únicamente son accesibles mediante extracción FFS. Por un lado, en la base de datos **"LocalKeyValue.sqlite"**, y por otro, en los **registros de logs** de la aplicación.

LocalKeyValue.sqlite

En la tabla **"ZWAKEYVALUEELEMENT"** de esta base de datos se encuentra registrada la información relativa a la vinculación de dispositivos.

Para determinar qué dispositivos se encuentran actualmente vinculados, es necesario consultar el valor **"mud.c"** en el campo **"ZNAMESPACE"**. Cuando un dispositivo se desvincula, este registro se elimina.

Una vez localizado este valor, en el campo **"ZKEY"** se almacena el identificador "jid" del dispositivo vinculado, junto con su número de vinculación y la fecha de vinculación en formato UTC Unix Epoch (segundos). Finalmente, en el campo **"ZVALUE"** se conserva, en formato protobuf, la información correspondiente al tipo de dispositivo vinculado.

Z_PK	Z_ENT	Z_OPT	ZSORT	ZVERSION	ZDATE	ZKEY	ZNAMESPACE	ZVALUE
1000	1	2	28	0	08/11/2025 21:03:45	346[REDACTED]@s.whatsapp.net-2-1762629364	mud.c	± 346423283646-346 iÄO, çÄp { kUW 8}Ee "Wz#8eq51s[" úÖp ß-346
1011	1	2	30	0	09/11/2025 09:19:50	346[REDACTED]@s.whatsapp.net-2-1762679986	mud.c	± 34642328364714E Ä 1sC<" çÖt Êñçèù Ê7B"8" úÖp 14E ("72)
1024	1	1	31	0	09/11/2025 14:21:50	346[REDACTED]@s.whatsapp.net-2-1762698106	mud.c	¼ 3464232836404EÄE é < Q6PA>n o 1s 1PEV 1s7" da " úÖp 04EÄE (

Tabla **ZWAKEYVALUEELEMENT** de la base de datos **LocalKeyValue.sqlite**

Ilustración 206. Selección de registros de vinculación de dispositivos ("ZNAMESPACE" =mud.c)

Una vez decodificado el campo “**ZVALUE**”, la información más relevante es la siguiente:

Campo	Campo	Descripción
1	1	Número de teléfono del usuario con prefijo internacional.
	2	Fecha de la vinculación en formato UTC Unix Epoch (segundos).
2	1 (sistema operativo del dispositivo vinculado)	iOS: iPhone. macOS: iPad. <i>Sistemas operativos macOS</i> (ordenadores y portátiles) se detecta por la presencia de un campo 2-1-13, con un valor numérico. <i>Android</i>, puede estar registrado el número de versión del S.O. (Ej: “15” o “8.1.0” para Android 15 o 8.1.0), por “Linux” o “Android” dependiendo del tipo de dispositivo. Windows: Windows. Linux: Linux. <i>VR Oculus</i>, número de versión de Android en la que se basa el S.O. (Ej: “14” para Android 14).
	3 (tipo plataforma de vinculación)	1: Navegador Chrome. 2: Navegador Firefox. 5: Navegador Safari. 6: Navegador Edge. 7: Aplicación de escritorio de macOS. 8: Aplicación para iPad. 9: Aplicación para tableta Android. 16: Aplicación para iPhone. 18: Aplicación para teléfono Android. 23: Aplicación de escritorio de Windows 24: Dispositivo de Realidad Virtual (Oculus).
	6	Ubicación (ciudad)
	7	Ubicación (provincia)

Ilustración 207. Archivo protobuf del campo “**ZVALUE**” de la tabla “**ZWAKEYVALUEELEMENT**”

Log

El registro de logs almacena la información relativa a la sincronización con dispositivos, por lo que, si han transcurrido solo unos pocos días, se puede obtener esa información a partir de alguno de los archivos ubicados en:

- /private/var/mobile/Containers/Shared/AppGroup/<GUID>/Logs/WhatsApp_2/

Por ejemplo, a partir del archivo de logs se puede obtener el identificador parcial “jid” y “lid” del nuevo dispositivo vinculado (*****5824:14@s.whatsapp.net y *****6203:14@lid, respectivamente) así como el tipo de dispositivo (Device 14; Android):

```
15:44:54.547 [ 31610] [main-thread ] [F] LLA pair-session//transition/2@dR6Y7wvRMTcQtbxdwrfOma-
5L0nCmAdqplRjUV9/sHTRGfG4s8wwlfoqe312nUAZmroCdiNsElbKbtsOw+TrDRkfkCt6UI8nPsi0=/s: 7 j:
<*****5824:14@s.whatsapp.net>
15:44:56.941 [ 31610] [main-thread ] [F] LLA device-storage-updater/devices/<*****8364@s.whatsapp.
net>/account-effect
LLA ->
LLA AccountEffect(l: DeviceListEffect.mutate(rawID: 465857144 ts: 1759848292 i:
[<*****5824:14@s.whatsapp.net>: 1] r: [] expectedTS: ETSEffect { .ignore } sync: false accType:
WAPBADVEncryptionType(rawValue: 0) accTypeUpdated: false) k: IdentityKeyEffect { primaryIdentity: Pri-
maryIdentityEffect.ignore, newKeys: [] })
15:44:56.957 [31610] [main-thread] [F] LLA pair-session//transition/2@dR6Y7wvRMTcQtbxdwrfOma-
5L0nCmAdqplRjUV9/sHTRGfG4s8wwlfoqe312nUAZmroCdiNsElbKbtsOw+TrDRkfkCt6UI8nPsi0=/s: 10 j:
<*****8364:14@s.whatsapp.net>
15:44:57.962 [ 80246] [NSManaged...0680] [F] LLA signal/manager/base//key-store/delegate/identi-
ty-created/<*****5824:14@s.whatsapp.net>
15:44:57.962 [80246] [NSManaged...0680] [F] LLA signal/manager/base//key-store/delegate/identity-crea-
ted/<*****6203:14@lid>
15:45:00.861 [79742] [NSManaged...e630] [F] LLA history-sync/data-fetcher/history-sync-data-fetcher/
messages fetched count=[2]
15:45:00.861 [79742] [NSManaged...e630] [F] LLA internal-participantJID/group-member-nil
15:45:01.013 [79998] [promises ] [F] LLA md/app-state/sync/Processing remote change set: Remote
change set: regular_low (v3)
LLA .mutations: ["72c9475f3a406191", "147a47f911157695", "d832cc9aa10f4d1e"]
LLA .encryptionKey: 000e0000f595
LLA .snapshotMAC: 34801959e4fcb2747805fdb88659405466e5fde0b1e2c9e3141c58f6c7c6d1a3
LLA .patchMAC: b16f3f99c5d4d0df5cf360c6b22c58ce93c4444a56f304c986c6969530b36da5
LLA .source: Device 14; Android
```

No menos importante puede ser determinar el dispositivo con el que se abrió por primera vez un mensaje.

En el campo "ZRECEIPTINFO" de la tabla "ZWMESSAGEINFO" se almacena información del dispositivo del usuario de esta cuenta con el que ha abierto por primera vez el mensaje. Esta información está en formato protobuf y debe decodificarse.

Diagram illustrating the relationship between database tables to identify the recipient device of a message.

Table ZWMESSAGE:

Z_PK	ZMEDIAITEM	ZMESSAGEINFO	ZMESSAGEDATE	ZSENTDATE	ZFROMJID	ZTEXT
771	634	653	08/12/2025 17:08:09	08/12/2025 17:11:35	148846453755945@lid	Mensaje abierto por un dispositivo vinculado

Table ZWMESSAGEINFO:

Z_PK	Z_ENT	Z_OPT	ZMESSAGE	ZRECEIPTINFO
653	11	1	771	Id#(60 (R \$ tUE)

Protobuf Decoder:

Tool to decode Protobuf without having the original .proto files. All decoding is done locally via JavaScript.

Input: 12 13 0a 07 81 34 64 23 28 36 4f 20 00 28 00 52 04 08 24 10 00 18 bf 8d dc c9 06 20 02

Result:

Byte Range	Field Number	Type	Content												
0-9	1	bytes	81 34												
9-11	4	varint	As uint: 0 As sint: 0												
11-13	5	varint	As uint: 0 As sint: 0												
13-19	10	protobuf	<table border="1"> <thead> <tr> <th>Byte Range</th> <th>Field Number</th> <th>Type</th> <th>Content</th> </tr> </thead> <tbody> <tr> <td>0-2</td> <td>1</td> <td>varint</td> <td>As uint: 36 As sint: 10</td> </tr> <tr> <td>2-4</td> <td>2</td> <td>varint</td> <td>As uint: 0 As sint: 0</td> </tr> </tbody> </table>	Byte Range	Field Number	Type	Content	0-2	1	varint	As uint: 36 As sint: 10	2-4	2	varint	As uint: 0 As sint: 0
Byte Range	Field Number	Type	Content												
0-2	1	varint	As uint: 36 As sint: 10												
2-4	2	varint	As uint: 0 As sint: 0												
21-27	3	varint	As uint: 1765213887 As sint: -882606944												
27-29	4	varint	As uint: 2 As sint: 1												

Decodificador online "Protobuf Decoder"

Table ZWAKEYVALUEELEMENT:

Z_PK	Z_ENT	Z_OPT	ZSORT	ZVERSION	ZDATE	ZKEY	ZNAMESPACE	ZVALUE
2247	1	2	49	0	786319092,058572	346	ps.whatsapp.net-2-1764626287	mud.c

Annotations:

- Yellow arrow: Points from ZMESSAGEINFO.ZRECEIPTINFO to the Protobuf Decoder input.
- Blue arrow: Points from the Protobuf Decoder result (Field 10) to the ZWAKEYVALUEELEMENT.ZKEY.
- Red arrow: Points from the ZWAKEYVALUEELEMENT.ZVALUE to the Protobuf Decoder result (Field 10).
- Green arrow: Points from the ZWAKEYVALUEELEMENT.ZKEY to the ZWMESSAGEINFO.ZRECEIPTINFO.

Ilustración 208. Relación entre tablas para identificar el dispositivo receptor del mensaje

De la misma forma, cuando el usuario envía un mensaje, también se registra la información en el archivo protobuf ubicado en el campo **"ZRECEIPTINFO"** de la tabla **"ZWMESSAGEINFO"** de los dispositivos del contacto que lo han recibido. En el siguiente ejemplo, el mensaje lo ha recibido el dispositivo principal del contacto (número "0") y su dispositivo vinculado número "35":

Protobuf Decoder

Tool to decode Protobuf without having the original .proto files. All decoding is done locally via JavaScript.

12 17 0a 07 81 34 67 25 72 38 71 20 00 52 04 08 00 10 00 52 04 08 23 10 00 18 9d ed 9a bb 06 20 02

Decode

Result

Número de teléfono del receptor del mensaje (el contacto)

Número de dispositivo que ha recibido el mensaje

Fecha de recepción del mensaje en formato UTC Unix Epoch (segundos)

Byte Range	Field Number	Type	Content																																												
0-25	2	protobuf	<table><thead><tr><th>Byte Range</th><th>Field Number</th><th>Type</th><th>Content</th></tr></thead><tbody><tr><td>0-9</td><td>1</td><td>bytes</td><td>81 34 67 25 72 38 71 20 00 52 04 08 00 10 00 18 9d ed 9a bb 06 20 02</td></tr><tr><td>9-11</td><td>4</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr><tr><td>11-17</td><td>10</td><td>protobuf</td><td><table><thead><tr><th>Byte Range</th><th>Field Number</th><th>Type</th><th>Content</th></tr></thead><tbody><tr><td>0-2</td><td>1</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr><tr><td>2-4</td><td>2</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr></tbody></table></td></tr><tr><td>17-23</td><td>10</td><td>protobuf</td><td><table><thead><tr><th>Byte Range</th><th>Field Number</th><th>Type</th><th>Content</th></tr></thead><tbody><tr><td>0-2</td><td>1</td><td>varint</td><td>As uint: 35 As sint: -18</td></tr><tr><td>2-4</td><td>2</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr></tbody></table></td></tr></tbody></table>	Byte Range	Field Number	Type	Content	0-9	1	bytes	81 34 67 25 72 38 71 20 00 52 04 08 00 10 00 18 9d ed 9a bb 06 20 02	9-11	4	varint	As uint: 0 As sint: 0	11-17	10	protobuf	<table><thead><tr><th>Byte Range</th><th>Field Number</th><th>Type</th><th>Content</th></tr></thead><tbody><tr><td>0-2</td><td>1</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr><tr><td>2-4</td><td>2</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr></tbody></table>	Byte Range	Field Number	Type	Content	0-2	1	varint	As uint: 0 As sint: 0	2-4	2	varint	As uint: 0 As sint: 0	17-23	10	protobuf	<table><thead><tr><th>Byte Range</th><th>Field Number</th><th>Type</th><th>Content</th></tr></thead><tbody><tr><td>0-2</td><td>1</td><td>varint</td><td>As uint: 35 As sint: -18</td></tr><tr><td>2-4</td><td>2</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr></tbody></table>	Byte Range	Field Number	Type	Content	0-2	1	varint	As uint: 35 As sint: -18	2-4	2	varint	As uint: 0 As sint: 0
Byte Range	Field Number	Type	Content																																												
0-9	1	bytes	81 34 67 25 72 38 71 20 00 52 04 08 00 10 00 18 9d ed 9a bb 06 20 02																																												
9-11	4	varint	As uint: 0 As sint: 0																																												
11-17	10	protobuf	<table><thead><tr><th>Byte Range</th><th>Field Number</th><th>Type</th><th>Content</th></tr></thead><tbody><tr><td>0-2</td><td>1</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr><tr><td>2-4</td><td>2</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr></tbody></table>	Byte Range	Field Number	Type	Content	0-2	1	varint	As uint: 0 As sint: 0	2-4	2	varint	As uint: 0 As sint: 0																																
Byte Range	Field Number	Type	Content																																												
0-2	1	varint	As uint: 0 As sint: 0																																												
2-4	2	varint	As uint: 0 As sint: 0																																												
17-23	10	protobuf	<table><thead><tr><th>Byte Range</th><th>Field Number</th><th>Type</th><th>Content</th></tr></thead><tbody><tr><td>0-2</td><td>1</td><td>varint</td><td>As uint: 35 As sint: -18</td></tr><tr><td>2-4</td><td>2</td><td>varint</td><td>As uint: 0 As sint: 0</td></tr></tbody></table>	Byte Range	Field Number	Type	Content	0-2	1	varint	As uint: 35 As sint: -18	2-4	2	varint	As uint: 0 As sint: 0																																
Byte Range	Field Number	Type	Content																																												
0-2	1	varint	As uint: 35 As sint: -18																																												
2-4	2	varint	As uint: 0 As sint: 0																																												
25-31	3	varint	As uint: 1734784669 As sint: -867392335																																												
31-33	4	varint	As uint: 2 As sint: 1																																												

Ilustración 209. Decodificación de archivo protobuf con el decodificador "Protobuf Decoder"

8.5. Restringir un chat

Se puede restringir un chat, de tal forma que no sea accesible en la aplicación salvo que se introduzca la autenticación del dispositivo (código de desbloqueo, huella dactilar o reconocimiento facial). En caso de que no esté establecido un método de autenticación, la aplicación obligará al usuario a establecer uno antes de permitir el bloqueo de un chat para que quede restringido su acceso.

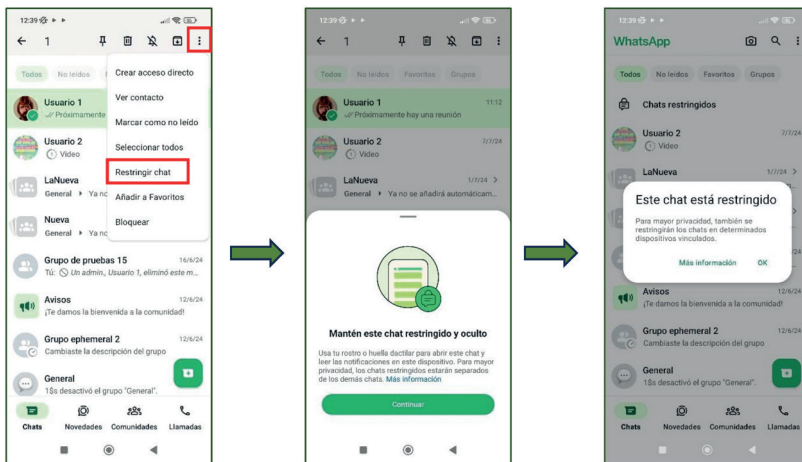


Ilustración 210. Proceso para restringir un chat en Android (similar en iOS)

En la pantalla principal de la aplicación, en la sección “Chats”, si se desliza la pantalla hacia abajo aparecerán los “Chats restringidos”. Cuando se seleccione, la aplicación solicita la autenticación y una vez desbloqueado, muestra todos los chats restringidos.

WhatsApp ha implementado la posibilidad de elevar la privacidad a los chats restringidos, permitiendo ocultarlos de la sección “Chats”. Esta opción se puede activar desde las opciones de “Chats restringidos”, exigiendo al usuario crear un código secreto para poder acceder a estos chats. El código puede ser alfanumérico o emojis y para abrir los chats restringidos debe introducirse en el buscador de la sección de “Chats” el código secreto y su apertura será automática. Si se establece un código secreto, el usuario podrá abrir sus chats restringidos en los dispositivos vinculados.

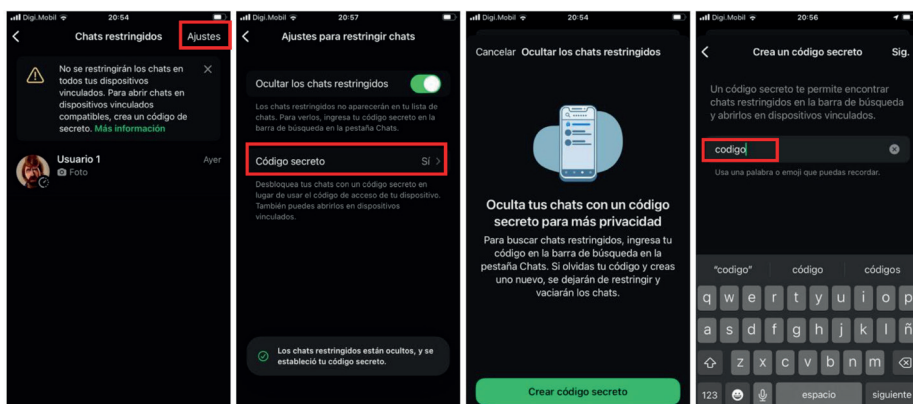


Ilustración 211. Proceso para aplicar un código secreto en los chats restringidos de iOS (similar en Android)

En las pruebas realizadas, el comportamiento del chat restringido es exactamente igual que el de un chat no restringido, excepto que hay que autenticarse para acceder al chat desde el dispositivo o introducir el código en el buscador de chats si está restringido y oculto. A nivel forense no supone ninguna diferencia en la forma de almacenar sus interacciones en las bases de datos o en las carpetas destinadas por la aplicación al almacenamiento de archivos multimedia.

No obstante, el principal motivo por el cual un usuario restringe un chat e incluso lo oculta con un código no es otro que la privacidad/seguridad de sus comunicaciones con otros contactos o grupos. Por ello, es necesario que el analista verifique la posible existencia de este tipo de chats.

Android

En Android, la información de los chats restringidos se localiza en el campo **"chat_lock"** de la tabla **"chat"** de la base de datos **"msgstore.db"**. En caso de que el chat esté restringido el valor del campo será **"1"**. Como se ha explicado previamente, vinculando los datos de la tabla **"chat"** con la tabla **"jid"** y la base de datos **"wa.db"**, se puede identificar plenamente el contacto con el que mantiene la conversación el usuario de esta cuenta.

Pero para poder comprobar si estos chats restringidos están también ocultos, hay que dirigirse al archivo de configuración com.whatsapp_preferences_light.xml, ubicado en la ruta /data/data/com.whatsapp/shared_prefs/:

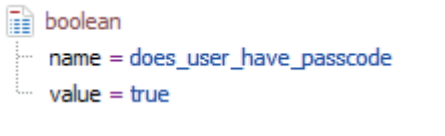
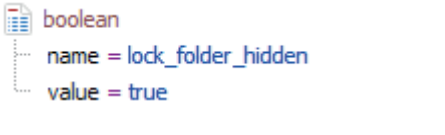
Nombre y valor del parámetro	Significado de los valores
	Los chats restringidos disponen de código secreto: true : cierto. false : falso.
	Los chats restringidos se encuentran ocultos: true : cierto. false : falso.

Ilustración 212. Opción activada de código secreto en el archivo com.whatsapp_preferences_light.xml

iOS

Para determinar qué chats se encuentran restringidos en la versión de iOS, se debe consultar la tabla “ZWCHATSESSION” de la base de datos “ChatStorage.sqlite”. Un chat se considera restringido cuando el campo “ZFLAGS” presenta alguno de los siguientes valores: “131344”, “655632”, “4849936”, “67240192”, “268566800” o “273285392”, con independencia de si el código secreto está activado o no.

En el hipotético caso de que se haya realizado una extracción FFS y se encuentre la base de datos “AppState.sqlite”, la tabla “ZAPPSTATE-CONFIRMEDMUTATIONENTITY” registrará los chats restringidos, los cuales presentarán el valor “lock” en el campo “ZACTIONNAME”, y el identificador “jid” del chat en el campo “ZTARGETID”.

Z_PK	Z_ENT	Z_OPT	ZCOLLECTIONID	ZSTATE	ZVERSION	ZACTIONNAME	ZTARGETID	ZENCRYPTIONKEYID	ZINDEX	ZVALUE
28	2	1	4	1	7	lock	120363320123164021@g.us		["lock","120363320123164021@g.us"]	ñâ Ñ 3
32	2	1	4	1	7	lock	120363328792612948@g.us		["lock","120363328792612948@g.us"]	ñâ Ñ 3
37	2	1	4	1	7	lock	34[redacted]@s.whatsapp.net		["lock","34646590111@s.whatsapp.net"]	ñâ Ñ 3
93	2	1	4	1	7	lock	34[redacted]@s.whatsapp.net		["lock","34610932592@s.whatsapp.net"]	Öpal 3

Ilustración 213. Tabla ZAPPSTATECONFIRMEDMUTATIONENTITY de la base de datos AppState.sqlite

8.6. Descarga de archivos recibidos

La aplicación permite elegir los tipos de archivos (imágenes, audio, vídeos y documentos) que se descargarán automáticamente y el tipo de conexión utilizada. En el caso de que no se descarguen automáticamente, el usuario podrá realizarlo manualmente. Es importante corroborar que el archivo ha sido descargado en el dispositivo analizado, para evitar errores en el análisis forense y no concluir que fue eliminado por el usuario.

La forma de elegir las opciones de descarga difiere en el criterio de la selección entre la versión de la aplicación en Android y en iOS, aun teniendo el mismo resultado.

Android

En este sistema operativo, se debe asignar el tipo de archivo (fotos, audio, vídeos y documentos) que se descargará automáticamente con cada tipo de conexión (datos móviles, Wi-Fi e itinerancia de datos):

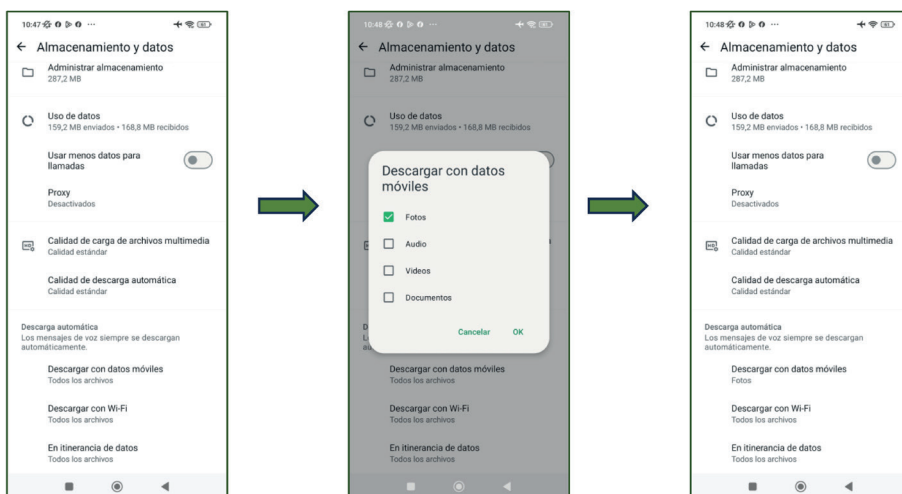


Ilustración 214. Opciones de descarga de archivos

La configuración establecida por el usuario se encuentra en el archivo **com.whatsapp_preferences_light.xml**, ubicado en la ruta /data/data/com.whatsapp/shared_prefs/.

Nombre y valor del parámetro	Significado de los valores
 <pre>int name = autodownload_roaming_mask value = 0</pre>	Existe un parámetro para cada tipo de conexión que permite la autodescarga: itinerancia de datos (roaming), datos móviles (celular) y Wi-Fi. Los valores que pueden adoptar dependen del tipo de archivo a descargar, y son los siguientes:
 <pre>int name = autodownload_cellular_mask value = 15</pre>	0: nada 1: fotos. 2: audio. 4: vídeos. 8: documentos.
 <pre>int name = autodownload_wifi_mask value = 0</pre>	Si la opción de descarga automática incluye más de un tipo de archivo, el valor se genera sumando los valores de todos los tipos de archivos que se pueden descargar: 3: fotos y audio. 5: fotos y vídeos. 7: fotos, audio y vídeos. 9: fotos y documentos. 10: audio y documentos. 11: fotos, audio y documentos. 12: vídeos y documentos. 13: fotos, vídeos y documentos. 14: audio, vídeos y documentos. 15: fotos, audio, vídeos y documentos.

*Ilustración 215. Opciones de descarga de archivos en Android (archivo **com.whatsapp_preferences_light.xml**)*

iOS

En el sistema operativo iOS la elección es a partir de cada tipo de archivo (fotos, audio, vídeo y documentos) y se selecciona el tipo de conexión a través de la que se realizará la descarga automática (Wi-Fi y datos móviles, Wi-Fi o nunca).

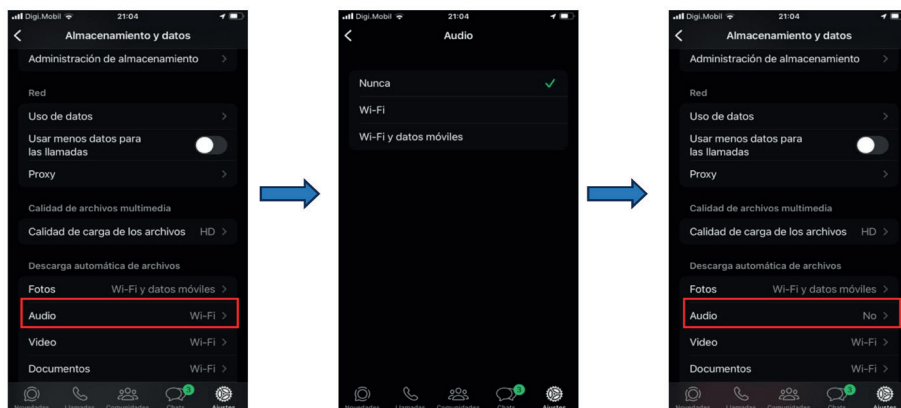


Ilustración 216. Opciones de descarga de archivos

La configuración establecida por el usuario se encuentra en el archivo **group.net.whatsapp.WhatsApp.shared.plist**. Entre la información recogida en este archivo "plist" de configuración está la sección de las políticas de descarga "**DownloadPolicy**", que incluye a su vez un archivo "bplist00" con las opciones de descarga elegidas por el usuario.

Nombre y valor del parámetro	Significado de los valores
DownloadPolicy = bplist00..... <Dictionary> - Classname = "WAMMS.MediaDownloadPolicySettings" - document = 0 - audio:time = 744151788,066952 - video:time = 746660928,161252 - image = 1 - video = 1 - image:time = 746660818,90448 - audio = 3	Opciones de descarga automática de archivos: 0: nunca. 1: Wi-Fi. 3: Wi-Fi y datos móviles. xxxx:time*: fecha en la que se asignó la opción en OS X Epoch Time. *xxxx= audio, video, image o document

Ilustración 217. Opciones de descarga de archivos en iOS (archivo **group.net.whatsapp.WhatsApp.shared.plist**)

8.7. Copias de seguridad / backups

Ambas plataformas, Android e iOS, permiten almacenar una copia de seguridad en la nube de los mensajes y archivos transmitidos a través de la aplicación. Esta copia puede ser iniciada manual o automáticamente con una frecuencia diaria, semanal o mensual. Además, las versiones para los dos sistemas operativos generan copias de seguridad en los propios dispositivos (local).

La recuperación, localización y descifrado de las copias de seguridad puede ser fundamental en investigaciones en la que se hayan eliminado mensajes posteriormente a su generación, permitiendo recuperar información e incluso en algunos casos archivos transmitidos.

Para recuperar las copias de seguridad almacenadas en la nube (**Google Drive** e **iCloud**), es necesario contar con algún método de autenticación válido del usuario (claves, tokens, etc.) y utilizar software especializado.

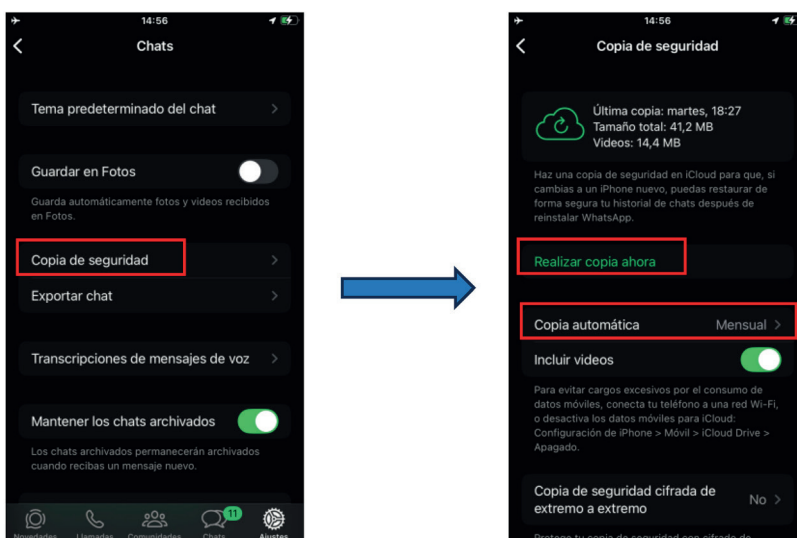


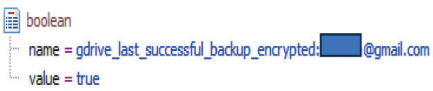
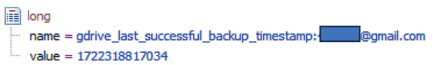
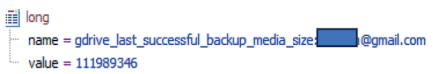
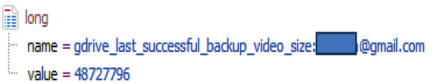
Ilustración 218. Activación de la copia de seguridad en iOS (similar en Android)

8.7.1. Copia de seguridad en Google Drive (Android)

La aplicación permite la creación de una copia de seguridad que se guardará en el servicio de almacenamiento en la nube Google Drive, vinculado a la cuenta de Google del usuario del dispositivo (por defecto) u otra cuenta proporcionada. El servicio se puede activar manualmente o programarse para que genere la copia diaria, semanal o mensualmente.

Entre las opciones de la copia de seguridad se encuentra la posibilidad de incluir o excluir los vídeos, debido a que son los archivos más pesados y su transferencia genera un mayor consumo de datos, así como la opción de cifrar la copia con una clave seleccionada por el usuario.

Cuando se realiza el análisis de la aplicación, los principales valores relacionados con las copias de seguridad se pueden consultar en los archivos de preferencias denominados **backup_prefs.xml** que se encuentran en la ruta `/data/data/com.whatsapp/shared_prefs/`. Algunos de estos parámetros se almacenaban anteriormente (primer trimestre de 2025) en el archivo **com.whatsapp_preferences_light.xml**.

Nombre y valor del parámetro	Significado de los valores
	Opción activada del cifrado en la última copia de seguridad almacenada en la cuenta indicada de Google Drive: true : cierto. false : falso.
	La fecha en formato UTC Unix Epoch (milisegundos) de la última copia de seguridad almacenada en la cuenta indicada de Google Drive.
	Tamaño en bytes de los archivos multimedia de la última copia de seguridad almacenada en la cuenta indicada de Google Drive.
	Tamaño en bytes de los vídeos de la última copia de seguridad almacenada en la cuenta indicada de Google Drive.

Nombre y valor del parámetro	Significado de los valores
 <pre> long name = msg_restore_timestamp value = 1735236668820 </pre>	Fecha en formato UTC Unix Epoch (milisegundos) en la que se restauraron los mensajes en la cuenta a partir de la copia de seguridad.
 <pre> long name = gdrive_last_successful_backup_total_size: [redacted]@gmail.com value = 115088523 </pre>	Tamaño en bytes de la última copia de seguridad completa almacenada en la cuenta indicada de Google Drive.
 <pre> string = 0 name = interface_gdrive_backup_network_setting </pre>	Guardar (copia de seguridad) usando datos móviles: 0: no. 1: sí.
 <pre> long name = msg_backup_timestamp value = 1736803705105 </pre>	Fecha en formato UTC Unix Epoch (milisegundos) en la se ha generado la copia de seguridad en el dispositivo (local).
 <pre> boolean name = gdrive_include_videos_in_backup value = true </pre>	Opción activada para incluir los vídeos en la copia de seguridad que se almacenará en Google Drive: true: se incluyen los vídeos. false: no se incluyen los vídeos.
 <pre> string = [redacted]@gmail.com name = gdrive_account_name </pre>	Cuenta de correo electrónico con la que está asociada Google Drive.
 <pre> string = password_encrypted name = backup_encryption_method </pre>	Cifrado de la copia de seguridad de extremo a extremo: password_encrypted: cifrado con una contraseña. unencrypted: sin cifrar.
 <pre> string = 3 name = interface_gdrive_backup_frequency </pre>	Frecuencia con el que se genera la copia de seguridad almacenada en la cuenta indicada de Google Drive. 0: Desactivado. 1: Diariamente. 2: Semanalmente. 3: Mensualmente. 4: Solo cuando toco "guardar".

*Ilustración 219. Opciones de la copia de seguridad en Android (archivo **backup_prefs.xml**)*

8.7.2. Copia de seguridad local (Android)

Las otras copias de respaldo que genera la aplicación de forma automática de la base de datos "**msgstore.db**" son los backups locales almacenados en el propio dispositivo, en la ruta /data/media/0/Android/media/com.whatsapp/WhatsApp/Databases/. El sistema puede llegar a generar varias copias de seguridad cifradas de diferentes días.

A la vez que se realizan estas copias de seguridad en local de la base de datos "**msgstore.db**", también se realiza de "**wa.db**" así como otras bases de datos de menor interés. La principal diferencia de estas copias de seguridad es que únicamente se almacena una copia de cada una y que se encuentran ubicadas en el subdirectorio /data/media/0/Android/media/com.whatsapp/WhatsApp/Backups/.

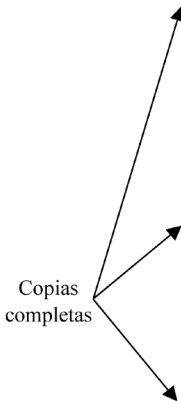
Hasta principios de 2024, los teléfonos podían contener hasta nueve (9) copias de seguridad cifradas de la base de datos "**msgstore.db**", que la aplicación estaba programada para grabar automáticamente a las 02:00 horas de los últimos nueve días que el dispositivo hubiese estado encendido.

Name	Modified (Canary)
 msgstore.db.crypt15	08/06/2023 02:01:01
 msgstore-2023-06-08.1.db.crypt15	07/06/2023 02:01:02
 msgstore-2023-06-07.1.db.crypt15	06/06/2023 02:06:02
 msgstore-2023-06-06.1.db.crypt15	05/06/2023 02:00:58
 msgstore-2023-06-05.1.db.crypt15	04/06/2023 02:01:07
 msgstore-2023-06-04.1.db.crypt15	03/06/2023 02:06:02
 msgstore-2023-06-03.1.db.crypt15	02/06/2023 02:06:00
 msgstore-2023-06-02.1.db.crypt15	01/06/2023 02:05:57
 msgstore-2023-06-01.1.db.crypt15	31/05/2023 02:01:00

*Ilustración 220. Nueve copias de seguridad de la base de datos **msgstore.db** (sistema antiguo)*

Desde mediados de 2024, la aplicación mantiene 3 copias de seguridad incrementales. Esto significa que hay tres copias completas con

una diferencia habitualmente de una semana entre ellas. Diariamente se generan copias incrementales en las que almacenan los cambios producidos en la base de datos "**msgstore.db**" durante un día.



Name	Modified (Canary)
msgstore-2025-08-30.1.db.crypt14	24/08/2025 03:01:49
msgstore-increment-1-2025-08-30.1.db.crypt14	25/08/2025 03:00:29
msgstore-increment-2-2025-08-30.1.db.crypt14	26/08/2025 03:04:09
msgstore-increment-3-2025-08-30.1.db.crypt14	27/08/2025 03:00:46
msgstore-increment-4-2025-08-30.1.db.crypt14	28/08/2025 03:00:42
msgstore-increment-5-2025-08-30.1.db.crypt14	29/08/2025 03:00:03
msgstore-2025-09-05.1.db.crypt14	30/08/2025 03:04:27
msgstore-increment-1-2025-09-05.1.db.crypt14	31/08/2025 03:04:27
msgstore-increment-2-2025-09-05.1.db.crypt14	01/09/2025 03:04:27
msgstore-increment-3-2025-09-05.1.db.crypt14	02/09/2025 03:04:25
msgstore-increment-4-2025-09-05.1.db.crypt14	03/09/2025 03:01:10
msgstore.db.crypt14	05/09/2025 03:00:45
msgstore-increment-1.db.crypt14	06/09/2025 03:00:46
msgstore-increment-2.db.crypt14	07/09/2025 03:00:09
msgstore-increment-3.db.crypt14	08/09/2025 03:04:46

*Ilustración 221. Copias de seguridad incrementales completas y diarias de la base de datos **msgstore.db** (sistema actual)*

A fecha del estudio, por defecto las copias de seguridad se cifran con "crypt14" a partir de la clave criptográfica "**key**". Si el usuario selecciona la copia de seguridad con el cifrado "de extremo a extremo", se cifrará con "crypt15" a partir de la clave criptográfica "**encrypted_backup.key**". En ambos casos la clave criptográfica se encontrará almacenada en la ruta **/data/data/com.whatsapp/files/**.

Existen herramientas de software libre, como **wa-crypt-tools** que es capaz de realizar el descifrado de "crypt14" o "crypt15", tanto de las actuales copias de seguridad incrementales completas (semanales) como la versión anterior (hasta mediados de 2024).

Las copias de seguridad *incrementales diarias* realmente no son la base de datos "**msgstore.db**" cifrada, sino un contenedor ZIP cifrado.

Cuando están cifradas con "crypt14" es posible descifrarlas con el archivo **key** tanto con herramientas comerciales como no comerciales como **wa-crypt-tools**, obteniendo el contenedor ZIP. Hasta la fecha, no se ha localizado una aplicación que sea capaz de descifrar las copias de seguridad incrementales diarias cuando están cifradas con "crypt15".

Dicho contenedor cifrado contiene un archivo binario (**messages.bin**) y varios archivos de tipo JSON. En el archivo binario se registran las modificaciones que se producirán en la copia de seguridad (semanal), con información tan importante como la eliminación de mensajes. Sin embargo, surge una limitación considerable: se ha comprobado que la herramienta Oxygen Detective es capaz de interpretar estos archivos "message.bin", pero no se ha hallado ninguna herramienta no comercial que pueda realizar esta función.

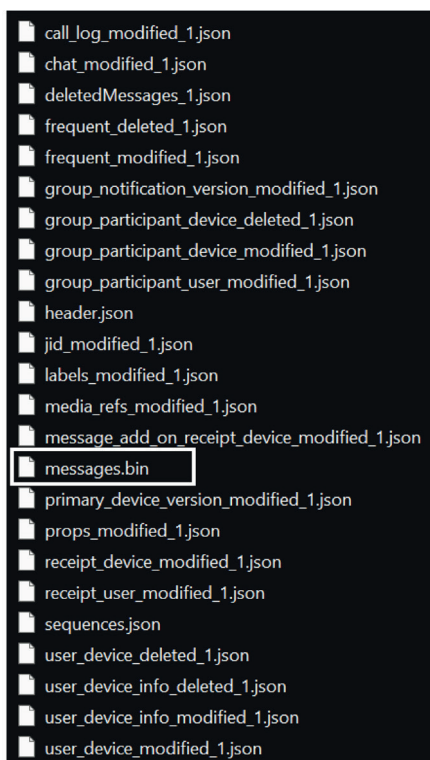


Ilustración 222. Contenido del contenedor .zip de una copia incremental diaria (message.bin y archivos json)

8.7.3. Copia de seguridad en iCloud (iOS)

Es posible realizar copias de seguridad de la aplicación en la cuenta de iCloud asociada al usuario de WhatsApp. Las opciones son similares a las de la versión de Android, permitiendo realizar la copia de forma automática en un intervalo de tiempo establecido (diaria, semanal o mensual) o manualmente cuando el usuario lo decida.

Se puede elegir que la copia incluya o no los vídeos, ya que estos archivos suelen ser los de mayor tamaño, implicando un mayor consumo de datos y almacenamiento. Además, se puede optar por cifrar la copia de seguridad de extremo a extremo.

La información sobre la configuración de la copia de seguridad se obtiene del archivo `group.net.whatsapp.WhatsApp.shared.plist`.

Nombre y valor del parámetro	Significado de los valores
 <code>AutoBackupCustom = 01/12/2025 14:52:43</code>	Fecha de la generación de la última copia de seguridad.
 <code>AutoBackupInterval = 720</code>	Horas programadas entre copias de seguridad: 720 (30 días). 168 (7 días). 24 (1 día). -1 (no se realiza).
 <code>RestoreBackupFinalChanges = True</code>	Restauración de copia de seguridad: True : cierto.
 <code>50 = 26/12/2024 18:05:00</code>	Fecha de activación de la cuenta en el dispositivo o fecha de restauración de la copia de seguridad de iCloud.

Ilustración 223. Opciones de la copia de seguridad en iOS (archivo `group.net.whatsapp.WhatsApp.shared.plist`)

8.7.4. Copia de seguridad local (iOS)

Cuando se genera una copia de seguridad para que se almacene en iCloud también se guarda una copia de seguridad en el propio terminal.

Esta copia local está formada por contenedores para cada tipo de archivo (vídeo, thumbnail, GIF, documento y media) así como las bases de datos más importantes de la aplicación cifradas (CallHistory.sqlite.enc, ChatStorage.sqlite.enc, ExtChatDatabase.sqlite.enc, Labels.sqlite.enc, LID.sqlite.ecn, Sticker.sqlite.enc).

Estos archivos se encuentran en la ruta (iTunes Backup y FFS):

- /private/var/mobile/Library/Mobile Documents/57T9237FN3~net~whatsapp~WhatsApp/Accounts/34xxxxxxxxx⁷/backup/

Name	Created (Canary)
Document.tar	26/12/2024 18:45:54
GIFs.tar	26/12/2024 18:45:55
Media.tar	26/12/2024 18:45:54
Stickers.tar	26/12/2024 18:45:55
Thumbnail.tar	26/12/2024 18:45:55
Video.tar	26/12/2024 18:45:54
AvatarCredentials.enc	26/12/2024 18:45:54
BackedUpKeyValue.sqlite.enc	26/12/2024 18:45:54
CallHistory.sqlite.enc	26/12/2024 18:45:54
ChatStorage.sqlite.enc	26/12/2024 18:45:54
ExtChatDatabase.sqlite.enc	26/12/2024 18:45:54
Labels.sqlite.enc	26/12/2024 18:45:54
LID.sqlite.enc	26/12/2024 18:45:54
Sticker.sqlite.enc	26/12/2024 18:45:54
UserDefaults.plist.enc	26/12/2024 18:45:54
Backup.plist	26/12/2024 18:45:55

Ilustración 224. Contenido de la copia de seguridad local

Por defecto la copia de seguridad no está cifrada “de extremo a extremo”. De este modo, los archivos que se encuentran en los contenedores “.tar⁸” (notas de vídeo, imágenes, notas de voz, etc) son visibles

7. Número de teléfono del usuario de esta cuenta.

8. Tape **AR**chiver (archivador en cinta) es un archivo o contenedor en que se pueden almacenar diferentes directorios y archivos.

y analizables, lo cual puede resultar de gran valor si, posteriormente a la creación de la copia de seguridad, el usuario elimina algún archivo transmitido.

Por el contrario, si el usuario activa la opción "Copia de seguridad cifrada de extremo a extremo", todos los archivos grabados en la copia de seguridad local se encontrarán cifrados, y hasta la fecha no se ha encontrado documentación de un método para su descifrado, lo que imposibilita su examen.

8.8. Inteligencia artificial

En un contexto en el que la inteligencia artificial está presente en todos los ámbitos, la aplicación de mensajería por excelencia no podía dejar pasar la oportunidad de integrar la solución desarrollada por Meta, denominada **"Meta AI"**.

En las versiones analizadas, Meta AI es capaz de responder preguntas, pero aún no genera imágenes, vídeos, audios, ni ofrece otras funciones avanzadas, como resumir chats o responder mensajes de forma autónoma. No obstante, WhatsApp tiene previsto ampliar sus funcionalidades en un futuro próximo; prueba de ello son las carpetas localizadas en la sección de medios de la aplicación, que previsiblemente estarán destinadas a almacenar archivos multimedia generados por inteligencia artificial, y que alguna base de datos tiene actualmente tablas que hacen referencia a la AI, aunque aún no contengan registros.

Con el objetivo de dar visibilidad a esta nueva herramienta y facilitar su uso, los desarrolladores han habilitado distintas vías de acceso. Por un lado, Meta AI cuenta con un icono propio en la aplicación que abre directamente un chat con la inteligencia artificial. Por otro, el usuario puede escribir su consulta en el buscador de chats, desde donde Meta AI responderá en su propio chat, y lógicamente también se puede preguntar en su propio chat.

Hay una cuarta opción, que es mencionar al bot de Meta AI en un chat privado o grupal con el texto "@Meta AI" seguido de la pregunta.

Ante la preocupación que causa entre los usuarios de que la inteligencia artificial adquiera información personal de los mensajes transmitidos en sus chats, los desarrolladores de WhatsApp han implementado una opción de "Privacidad avanzada del chat" que, entre otras, no permite usar las funciones de inteligencia artificial de Meta AI. Todas las implicaciones que presenta esta opción se desarrollan en el siguiente apartado.



Ilustración 225. Activación del asistente Meta AI en Android (similar en iOS)

El asistente creado por Meta presenta identificador "jid": **13135550002@s.whatsapp.net** y cuando es invocado en un chat cualquiera con el texto "@Meta AI", se identificará con su dominio de bot: **867051314767696@bot**. Ese identificador "bot" es el que se registra en el campo "ZTEXT" de la tabla "ZWAMESSAGE" en iOS y en el campo "text_data" de la tabla "message" cuando se solicita su asistencia en un chat.

Mención especial tiene el asistente **Chat GPT**, siendo posible interactuar con la inteligencia artificial de OpenAI en un chat. Es necesario añadir como contacto el número de teléfono 18002428478 e iniciar la conversación. El identificador "jid" de Chat GPT es **18002428478@s.whatsapp.net** y el identificador "lid" es **30722505109681@lid**.

Además de asistir y responder a preguntas, en el momento de este estudio, Chat GPT es capaz de generar imágenes.



Ilustración 226. Chat con el asistente de Chat GPT en iOS (similar en Android)

Android

El asistente Meta AI es un bot creado por Meta y por ello se encuentra registrado en la tabla "**wa_bot_profiles**" de la base de datos "**wa.db**". Como la cuenta de Meta AI es de tipo WhatsApp Business, también se encuentra registrado su identificador "jid" en la tabla "**wa_biz_profiles**" de la misma base de datos.

En la tabla "**bot_message_info**" de la base de datos "**msgstore.db**", se registran los mensajes emitidos por "Meta AI". Es bien conocido que la tabla "**message**", de la misma base de datos, contiene datos de todos

los mensajes transmitidos. Pero el campo **"invoker_jid_row_id"** de esta tabla complementa dicha información, indicando el participante que ha invocado a la inteligencia artificial en el chat.

El asistente "Meta AI" puede ser invocado por el propio usuario de la cuenta, desde el chat de "Meta AI" o desde la barra de búsqueda de chats. En ese caso el campo **"invoker_jid_row_id"** se encontrará vacío. Pero también puede solicitar su asistencia cualquier participante (incluido el usuario) en chats individuales con otros contactos y en chats grupales mencionándolo como "@Meta AI", previo a la pregunta. A partir del valor del campo **"invoker_jid_row_id"** se puede identificar del usuario o contacto que ha invocado al bot. El valor se corresponde con el campo **"_id"** de la tabla **"jid"**.

message_row_id	target_id	message_state	invoker_jid_row_id	model_type
3900	3379EAB82BF66AF71F5200A240963FCB	3	3	1
3926	F703F98E6D910C9BA0CECD90F02C0968	3	9	1
3930	05D7DA9339FF3109CBC03D32D8DD140D	3		1
4154	3975A0077A65501AA4269614A7E68CFF	3	3	1
4173	F090192399EB27BB1B892F2065C474C3	3	8	1

Ilustración 227. Tabla **"bot_message_info"**

El asistente de ChatGPT es registrado como una cuenta de WhatsApp Business corriente (constará en la tabla **"wa_biz_profiles"** de la base de datos **"wa.db"**), y por ello la aplicación no registra de ninguna manera especial la interacción con esta inteligencia artificial.

iOS

En las pruebas practicadas sobre la versión para iOS no se ha observado ninguna diferencia respecto a cualquier otro chat en el que participa el usuario de la cuenta analizada.

8.9. Privacidad avanzada del chat

Esta funcionalidad añade una capa adicional de seguridad para proteger el contenido compartido en chats individuales y grupales. Su

finalidad es impedir que los mensajes y archivos transmitidos puedan exportarse fuera de WhatsApp (exportar chat) o utilizarse en procesos de inteligencia artificial. De este modo no es posible invocar a Meta AI iniciando el mensaje con el texto "@Meta AI" en los chats.

Los archivos multimedia recibidos no se muestran en la galería de los dispositivos de los participantes en el chat, presumiblemente para dificultar el acceso a ellos.

Además, los mensajes transmitidos no pueden ser usados para funciones de inteligencia artificial, impidiendo que se compartan con Meta AI.

Android

Para verificar del estado de activación de la funcionalidad denominada "Privacidad avanzada del chat", se debe comprobar que el campo **"message_type"** de la tabla **"message"** presenta el valor **"112"**. Esta información se complementa con el análisis del campo **"enabled"** de la tabla **"message_limit_sharing_setting"**, el cual puede adoptar dos valores: **"0"**, correspondiente a la opción *desactivado*, o **"1"**, correspondiente a la opción *activado*.

La activación de la "Privacidad avanzada del chat" determina que los archivos recibidos se almacenen en el subdirectorio **/Private/** de cada tipo de archivo. Los archivos que se encuentran en estos subdirectorios no se muestran en la galería del teléfono y por tanto añade un grado de privacidad adicional. Pero esta restricción es limitada, ya que, conociendo la ruta, cualquier usuario con conocimientos básicos puede acceder a través de un explorador de archivos para compartirlos o copiarlos.

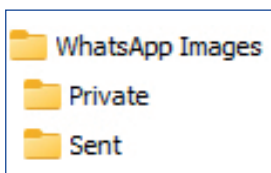


Ilustración 228. Carpeta en ruta "/data/media/0/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Images"

iOS

En la versión de iOS es posible determinar si “Privacidad avanzada del chat” está activada o desactivada, y la fecha en la que se seleccionó la opción, en el archivo protobuf almacenado en el campo **“ZLASTMESSAGETEXT”** de la tabla **“ZWACHATSESSION”**:

Campo	Descripción
74	Privacidad avanzada del chat: 0 : desactivada 1 : activada
76	Fecha en la que se activó o desactivó la “Privacidad avanzada del chat” en formato UTC Unix Epoch (milisegundos).

*Ilustración 229. Archivo protobuf del campo **“ZLASTMESSAGETEXT”** de la tabla **“ZWACHATSESSION”***

Cuando se activa o desactiva esta opción en un chat individual, se genera un mensaje del sistema específico que se corresponde con el valor **“73”** en el campo **“ZMESSAGETYPE”** de la tabla **“ZWAMESSAGE”** y un mensaje del sistema genérico con valor **“10”**. En los chats grupales, solo se genera el mensaje genérico con valor **“10”**, aunque es posible determinar su origen mediante la vinculación entre tablas.

Vinculando estos mensajes de la tabla **“ZWAMESSAGE”** con la tabla **“ZWAMEDIAITEM”** a través del campo **“Z_PK”** de la primera tabla que se corresponde con el campo **“ZMESSAGE”** de la segunda se obtiene los datos de la activación o desactivación de la opción de privacidad. En el registro correspondiente de la tabla **“ZWAMEDIAITEM”**, el campo **“ZMETADATA”** contiene un archivo protobuf con la información de privacidad:

Z_PK	ZISFROMME	ZMESSAGESTATUS	ZMESSAGE	ZCHATSESSION	ZMEDIAITEM	ZSORT	ZMESSAGE	ZMESSAGE
2181	0	6	73	113	1723	177	29/09/2025 16:28:52	
2182	0	0	10	113	1724	178	29/09/2025 16:28:52	

Tabla **ZWMESSAGE**

Z_PK	Z_ENT	Z_OPT	ZFILESIZE	ZMEDIAORIGIN	ZMOVEDURATION	ZMESSAGE	ZMETADATA
1723	8	1	0	0	0	2181	¢ NK»\0)u rExNOhçO× É¼) æ @g pú ,i,²3
1724	8	1	0	0	0	2182	ú ,i,²3

Tabla **ZWAMEDIAITEM**

Ilustración 230. Relación entre tablas en la activación o desactivación de la "Privacidad avanzada del chat"

Campo	Campo	Descripción
159 (opción "Privacidad avanzada del chat")	1	Privacidad avanzada del chat: 0 : desactivada 1 : activada
	3	Fecha en la que se seleccionó la opción en formato UTC Unix Epoch (milisegundos).

Ilustración 231. Campos del archivo protobuf del campo "ZMETADATA" de la tabla "ZWAMEDIAITEM"

Al activarse la "Privacidad avanzada del chat", se anula en dicho chat la opción "Guardar en Fotos" (si está activa en el dispositivo), por lo que no se almacenará copia alguna de las fotos y vídeos recibidos en "Fotos".

9. Análisis de mensajes (Android – iOS)

9.1. Mensajes de texto

Son los mensajes originarios de la aplicación y los más habituales. Los mensajes que únicamente son de texto (con o sin emojis) se graban como un tipo concreto de mensaje, **"message_type" = "0"** en Android (tabla **"message"**) y **"ZMESSAGE" = "0"** en iOS (tabla **"ZWAME-SAGE"**). También se puede añadir texto a los mensajes con archivos adjuntos de vídeo, imagen, documentos, GIFs o ubicaciones en tiempo real, pero en estos casos, el tipo de mensaje se identificará por el archivo adjunto que se ha transmitido, tenga o no texto añadido.

9.1.1. Mensajes editados

La aplicación permite la edición por parte del emisor del mensaje, del texto que contiene un mensaje hasta 15 minutos después de haberlo enviado. Durante ese periodo de tiempo, el emisor puede editar el texto tantas veces como considere oportunas. Se puede editar el mensaje de texto, así como el comentario añadido por el usuario a los mensajes con imágenes, vídeos, GIFs y documentos.

El mensaje editado mantiene la fecha y posición en el chat del mensaje inicial, añadiendo el texto "editado" debajo del mensaje, en el mismo bocadillo junto a la hora.

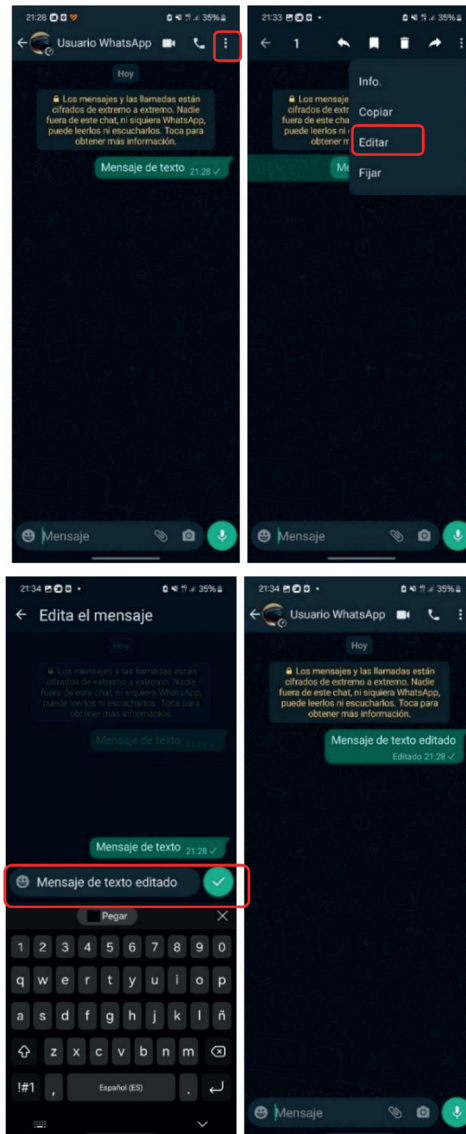


Ilustración 232. Secuencia de la edición de un mensaje de texto en Android (similar en iOS)

Android

El texto de los mensajes se encuentra en la tabla **"message"** de la base de datos **"msgstore.db"**. Cuando un mensaje se edita, el propio registro del mensaje se actualiza, sin que quede rastro en dicha tabla de que fue editado el mensaje ni cuál era su contenido original. Actualmente la mayoría de los programas de análisis no ofrecen resultados de la edición de mensajes, aunque se puede indagar en las diferentes tablas de la aplicación para determinar una línea temporal que explique las modificaciones que haya realizado su emisor.

En las bases de datos se registra la información de los mensajes editados, tanto los enviados por el usuario de la cuenta analizada como los editados por los contactos (recibidos).

La tabla **"message_edit_info"** registra todos los mensajes que han sido editados, tanto los enviados como los recibidos. El vínculo que existe entre las diferentes tablas para conectarlas por un mismo valor es el del campo de identificación de la fila ("**_id**") de la tabla **"message"**, que será el mismo valor que el del campo **"message_row_id"** de la tabla **"message_edit_info"** y del campo **"docid"** de la tabla **"message_ftv2_content"**.

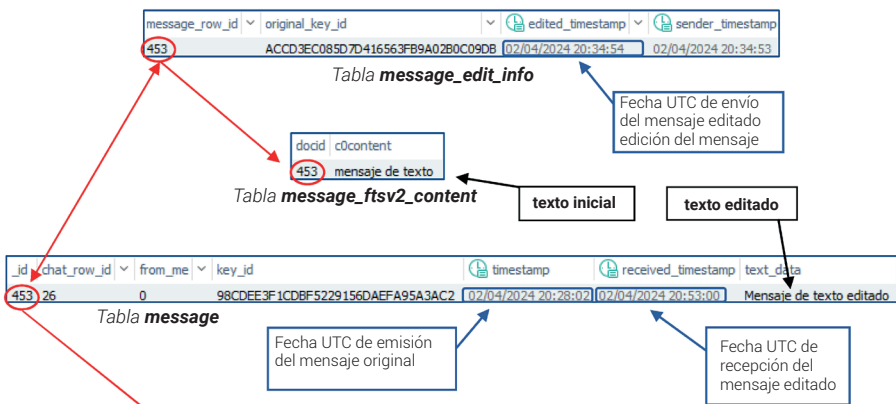
El texto del mensaje original (previo a la edición) es el que se muestra en el campo **"c0content"** de la tabla **"message_ftv2_content"**, en este ejemplo: *"mensaje de texto"*.

El texto final editado, que es el que se ve en el chat, se muestra en el campo **"text_data"** de la tabla **"message"**, en este ejemplo: *"Mensaje de texto se ha editado"*. Si el mensaje inicial se edita en varias ocasiones, no se podrá conocer ni la cantidad de veces que ha sido editado ni su contenido, excepto el mensaje inicial y el final editado que es el que mostrará en el chat.

Se puede determinar a qué hora fue enviado el mensaje original, cuándo fue editado y cuándo fue entregado. Para ello hay que trasladarse al campo **"timestamp"** de la tabla **"message"**, donde se muestra la fecha de envío del mensaje original desde el teléfono analizado y el campo **"received_timestamp"** es la fecha de la entrega del mensaje editado

en el receptor. La fecha de edición del texto se localiza en el campo **"edited_timestamp"** de la tabla **"message_edit_info"**.

Ejemplo de un mensaje recibido por el usuario de la cuenta analizada y editado por el emisor:



Adicionalmente se puede verificar esta información con la tabla **"message_add_on"**, la cual también registra los mensajes editados, en el campo **"message_add_on_type"** con el valor **"74"**:

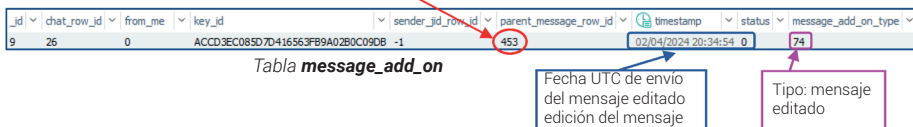


Ilustración 233. Relación entre tablas de un mensaje editado

Hay que aclarar que los valores del identificador de mensaje ("`key_id`" u "`original_key_id`") del mensaje editado coinciden en las tablas **"message_edit_info"** y **"message_add_on"**, y se corresponden con la "`key_id`" que se asignó al mensaje originalmente. Ese valor difiere del registrado en la tabla **"message"**, que es el nuevo valor asignado tras la edición del mensaje.

iOS

Los mensajes de texto quedan registrados en la tabla **"ZWMESSAGE"**, concretamente en el campo **"ZTEXT"** se graba el texto. Cuando el texto es editado, queda constancia de la modificación en el campo **"ZPUSHNAME"** de la misma tabla, donde se almacena un archivo protobuf codificado en Base64. Los datos en Base64 se deben decodificar a hexadecimal para posteriormente decodificarlos como datos protobuf.

Al editar un mensaje, el identificador del nuevo mensaje se actualiza y sobrescribe al anterior, registrándose en el campo **"ZSTANZAID"** de la tabla **"ZWMESSAGE"**. El identificador del mensaje original se conserva en el archivo protobuf, dentro del campo **"ZPUSHNAME"**.

En la versión de la aplicación para iOS, cuando se realiza un análisis manual no existen campos en las tablas que permitan identificar de manera inmediata si se ha aplicado una determinada característica a un mensaje. Para confirmar si un mensaje ha sido editado, es necesario recurrir a indicios. Uno de ellos es que el contenido del campo **"ZPUSHNAME"** suele ser más extenso que en el resto de los mensajes. Una vez decodificado, se puede determinar con claridad que se trata de un mensaje editado, ya que los campos 7 y 8 solo aparecen en este tipo de mensajes.

En ningún caso es posible recuperar el texto del mensaje previo a la edición.

ZPUSHNAME	ZSTANZAID	ZTEXT
CIGh/rcGGhozNDY0MTk4NTQyNEBzLndoYXRzYXBwLm5ldCABOHzOUMyOD...	3A27325143F5563AE0E5	Mensaje editado por iOS

Tabla **ZWMESSAGE**

Campo	Descripción
1	Fecha en la que fue enviado el mensaje original antes de ser editado, en formato UTC Unix Epoch (segundos).
3	Identificador "jid" del usuario de esta cuenta.
4	Dirección del mensaje: 0: mensaje recibido por el usuario de esta cuenta. 1: mensaje enviado por el usuario de esta cuenta.

Campo	Descripción
7	Identificador del mensaje antes de ser editado.
8	Fecha en la que fue editado el mensaje en formato UTC Unix Epoch (milisegundos).
15	Fecha en la que fue enviado o recibido el mensaje editado en este dispositivo en formato UTC Unix Epoch (milisegundos).

Ilustración 234. Tabla “ZWMESSAGE” y campos del archivo protobuf almacenado en el campo “ZPUSHNAME”

Exclusivamente, cuando la edición la realiza el usuario de esta cuenta, se graba información del cambio en el archivo protobuf almacenado en el campo “ZRECEIPTINFO” de la tabla “ZWMESSAGEINFO”.

Campo	Campo	Descripción
2	1	Número de teléfono del contacto o usuario de esta cuenta que ha recibido o enviado el mensaje editado, con prefijo internacional, precedido del número “81” y finalizado con el carácter “f”. Ejemplo: 8134677456456f <i>*Si se trata de un chat grupal, hay tantos campos como éste como contactos hayan recibido el mensaje editado.</i>
3		Fecha en la que se transmitió el mensaje original antes de ser editado, en formato UTC Unix Epoch (segundos).
10 (información de la edición del mensaje)	2	Identificador del mensaje antes de ser editado.
	3	Texto final del mensaje, tras haber sido editado.
	4	Fecha en la que se editó el mensaje en formato UTC Unix Epoch (milisegundos).

Ilustración 235. Archivo protobuf del campo “ZRECEIPTINFO” de la tabla “ZWMESSAGEINFO”

9.2. Notas de voz y vídeo

Las notas de voz son un tipo de mensaje cuyo uso se ha extendido entre los usuarios por la rapidez y comodidad que supone para las comunicaciones diarias. Las notas de vídeo se han implantado recientemente y no hay que confundirlas con el envío de archivos de vídeo.

Cuando se graba y envía una nota de voz, en la pantalla del chat se muestra un reproductor de audio, y en el caso de la nota de vídeo, se muestra un fotograma en un círculo. En las versiones analizadas de Android e iOS es posible la transcripción de las notas de voz en varios idiomas, entre los que se encuentra el español.

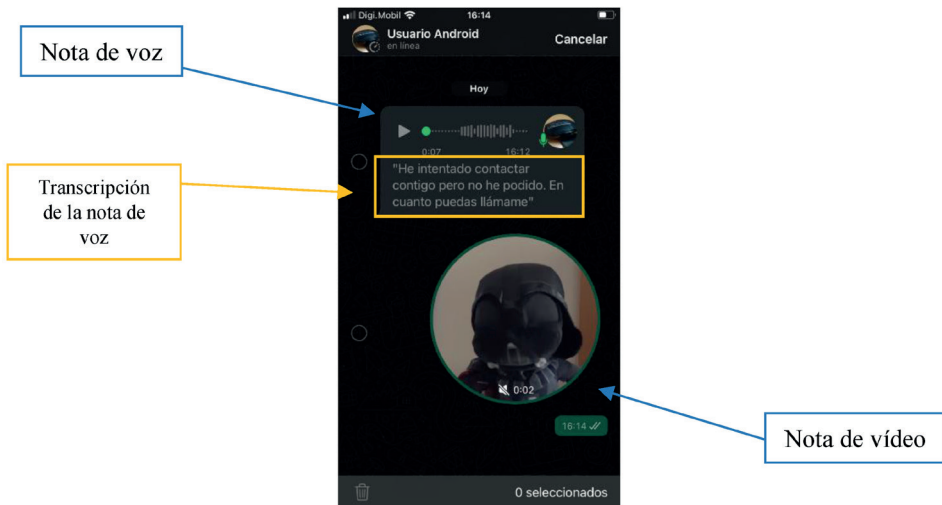


Ilustración 236. Nota de voz y de vídeo en iOS (similar en Android)

Hay un par de diferencias significativas entre las notas de voz y las notas de vídeo. La primera es que existe la posibilidad de enviar notas de voz de visualización única, que tras su reproducción son eliminadas, pero no existe esa opción con las notas de vídeo. Por otro lado, las notas de voz se descargan automáticamente, independientemente de las opciones de descarga que tenga asignadas el usuario, mientras que las notas de vídeo dependen de esas opciones.

Android

Estos mensajes tienen ciertas particularidades, algunas compartidas con los mensajes de visualización única. Como con todos los mensajes, hay que consultar la tabla **"message"** de la base de datos **"msgstore.db"**. El campo por el que se define el tipo de mensaje denominado **"message_type"**, es determinante en el caso de las notas de vídeo, que adquiere el valor **"81"** y en las notas de voz de visualización única el valor **"82"**. Con las notas de voz "normales" es algo más complejo, ya que los desarrolladores no le han otorgado un valor único para el campo **"message_type"**, sino que comparte con los archivos de audio el valor **"2"**.

Una de las diferencias entre ambos tipos de mensaje (nota de voz vs. audio) se observa en el campo **"origination_flags"** de la tabla **"message"** que, en las pruebas realizadas, las notas de voz presentan exclusivamente alguno de estos valores: **"32768"**, **"32769"**, **"33024"** o **"33025"**. Se puede confirmar que se trata de una nota de voz consultando el archivo que se ha transmitido en la tabla **"message_media"**. Si es un archivo de audio, el nombre del archivo comenzará por **"AUD-"**, mientras que una nota de voz empezará por **"PTT-"**.

Las notas de voz se descargarán automáticamente en el dispositivo sea cual sea la configuración asignada en las opciones de descarga del usuario. En el caso de las notas de vídeo, dependerá de las opciones asignadas por el usuario.

Si el usuario hace uso de la transcripción de la nota de voz, el audio transcrito se localiza en los campos **"raw_transcription_text"** y **"c0content"** de las tablas **"message_media"** y **"message_ftsv2_content"** respectivamente.

En la última versión de la aplicación para Android analizada (2.25.32.75), **en el supuesto de que la nota de voz de visualización única sea transcrita, el texto permanece** en el campo **"raw_transcription_text"** de la tabla **"message_media"**. Cuando el usuario pulsa la función transcribir en la nota de voz de visualización única, no se muestra en pantalla la transcripción (el usuario creerá que no lo ha llevado a cabo) pero realmente se realiza y se graba en la base de datos.

iOS

En la versión de iOS, el tipo de mensaje se almacena en el campo **"ZMESSAGE"** de la tabla **"ZWMESSAGE"**. Las notas de voz, al igual que los archivos de audio, adquieren el valor **"3"** en el campo **"ZMESSAGE"**. A pesar de este inconveniente, se pueden diferenciar nota de voz y archivo de audio por el **tipo MIME** registrado en el campo **"ZVCARDSTRING"** de la tabla **"ZWAMEDIAITEM"**: en la primera, "audio/ogg; codecs=opus"; en el archivo de audio, frecuentemente "audio/mpeg".

Las notas de vídeo presentan el valor **"54"** y las notas de voz de visualización única el valor **"53"**.

Si el usuario hace uso de la transcripción de la nota de voz, el audio transcrito se localiza en el archivo protobuf del campo **"ZMETADATA"** de la tabla **"ZWAMEDIAITEM"**. Una vez decodificado el archivo, el texto de la transcripción se encuentra en el campo **74-2**. Los campos comunes del archivo protobuf, se pueden consultar en el apartado 5.3.7 **ZWAMEDIAITEM**.

En el supuesto de que la nota de voz de visualización única sea transcrita, ésta no se grabará en las bases de datos.

9.3. Mensajes adjuntando imágenes y vídeos

La aplicación WhatsApp está desarrollada para facilitar al usuario el envío de este tipo de archivos e intenta que sea lo más dinámico posible. Por ello, posibilita el envío desde varias opciones diferentes. El método utilizado para enviar la imagen/vídeo tiene una gran repercusión en la forma en la que la aplicación procesará el archivo y el modo en el que se registrará la interacción en las bases de datos.

Francisco Arenaz Benito
Análisis de mensajes (Android – iOS)



Ilustración 237. Opciones para adjuntar archivos de la aplicación en Android (dcha.) e iOS (izq.)

La aplicación admite enviar los archivos en calidad estándar (con alta tasa de compresión) o en alta calidad "HD" (con compresión menor, sin llegar a la calidad original), tanto cuando se envían los archivos generados con la cámara a través de la aplicación como cuando se seleccionan desde el almacenamiento del dispositivo (Galería en Android o Fotos en iOS):

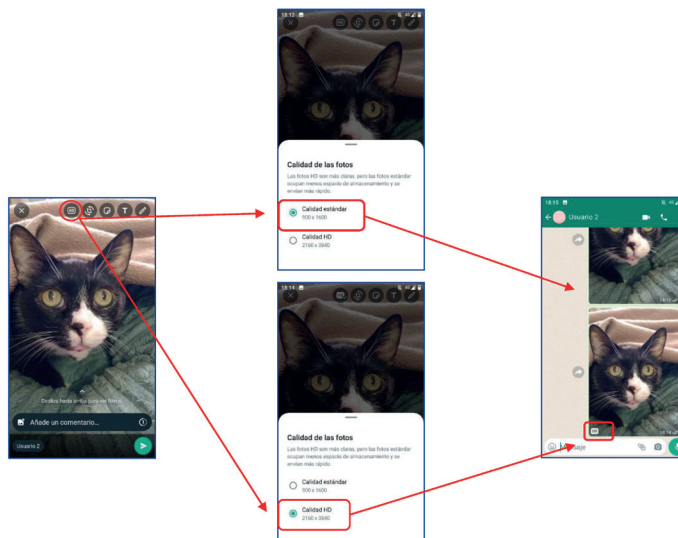
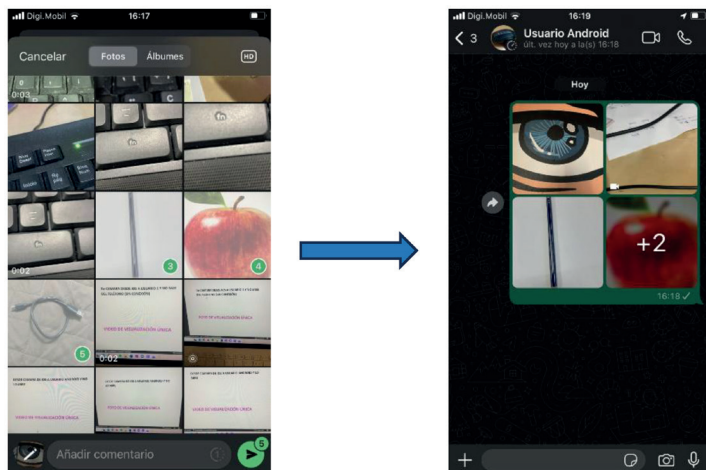


Ilustración 238. Envío de imágenes en calidad estándar y HD en la versión de Android (similar en iOS)

Por otro lado, la aplicación permite transmitir dos o más archivos de imagen y vídeo en un solo envío, a lo que WhatsApp denomina el envío de un “**álbum**”:



*Ilustración 239. Selección de imágenes y vídeos para el envío de un “**álbum**” en la versión de iOS (similar en Android)*

Android

En primer lugar, se puede seleccionar y enviar archivos de imagen o vídeo desde la galería del teléfono. La aplicación generará una copia de la imagen o del vídeo original, pero comprimido (conlleva la eliminación de los metadatos), para que tenga menor tamaño y sean necesarios menos recursos para su transmisión. Los archivos enviados se almacenarán en la carpeta **.../media/com.whatsapp/WhatsApp/Media/WhatsApp Images/Sent** (imágenes) o **.../media/com.whatsapp/WhatsApp/Media/WhatsApp Video/Sent** (vídeos) y se enviarán al chat correspondiente.

En segundo lugar, se puede capturar una imagen o un vídeo seleccionando el icono de la cámara desde la propia aplicación de WhatsApp que será enviado al chat elegido. La imagen o vídeo capturado por la cámara será almacenado en la carpeta **.../media/com.whatsapp/WhatsApp/Media/WhatsApp Images/** (las imágenes) o **.../media/com.**

whatsapp/WhatsApp/Media/WhatsApp Video/ (los vídeos). Al obtener el archivo por medio de la aplicación, el archivo creado tendrá la nomenclatura típica, “IMG” o “VID” seguida de “-AAAAMMDD-WAXXXX⁹”, manteniendo la resolución predeterminada de la cámara y conteniendo metadatos.

Seguidamente, la aplicación generará una copia comprimida del archivo (lo que implica la eliminación de los metadatos), la renombrará con numeración secuencial y la enviará. Por ejemplo, si la imagen tomada con la cámara es IMG-20230825-WA0001, la imagen comprimida y finalmente enviada será la IMG-20230825-WA0002. Si el archivo es una imagen, lo guardará en la carpeta **.../media/com.whatsapp/WhatsApp/Media/ WhatsApp Images/Sent** y si fuera un vídeo en **.../media/com.whatsapp/WhatsApp/Media/ WhatsApp Video/Sent** y lo enviará al chat correspondiente.

Tanto en el primer caso (envío de una imagen o vídeo almacenado en el teléfono) como en el segundo (captura con la cámara del dispositivo), se puede obtener el hash SHA-256 del archivo original y del archivo enviado (comprimido) en la tabla “**message_media**”. Hay que aclarar que solo se obtendrá información del hash del archivo original en los mensajes enviados por el usuario de la cuenta y únicamente la primera vez que se envíe:

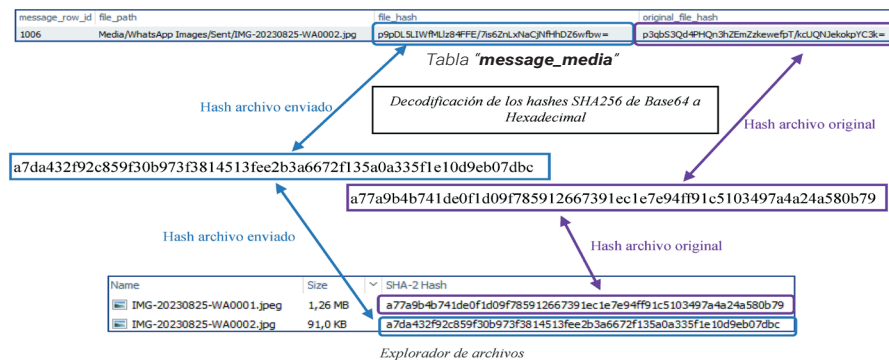


Ilustración 240. Obtención de hashes SHA-256 de los archivos originales y sus comprimidos enviados.

9. AAAA es el año, MM es el mes, DD es el día y XXXX es la numeración que empieza desde 0000 va incrementando en una unidad.

message_row_id	chat_row_id	file_path	file_hash	original_file_hash
2871	239	Media/WhatsApp Images/Sent/DMS-20250110-WA0070.jpg	UUqJ3HEOd3xRDctpq7EHnbgJlPpp2R9eqtgJuhKE=	HeysGRpdmBP22R6G1WIEYn8fbx5TEJlvZn2GDM=
2873	242	Media/WhatsApp Images/Sent/DMS-20250110-WA0070.jpg	UUqJ3HEOd3xRDctpq7EHnbgJlPpp2R9eqtgJuhKE=	

Ilustración 241. Envío de la misma fotografía a dos chats y únicamente del primer envío se registra el hash del original.

Como tercera opción, se puede adjuntar la imagen o el vídeo como documento. La aplicación admite navegar por un explorador de archivos y elegir cualquier tipo de archivo, entre ellos imágenes y vídeos. Este método es el menos intuitivo y conlleva diferencias relevantes respecto a los otros dos: **no se comprime ni pierde metadatos**, pero genera una copia del original a la que se le asignará el nombre "DOC-AAAAM-MDD-WAXXXX" (indistintamente sea imagen o vídeo) que será almacenada en la carpeta **.../media/com.whatsapp/WhatsApp/Media/WhatsApp Documents/sent** y lo enviará al correspondiente chat.

Otra de las particularidades del envío de una imagen o un vídeo como documento, es que la aplicación no genera miniatura (thumbnail) ni en el dispositivo que envía ni en el que recibe; por tanto, no se muestra una imagen como representación del archivo, a diferencia de los otros dos casos.

Por otro lado, la aplicación permite transmitir dos o más archivos de imagen o vídeo en un "álbum", seleccionándolos desde la Galería. Cuando se recibe o envía un álbum se genera un registro en la tabla **"message"**, en cuyo campo **"message_type"** presenta el valor **"99"**. Tras este mensaje de álbum se registra un mensaje por cada archivo multimedia transmitido, con la particularidad de que todos los mensajes tendrán aproximadamente la misma fecha de salida o entrada y todos presentan el mismo **"origination_flags"**:

_id	chat_row_id	from_me	key_id	sender_id_row_id	status	broadcast	recipient_count	origination_flags	origin	timestamp	message_type
4782	322	0	ACA8468626EB1CF0FC0769070F5A5B26	0	0	0	0	256	0	04/11/2025 15:53:43	99
4783	322	0	ACE0DAED22E4EF4FCA12C4E173A338C	0	0	0	0	67109120	0	04/11/2025 15:53:43	3
4784	322	0	ACRE9B9626D7C6E1EDAF538DE9293D4A	0	0	0	0	67109120	0	04/11/2025 15:53:44	1
4785	322	0	AC6E2FE077D23B2CCEB51FCB55E1A6BD5	0	0	0	0	67109120	0	04/11/2025 15:53:44	1
4786	322	0	AC589FE949780F872C82D7565413C697	0	0	0	0	67109120	0	04/11/2025 15:53:44	3

Ilustración 242. Tabla "message"

La confirmación de los mensajes enviados en un mismo álbum se registra en la tabla **"message_association"**, donde todos los mensajes

de archivos multimedia del álbum (campo **"child_message_row_id"**) están asociados al mismo mensaje de álbum (campo **"parent_message_row_id"**):

id	child_message_row_id	parent_message_row_id
156	4783	4782
159	4786	4782
160	4787	4782
161	4784	4782

Ilustración 243. Tabla **"message_association"**

Excepciones

En una investigación nos podemos encontrar que supuesta o aparentemente falte un archivo. Analizando los chats de un día concreto, se observa que hay un salto de una unidad en la numeración de los archivos transmitidos. En la siguiente imagen se muestra como en la tabla **"message_media"** falta supuestamente un archivo (con numeración WA0001):

message_row_id	file_path	media_key_timestamp
1005	Media/WhatsApp Images/Sent/IMG-20230825-WA0000.jpg	25/08/2023 6:37:38
1006	Media/WhatsApp Images/Sent/IMG-20230825-WA0002.jpg	25/08/2023 6:38:09
1007	Media/WhatsApp Video/Sent/VID-20230825-WA0003.mp4	25/08/2023 6:39:29

Ilustración 244. Tabla **"message_media"**

Podría haber sido borrado el mensaje con su correspondiente archivo, pero como se puede observar en el campo **"message_row_id"** los mensajes son secuenciales y no falta ninguno; por lo tanto, no hay ningún mensaje eliminado. En este caso, lo que ha sucedido es que se generó una fotografía desde la propia aplicación de WhatsApp. Si dicha fotografía se envía en un chat, por un lado, guardará la fotografía original en la carpeta **/data/media/0/WhatsApp/Media/WhatsApp Images/** y por otro, se creará a partir de la original una *fotografía comprimida*, que se guardará en la carpeta **/data/media/0/WhatsApp/Media/WhatsApp Images/Sent** y se enviará al chat.

En la siguiente imagen se presentan los datos de la fotografía cuyo nombre es IMG-20230825-WA0001.jpeg, la cual es la fotografía original

a partir de la que se ha generado la fotografía enviada con nombre IMG-20230825-WA0002.jpg:

Name	Size	Created (Canary)	Modified (Canary)	Full path
IMG-20230825-WA0001.jpeg	1,26 MB	25/08/2023 07:38:05 enr	25/08/2023 07:38:05	/data/media/0/WhatsApp/Media/WhatsApp Images/IMG-20230825-WA0001.jpeg
IMG-20230825-WA0002.jpg	91,0 KB		25/08/2023 07:38:08	/data/media/0/WhatsApp/Media/WhatsApp Images/Sent/IMG-20230825-WA0002.jpg

Ilustración 245. Explorador de archivos

Pero qué sucede si desde la aplicación WhatsApp se abre la cámara y se obtiene una fotografía o un vídeo, pero finalmente no se envía a ningún chat. Como se ha creado un archivo, aunque temporalmente, la aplicación le asigna la siguiente numeración que le corresponde como archivo de WhatsApp. Debido a que no se envía, finalmente no se graba en el dispositivo y la numeración del archivo se pierde.

Este es otro motivo por el cual puede aparentemente "faltar" un archivo de fotografía o vídeo (por numeración): tras la captura, el usuario descartó el envío. Toda esta casuística debe considerarse antes de afirmar y determinar que se eliminó un archivo transmitido.

Por otro lado, cuando se envía y/o recibe en más de una ocasión un mismo archivo, únicamente se almacenará una copia y mantendrá el mismo nombre en los mensajes. Tiene que ser exactamente el mismo archivo y se almacenará en la ubicación donde le correspondió al primer archivo por el tipo de transmisión.

Por ejemplo, si se recibe una imagen con temporalidad, procedente de un chat restringido o un chat con la "privacidad avanzada del chat" activada, se almacenará en la carpeta **.../WhatsApp/Media/WhatsApp Images/Private**. Al reenviarlo, no se creará uno nuevo en la carpeta **.../WhatsApp/Media/WhatsApp Images/Sent** sino que se mantendrá únicamente el primero. Para poder determinar la cantidad de copias de un archivo que se ha enviado/recibido se puede consultar la tabla "**media_refs**" de la base de datos "**msgstore.db**".

Si se elimina un mensaje con ese archivo, también disminuirá en una unidad la contabilización en dicha tabla. Esta eficiencia de almacenamiento de archivos no es exclusiva de imágenes y vídeos, se aplica también a otros tipos (GIFs, avatares, notas de voz, etc.). Se ha incluido

en este apartado porque suele ser más común entre los usuarios de WhatsApp el envío a múltiples chats de imágenes y vídeos.

Los documentos presentan la particularidad de diferenciarse entre enviados (nomenclatura "DOC- ") y los recibidos (conservan el nombre original).

Análisis de las bases de datos

Las tablas que son de interés en la transmisión de este tipo de archivos son **"message"**, **"message_media"** y **"message_thumbnail"**.

A partir de la tabla **"message"** se puede determinar el tipo de archivo que se transmitió, participantes, dirección del envío y fecha, entre otros datos, así como relacionarlo con las otras dos tablas. Dependiendo del tipo de análisis que se esté efectuando, puede ser conveniente consultar el campo **"origin"** para identificar el origen del archivo transmitido (la aplicación, galería, terceras aplicaciones, etc).

De la tabla **"message_media"** se obtiene el nombre del archivo transmitido y su hash SHA-256. Siempre que sea un archivo enviado por el usuario, se registrará el hash SHA-256 del archivo original (sin comprimir). Anteriormente ya se ha explicado que el hash está codificado en Base64 y hay que decodificarlo a hexadecimal para obtener el hash. También almacena mucha más información, como es el tamaño del archivo, si se ha descargado en el dispositivo, etc.

Asimismo, esta tabla contiene un campo de gran importancia cuando se envía una imagen o vídeo como documento. Se trata del campo **"mime_type"**, que indica el tipo de MIME real del archivo. En el siguiente ejemplo se ha enviado una imagen como documento, pero por el tipo de MIME se determina que es una imagen:

message_row_id	chat_row_id	file_path	mime_type	thumbnail_height_width_ratio
1250	81	Media/WhatsApp Documents/Sent/DOC-20230903-WA0009.	image/jpeg	0

Ilustración 246. Tabla **"message_media"**

Con respecto a los thumbnails o miniaturas generadas por la aplicación, se almacenan en la propia base de datos, concretamente en la tabla **"message_thumbnail"**. Por tanto, el borrado de imágenes, vídeos o archivos pdf desde la galería del dispositivo no afecta a sus respectivas miniaturas, las cuales se conservan en la base de datos.

La forma de relacionar las tres tablas **"message"**, **"message_media"** y **"message_thumbnail"** es a través del número de fila o registro (campo **"_id"**) de la tabla **"message"**:

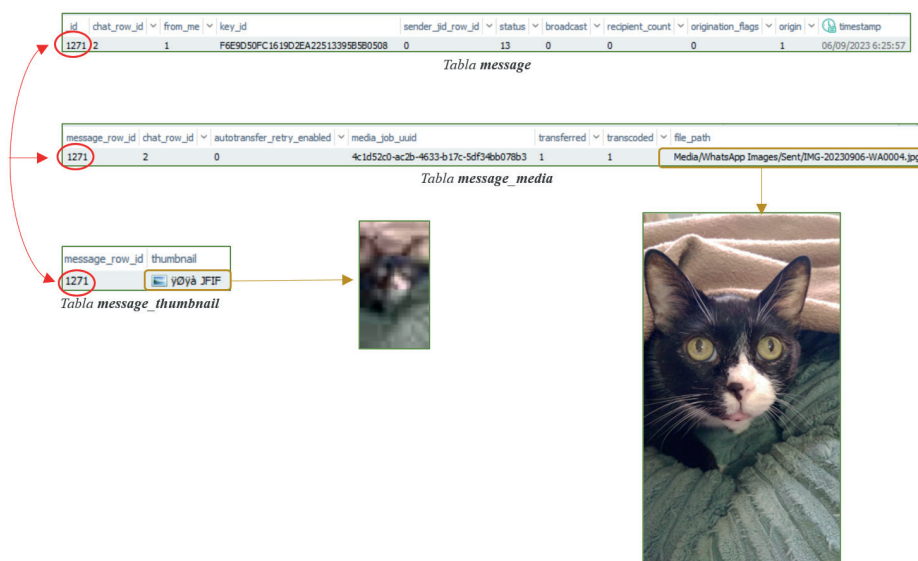


Ilustración 247. Relación entre tablas de la imagen transmitida y su thumbnail

Cuando el usuario elimina una imagen o un vídeo desde la galería o el explorador de archivos del dispositivo, la información almacenada en las bases de datos permanece intacta. Dado que no se ha interactuado directamente con la aplicación para realizar esta eliminación, toda la información en las bases de datos permanece intacta. En los casos en que el archivo haya sido recibido de otro usuario, se almacenará el hash del archivo recibido (comprimido) y el **thumbnail**. Si el archivo fue enviado desde este dispositivo, se guardará tanto el hash del archivo comprimido como el hash del archivo original, además del **thumbnail**.

Cabe recordar que, cuando se envía una imagen o un vídeo capturado a través de WhatsApp o seleccionado desde la galería, se genera un archivo comprimido que es el que realmente se transmite. Por lo tanto, es posible que el usuario elimine uno de los dos archivos (el comprimido o el original), mientras que el otro permanece en el dispositivo. Gracias a la base de datos **“msgstore.db”**, se podría vincular el archivo conservado con el mensaje enviado.

Si se elimina desde el chat un mensaje que contiene imagen o vídeo (enviado o recibido), el usuario puede optar por borrar solo el mensaje o de eliminarlo junto con el archivo de la galería. En ambos casos, se perderá la información de las bases de datos relacionada con el envío o la recepción del archivo (incluido el thumbnail), y en la segunda opción, también se borrará el archivo en sí.

Sin embargo, como se explicó anteriormente, cuando se envía una imagen o un vídeo generados desde WhatsApp, ésta comprime el original antes de enviarlo. Al eliminar el mensaje, la aplicación eliminará el archivo comprimido, pero no el original, que permanecerá en la galería del dispositivo en la ruta de la carpeta de WhatsApp (.../media/com.whatsapp/WhatsApp/Media/WhatsApp Images/ para imágenes, o .../media/com.whatsapp/WhatsApp/Media/WhatsApp Video/ para vídeos).

Es importante destacar que, aunque el archivo original se mantenga en el dispositivo, **NO será posible vincularlo con el chat en el que se transmitió.**

iOS

Al igual que en Android, desde un iPhone se puede seleccionar una imagen o un vídeo desde la aplicación Fotos para enviarla. WhatsApp generará una versión comprimida del archivo, sin metadatos, para su transmisión. Esta versión comprimida se almacenará en el directorio que crea la aplicación para cada uno de los chats **.../Message/Media/xxxxxxxxxxxxx /** (representando las "x" el identificador "jid" del contacto, grupo, canal...).

Es conveniente recordar que, en la versión de iOS, todos los archivos (tanto enviados como recibidos) compartidos con un contacto, grupo, etc. se almacenan en el directorio que crea la aplicación para cada uno de ellos. También se guardan en esos directorios los thumbnails de las imágenes y vídeos transmitidos, siendo una gran diferencia respecto a Android, que los almacena en la base de datos.

Otra opción es obtener una fotografía o un vídeo desde la propia aplicación WhatsApp mediante la cámara del dispositivo. Ese archivo creado en WhatsApp no difiere de otro que se genere desde la aplicación de la cámara, mantendrá los metadatos, se almacenará en la ruta **/private/var/mobile/Media/DCIM/100APPLE/** con el correspondiente nombre "IMG_XXXX.MP4" (vídeos) o "IMG_XXXX.JPG" (fotografías). Partiendo de este archivo, WhatsApp generará uno comprimido, eliminando sus metadatos y renombrándolo con un UUID, "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" secuencia de 32 caracteres hexadecimales seguido por la extensión del archivo.

La tercera posibilidad es adjuntándolo como documento. Este tipo de envío tiene importantes particularidades, como son que **no se comprime, no pierde ni calidad de imagen ni metadatos**, y no se genera una miniatura o thumbnail.

Por otro lado, la aplicación permite transmitir un "álbum" con dos o más archivos de imagen y/o vídeo en un solo envío, seleccionándolos desde "Fotos". Cuando se recibe o envía un álbum, se generará un registro en la base de datos que almacena los mensajes. Concretamente, en la tabla **"ZWMESSAGE"**, de la base de datos **"ChatStorage.sqlite"**, el campo **"ZMESSAGETYPE"** tomará el valor **"66"**. Tras este mensaje de

álbum, se registrará un mensaje por cada archivo multimedia transmitido, con la particularidad de que tendrán aproximadamente la misma fecha de salida o entrada:

Z_PK	ZMESSAGESTATUS	ZISFROMME	ZSPOTLIGHTSTATUS	ZMESSAGEID	ZSORT	ZCHATSESSION	ZMESSAGEDATE	ZSENTDATE	ZSTANZAID
2106	6	1	-32768	56	151	113	24/09/2025 06:22:27	24/09/2025 06:22:27	3A00BA40B4F33F17C8CD
2107	6	1	-32768	1	152	113	24/09/2025 06:22:27	24/09/2025 06:22:27	3A7AF9F1B36DD3582733
2108	6	1	-32768	1	153	113	24/09/2025 06:22:27	24/09/2025 06:22:27	3ADF52F8128CEC2FCDA
2109	6	1	-32768	1	154	113	24/09/2025 06:22:27	24/09/2025 06:22:27	3A26093815477AE12A71
2110	6	1	-32768	2	155	113	24/09/2025 06:22:27	24/09/2025 06:22:27	3A961E84A6CFE67BF171

Ilustración 248. Tabla "ZWMESSAGE"

La validación de que esos archivos multimedia han sido transmitidos en un álbum se obtendrá del análisis de la tabla "**message_parent_association**" de la base de datos "**ExtChatDatabase.sqlite**", donde se localizará un registro con la identificación de mensaje de cada archivo de imagen y/o vídeo (campo "**stanza_id**") asociado al mensaje del sistema de la transmisión de un album (campo "**parent_stanza_id**"):

stanza_id	parent_stanza_id	type	sort	chat_jid	
3A7AF9F1B36DD3582733	3A00BA40B4F33F17C8CD	1	152	346	@s.whatsapp.net
3ADF52F8128CEC2FCDA	3A00BA40B4F33F17C8CD	1	153	346	@s.whatsapp.net
3A26093815477AE12A71	3A00BA40B4F33F17C8CD	1	154	346	@s.whatsapp.net
3A961E84A6CFE67BF171	3A00BA40B4F33F17C8CD	1	155	346	@s.whatsapp.net

Ilustración 249. Tabla "ZWMESSAGE"

Cuando el usuario tiene activada la opción de "Guardar en Fotos" y recibe una imagen o un vídeo, la aplicación almacena una copia del archivo en la ruta **/private/var/mobile/Media/DCIM/100APPLE/** junto con su thumbnail. Es preciso que el chat en el que se han transmitido los archivos tenga desactivados los mensajes temporales, la "Privacidad avanzada del chat" y no sea un chat restringido, porque en caso contrario no se almacenará en "Fotos".

Esta opción "Guardar en Fotos" activada también puede generar otra copia en la caché, concretamente en la ruta **/private/var/mobile/Media/PhotoData/CPL/storage/filecache/ARM/**.

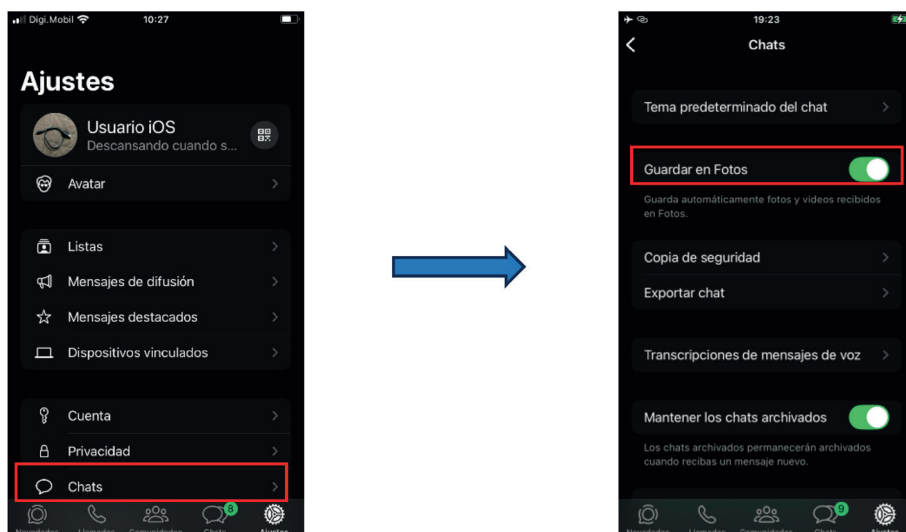


Ilustración 250. Activación del ajuste "Guardar en Fotos"

9.4. Mensajes adjuntando documentos

Cuando se transmite un archivo como documento, WhatsApp adopta un comportamiento diferente al del envío de archivos multimedia. Se considera "documento" cualquier archivo enviado a través de esta opción, aunque no sea un archivo específicamente diseñado como documento (como un PDF, Word, TXT, etc.). En realidad, puede ser cualquier tipo de archivo, incluyendo imágenes o vídeos.

Sin embargo, a diferencia de los archivos multimedia, cuando se envía un archivo como documento, **no se comprime ni pierde sus metadatos** (como ocurre con las imágenes o vídeos enviados de manera convencional).

La aplicación genera una miniatura (thumbnail) únicamente para los documentos de tipo "**pdf**", tanto cuando se envían como cuando se reciben.

El tamaño máximo de un archivo enviado como documento es de 2 GB.

Android

Cuando se envía un documento, se guarda una copia exactamente igual al original, sin compresión, en el directorio **/data/media/0/Android/media/com.whatsapp/WhatsApp/Media /Documents/Sent**, con la nomenclatura **DOC-AAAAMMDD-WAXXXX**. Cuando se recibe el archivo se almacena con su nombre original en el directorio **/data/media/0/Android/media/com.whatsapp/ WhatsApp/Media/ Documents/**.

Los thumbnails que se generan cuando se transmiten archivos de tipo "pdf" se almacenarán en la tabla **"message_thumbnail"**.

Una nueva implementación que se ha incorporado a la aplicación se encuentra el uso de la cámara para escanear documentos en formato "pdf". A los archivos generados como documento escaneado se les asigna el título "Whatsapp Scan DÍA de MES de AÑO at hh.mm.ss.pdf". Pero ese nombre únicamente se establece para mostrarlo en la aplicación, mientras el asignado al archivo generado, tal y como se almacena en el teléfono, se le aplica el nombre estándar para un documento "DOC-AAAAMMDD-WAXX".

file_path	media_name
Media/WhatsApp Documents/Sent/DOC-20251112-WA0030.pdf	Whatsapp Scan 12 de noviembre de 2025 at 10.19.00.pdf

Ilustración 251. Diferencia entre nombre real en el sistema de archivos (file_path) y el título asignado por la aplicación cuando escanea un documento (media_name), en la tabla "message_media"

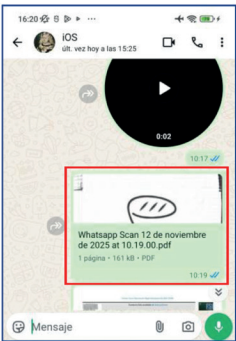


Ilustración 252. Documento escaneado enviado desde teléfono Android, con título "Whatsapp Scan 12 de noviembre de 2025 at 10.19.00.pdf", pero con nombre en el sistema de archivos "DOC-20251112-WA0030.pdf".

iOS

Cuando se envía o recibe un documento en un iPhone, se almacena en el directorio que crea la aplicación para cada uno de los chats **.../Message/Media/xxxxxxxxxxx /** (representado las "x" el identificador "jid" del contacto, grupo, canal...).

Los thumbnails que se generan cuando se transmiten archivos de tipo "pdf" se almacenarán en la misma ruta que el documento.

Entre las funcionalidades de la aplicación se encuentra el uso de la cámara para escanear documentos en formato "pdf". A los archivos generados como documento escaneado se les asigna el nombre "WhatsApp Scan AAAA-MM-DD at hh.mm.ss.pdf".

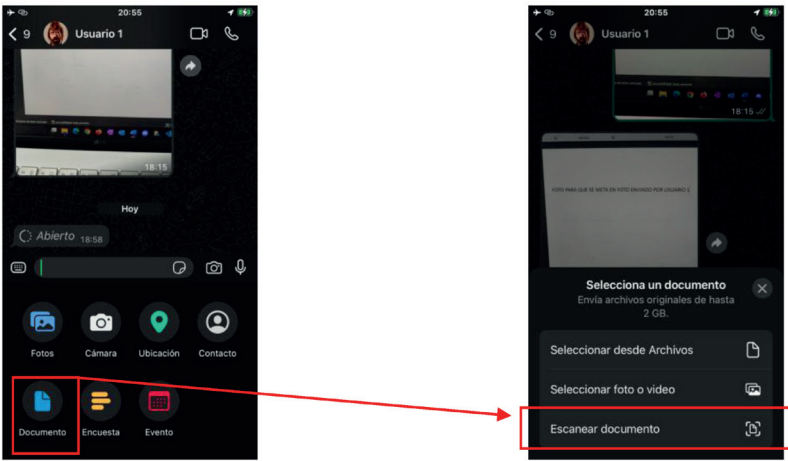


Ilustración 253. Envío de documento escaneado

En iOS, los archivos no mantienen su título en el nombre del archivo almacenado en el sistema de archivos:

ZAUTHORNAME	ZMEDIALOCALPATH
Whatsapp Scan 12 de noviembre de 2025 at 11.08.41.pdf	Media/34672572387@s.whatsapp.net/e/d/ed425966-c6d7-47ef-a0ab-9d899b12f1cf.pdf

Ilustración 254. Diferencia entre el título de un documento (ZAUTHORNAME) y el nombre real en el sistema de archivos (ZMEDIALOCALPATH) en la tabla "ZWAMEDIAITEM"

9.5. Mensajes de ubicación

La aplicación WhatsApp permite compartir la ubicación del usuario con otros participantes en chats individuales o grupales. La ubicación puede ser “en tiempo real”, de tipo dinámica (una ruta), o la denominada “actual”, que es de tipo estática (un punto geográfico).

9.5.1. Ubicación en tiempo real

Se envía en tiempo real el posicionamiento del teléfono por un periodo de tiempo predeterminado de **15 minutos, 1 hora u 8 horas**. Aunque una vez iniciada y compartida la ubicación, el usuario puede detener la comunicación cuando lo desee.

9.5.2. Ubicación actual o lugares cercanos

Se envía un posicionamiento estático del teléfono o en su caso, permite enviar la posición de un lugar cercano al dispositivo y que se pueda considerar de interés, como son comercios, restaurantes...

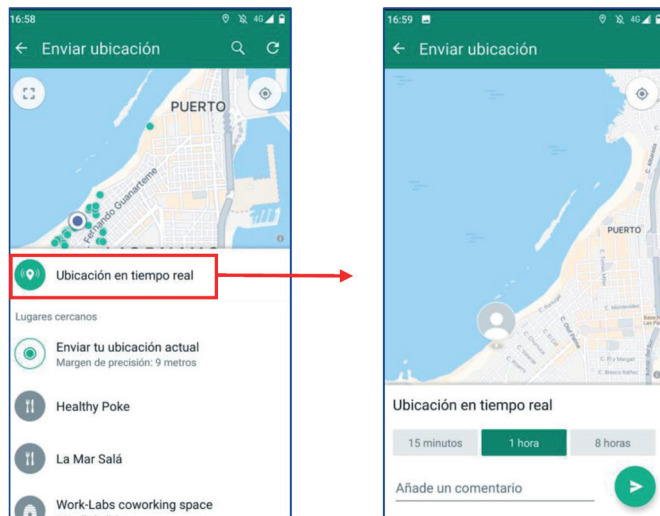


Ilustración 255. Compartir ubicación en la versión de Android (similar en iOS)

Android

Una vez localizado el registro del mensaje en el que se ha compartido la ubicación en la tabla **"message"** (valor **"5"** o **"16"** en el campo **"message_type"**), es necesario vincular y centrarse en la tabla **"message_location"** de la base de datos **"msgstore.db"**. En esta tabla se registra la información tanto cuando se ha compartido la ubicación en tiempo real como cuando se ha compartido la ubicación actual o lugares cercanos. A partir de los diferentes campos de la tabla **"message_location"**, se puede obtener información fundamental sobre las ubicaciones que ha compartido o recibido de otros contactos.

Otro archivo relevante para analizar las últimas localizaciones en tiempo real intercambiadas es la base de datos **"location.db"**. Aunque la mayoría de sus tablas suelen encontrarse vacías, gracias al archivo **"WAL"** se puede recuperar información de posiciones puntuales compartidas en las últimas localizaciones en tiempo real.

iOS

Cuando se ha determinado que se ha transmitido un mensaje con la ubicación en tiempo real o actual/lugares cercanos en la tabla **"ZWMESSAGE"** (valor **"5"** en el campo **"ZMESSAGETYPE"**), se debe consultar la tabla **"ZWAMEDIAITEM"** vinculada a dicho mensaje. En la tabla **"ZWAMEDIAITEM"** se almacena la información del inicio de la transmisión de la ubicación, la latitud y longitud, así como la duración de la transmisión.

Ocasionalmente, se puede localizar información en las tablas **"ZWAFINALLOCATIONRECIPIENT"** y **"ZWALOCATIONSENDER"** de la base de datos **"Location.sqlite"**. Estos datos se almacenan temporalmente.

9.6. Reacción a un mensaje

La reacción a un mensaje permite añadir un emoji a un mensaje recibido o enviado como modo de respuesta rápida.

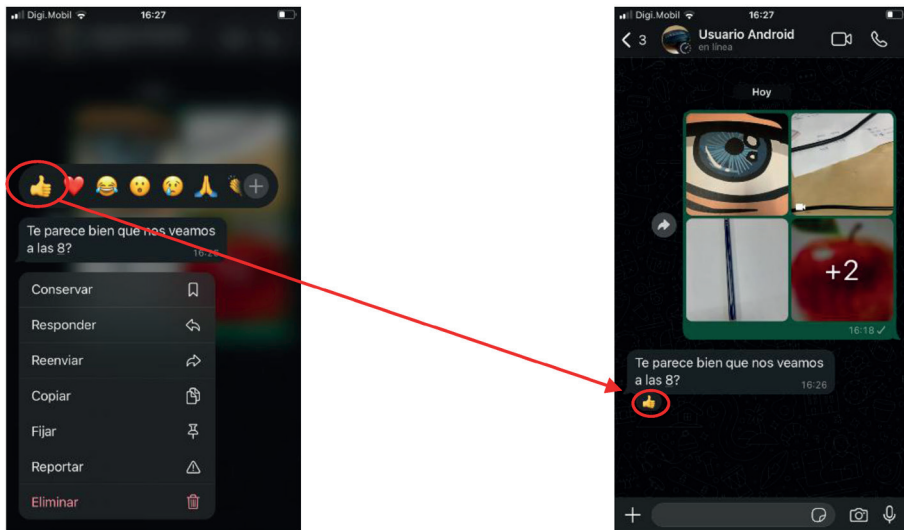


Ilustración 256. Reacción a un mensaje en la versión de iOS (similar en Android)

Android

Para determinar las reacciones a los mensajes, se debe consultar las tablas **"message"**, **"message_add_on"** y **"message_add_on_reaction"**. El dato característico de una reacción a un mensaje se encuentra en el campo **"message_add_on_type"** de la tabla **"message_add_on"**, cuyo valor será **"56"**. Esta última tabla vincula el mensaje de la tabla **"message"** con el emoji almacenado en la tabla **"message_add_on_reaction"**.

iOS

El campo **"ZRECEIPTINFO"** de la tabla **"ZWAMESSAGEINFO"** contiene un archivo **protobuf** con diferente información, incluyendo las

reacciones a un mensaje. Para determinar a qué mensaje se ha reaccionado, es necesario vincular esta tabla con **"ZWMESSAGE"** a través del campo **"ZMESSAGEINFO"**.

En el archivo **protobuf**, la existencia del campo número **7** indica que el mensaje ha recibido reacciones. Sin embargo, la estructura de este campo **7** varía según el contexto:

- Si la reacción ha sido del propio usuario.
- Si la reacción proviene de un contacto.
- Si la reacción corresponde a un mensaje dentro de un canal.

El resto de los campos presentes en este archivo **protobuf** están descritos en el apartado 5.3.10 **ZWMESSAGEINFO**.

Reacción al mensaje

Campo	Campo	Campo	Descripción
7 (reacción al mensaje)	1 (un contacto ha reaccionado) Hay tantos campos 7-1 como contactos reaccionen al mensaje.	1	Identificador del mensaje de reacción del contacto al mensaje.
		2	Identificador "jid" del contacto que ha reaccionado al mensaje.
		3	Emoji de reacción.
		4	Fecha en la que se produjo la reacción al mensaje en formato UTC Unix Epoch (milisegundos).
	2 (el usuario de esta cuenta ha reaccionado)	1	Identificador del mensaje de reacción de este usuario al mensaje.
		2	Emoji de reacción.
		3	Fecha en la que se produjo la reacción al mensaje en formato UTC Unix Epoch (milisegundos).

Campo	Campo	Campo	Descripción
7 (reacción al mensaje)	3 (un seguidor del canal ha reaccionado a un mensaje del canal) Hay tantos campos 7-3 como re-acciones al mensaje del canal.	1	Emoji de reacción.

Ilustración 257. Archivo protobuf del campo “ZRECEIPTINFO” de la tabla “ZWAMESSAGEINFO”

9.7. Mensaje reenviado

El concepto de reenvío de mensajes puede ser algo confuso. Por un lado, cuando se hace uso de la aplicación, permite seleccionar tanto el reenvío de mensajes recibidos como los mensajes que han sido enviados por el usuario de la cuenta. En ambos casos la aplicación lo denomina “reenvío” en las opciones de envío.

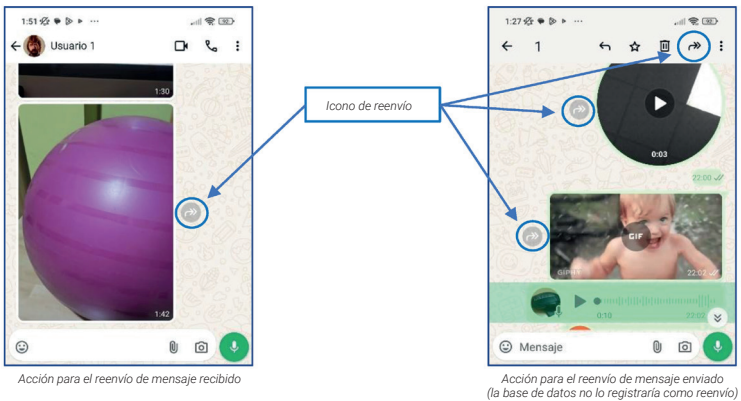


Ilustración 258. Reenvío de mensajes en la versión de Android (similar en iOS)

Sin embargo, en la base de datos, única y exclusivamente se considera reenviado cuando se emite un mensaje recibido previamente de otro contacto y no cuando el usuario vuelve a enviar un mensaje propio (aunque sea a contactos distintos).

El mensaje puede ser entrante (un contacto reenvía un mensaje que recibió de un tercero) o saliente (el usuario reenvía a un contacto un mensaje que recibió de otro contacto). Solo en estos casos se puede observar en la parte superior del bocadillo del mensaje el término "reenviado"; y cuando el reenvío entre distintos usuarios llega a las 5 ocasiones o más, la aplicación advierte a los usuarios que se ha "Reenviado muchas veces".

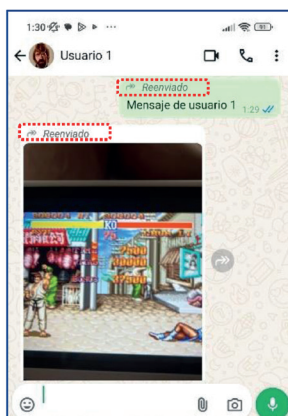


Ilustración 259. Mensajes reenviados en la versión de Android (similar en iOS)

Hay una serie de particularidades que tiene la opción de reenvío de mensajes, entre las que se encuentran las siguientes:

- La aplicación no permite reenviar notas de vídeo recibidas ni encuestas.
- No se puede aplicar la visualización única a los archivos reenviados de imagen, vídeo y notas de voz.

Android

Para determinar que un mensaje ha sido reenviado, se tiene que consultar la tabla **"message_forwarded"**. Dentro de dicha tabla, el valor del campo **"message_row_id"** se corresponde con el del campo **"_id"** de la tabla **"message"**, señalando el mensaje que fue reenviado.

En el campo **"forward_score"** se registra el número de veces que se ha reenviado un mensaje. A partir de 5 reenvíos, se registra el valor **"127"**, advirtiendo que el mensaje se ha "Reenviado muchas veces".

iOS

El reenvío de mensajes se verifica en el archivo protobuf del campo **"ZMETADATA"** de la tabla **"ZWAMEDIAITEM"**. Tras su decodificación, la existencia del campo **"17"** especifica que es un mensaje reenviado.

Partiendo del mensaje que interesa en la tabla **"ZWAMESSAGE"**, se consulta el valor del campo **"ZMEDIAITEM"**, que coincide con el valor del campo **"Z_PK"** de la tabla **"ZWAMEDIAITEM"**, siendo donde se encuentra la información que determina este tipo de mensaje (campo **"ZMETADATA"**).

Archivo protobuf del campo **"ZMETADATA"** de la Tabla **"ZWAMEDIAITEM"** decodificado

Campos comunes:

Campo	Campo	Descripción
4		URL parcial en la que se encuentra el archivo del mensaje.
29		Temporalidad aplicada al mensaje.
33		Fecha en la que se envió el mensaje en formato UTC OS X Epoch.
35		Fecha en la que se cambió la temporalidad de los mensajes en el chat en formato UTC Unix Epoch (segundos)
47	3	Resolución horizontal (píxeles) del thumbnail señalado en el campo "47-8".

Campo	Campo	Descripción
47	4	Resolución vertical (píxeles) del thumbnail señalado en el campo "47-8".
	6	Hash SHA256 del thumbnail señalado en el campo "47-8".
	8	Ruta parcial en el dispositivo en el que se encuentra el thumbnail del archivo pdf que se encuentra en el mensaje.

Ilustración 260. Archivo protobuf del campo "ZMETADATA" de la Tabla "ZWAMEDIAITEM"

Campo "17" determina que se trata de un mensaje reenviado:

Campo	Descripción
17 (mensaje reenviado)	Valores del 1 al 4 indican el número de veces que el mensaje ha sido reenviado entre diferentes usuarios. Valor " 127 " indica que se ha reenviado al menos 5 veces y se muestra el texto "Reenviado muchas veces" en el chat.
21	Identificador "jid" del contacto que envió el mensaje al usuario de esta cuenta y que éste ha reenviado. Este campo aparece exclusivamente cuando el mensaje ha sido reenviado por el usuario de esta cuenta.

Ilustración 261. Archivo protobuf del campo "ZMETADATA" de la Tabla "ZWAMEDIAITEM"

9.8. Citar un mensaje

Los mensajes que citan otros mensajes son los que responden a un mensaje transmitido previamente; puede ser propio o de un contacto.



Ilustración 262. Mensaje citado en la versión de Android (similar en iOS)

Android

Tanto los mensajes en los que el usuario cita un mensaje como aquellos en los que el interlocutor cita un mensaje, quedan registrados en la tabla **"message_quoted"**, a partir de la cual se puede establecer el mensaje que se ha citado (campo **"message_row_id"**), en qué chat (campo **"chat_row_id"**), el texto añadido (campo **"text_data"**) y otros datos de interés.

Gracias al valor del campo **"message_row_id"**, que coincide con el valor del campo **"_id"** de la tabla **"message"**, pueden vincularse ambas tablas y localizar el mensaje que ha sido citado.

iOS

La información que almacena el dispositivo es más amplia si el usuario de la cuenta cita un mensaje que si lo lleva a cabo un contacto. Como la mayoría de las características que se pueden aplicar a los mensajes en sistemas iOS, la información reside en archivos protobuf.

El mensaje que cita a otro es el que almacena la información de esta característica. Se genera un archivo protobuf en el campo **"ZMETA-DATA"** de la tabla **"ZWAMEDIAITEM"** con la información relativa a la citación del mensaje. Por otro lado, entre los datos registrados en la base de datos del mensaje citado no hay ninguno que indique que haya sido citado.

Partiendo del mensaje que interesa en la tabla **"ZWAMESSAGE"**, se consulta el valor del campo **"ZMEDIAITEM"**, el cual es el mismo que el valor del campo **"Z_PK"** de la tabla **"ZWAMEDIAITEM"**. En esta última tabla es donde se encuentra la información que determina este tipo de mensaje (campo **"ZMETADATA"**).

Una vez decodificado el archivo protobuf, la presencia del campo **"19"** indica que este mensaje cita otro mensaje. Dentro de este campo **"19"** se generan subcampos específicos por el tipo de mensaje que se ha citado (vídeo, texto, imagen, documento...). Además, se añade una

mayor complejidad a la interpretación de este archivo, porque los subcampos con la misma numeración pueden variar en su significado según el tipo de archivo al que se haga referencia. Por ello, primero se exponen los campos comunes para todos los tipos de mensajes y posteriormente se detalla el campo número “19” según cada tipo de archivo:

Archivo protobuf del campo “ZMETADATA” de la Tabla “ZWAMEDIAITEM” decodificado

Campos comunes:

Campo	Campo	Descripción
4		URL parcial en la que se encuentra el archivo del mensaje que cita a otro mensaje.
5		Identificador del mensaje que ha sido citado.
6		Identificador “jid” del emisor del mensaje que ha sido citado. Cuando el mensaje citado es el usuario de esta cuenta no se encontrará este campo.
7		Cuando se menciona de forma privada al usuario o un contacto en un estado, el valor es “status@broadcast”.
29		Temporalidad aplicada al mensaje que cita otro mensaje.
32	4	Fecha en la que se transmitió el mensaje que cita otro mensaje en formato UTC Unix Epoch (milisegundos).
33		Fecha en la que se envió el mensaje que cita otro mensaje en formato UTC OS X Epoch.
35		Fecha en la que se aplicó la temporalidad en el chat en que se cita el mensaje en formato UTC Unix Epoch (segundos).
47	3	Resolución horizontal (píxeles) del thumbnail señalado en el campo “47-8”.
	4	Resolución vertical (píxeles) del thumbnail señalado en el campo “47-8”.
	6	Hash SHA256 del thumbnail señalado en el campo “47-8”.
	8	Ruta parcial en el dispositivo en el que se encuentra el thumbnail del archivo pdf que se encuentra en el mensaje que cita a otro mensaje.

Ilustración 263. Archivo protobuf del campo “ZMETADATA” de la tabla “ZWAMEDIAITEM”

El tipo de archivo citado está determinado por el subcampo que se encuentra dentro del campo "19":

Mensaje de texto (1 o 6), enlace o link (6):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	1 (mensaje de texto)	1	Texto del mensaje citado.
		2	URL a la que dirige el enlace.
		4	URL a la que dirige el enlace.
		5	Descripción del enlace.
		6	Descripción del enlace.
		10	Thumbnail o miniatura en hexadecimal de la imagen del enlace citado (si se genera un archivo a partir del contenido en un editor de hexadecimal será visible).
	6 (mensaje de texto o link)	11	URL parcial en la que se encuentra el archivo del mensaje citado.
		12	Fecha en la que se transmitió el mensaje citado en formato UTC Unix Epoch (segundos).
		16	Thumbnail o miniatura en hexadecimal del archivo que se encuentra en el mensaje citado (si se genera un archivo a partir del contenido, en un editor de hexadecimal, se creará una imagen visible).
		17	25 Temporalidad aplicada al mensaje citado.
			26 Fecha en la que se aplicó la temporalidad en el chat del mensaje citado en formato UTC Unix Epoch (segundos).
		19	Fecha en la que se transmitió el mensaje citado en formato UTC Unix Epoch (segundos).

Ilustración 264. Archivo protobuf del campo "ZMETADATA" de la tabla "ZWAMEDIAITEM"

Imagen (3) o imagen de visualización única (55-1-3):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	3 (imagen) 55-1-3 (imagen visualización única)	1	URL en la que se encuentra el archivo del mensaje citado.
		2	Tipo de MIME del archivo del mensaje citado.
		3	Texto del mensaje citado.
		4	Hash SHA256 del archivo que se encuentra en el mensaje citado.
		5	Tamaño en bytes del archivo del mensaje citado.
		6	Resolución horizontal (píxeles) imagen o vídeo del mensaje citado.
		7	Resolución vertical (píxeles) de la imagen o vídeo del mensaje citado.
		11	URL parcial en la que se encuentra el archivo del mensaje citado.
		12	Fecha en la que se transmitió el mensaje citado en formato UTC Unix Epoch (segundos).
		16	Thumbnail o miniatura en hexadecimal del archivo que se encuentra en el mensaje citado (si se genera un archivo a partir del contenido, en un editor de hexadecimal, se creará una imagen visible).
		17	25 Temporalidad aplicada al mensaje citado.
		26	Fecha en la que se aplicó la temporalidad en el chat del mensaje citado en formato UTC Unix Epoch (segundos).

Ilustración 265. Archivo protobuf del campo **"ZMETADATA"** de la tabla **"ZWAMEDIAITEM"**

Tarjeta de contacto (4):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	4 (tarjeta de contacto)	1	Nombre del contacto.
		16	Información de la tarjeta de contacto.
		17	25 Temporalidad aplicada al mensaje citado.

Ilustración 266. Archivo protobuf del campo **"ZMETADATA"** de la tabla **"ZWAMEDIAITEM"**

Ubicación actual o sitios cercanos (5):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	5 (ubicación actual)	1	Latitud geográfica del dispositivo.
		2	Longitud geográfica del dispositivo.
		16	Thumbnail o miniatura en hexadecimal del archivo que se encuentra en el mensaje citado (si se genera un archivo a partir del contenido, en un editor de hexadecimal, se creará una imagen visible).
		17	25 Temporalidad aplicada al mensaje citado.
			26 Fecha en la que se aplicó la temporalidad en el chat del mensaje citado en formato UTC Unix Epoch (segundos).

Ilustración 267. Archivo protobuf del campo “ZMETADATA” de la tabla “ZWAMEDIAITEM”

Documentos (archivos enviados como documentos) (7 o 53-1-7):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	7 (documento en chat individual)	1	URL en la que se encuentra el archivo del mensaje citado.
		2	Tipo de MIME del archivo del mensaje citado.
		4	Hash SHA256 del archivo que se encuentra en el mensaje citado.
		5	Tamaño en bytes del archivo del mensaje citado.
		6	Número de páginas del documento citado.
	53-1-7 (documento en chat grupal)	8	Título o nombre del archivo citado.
		10	URL parcial en la que se encuentra el archivo del mensaje citado.
		11	Fecha en la que se transmitió el mensaje citado en formato UTC Unix Epoch (segundos).

Campo	Campo	Campo	Descripción
19 (mensaje citado)	53-1-7 (documento en chat grupal)	16	Thumbnail o miniatura en hexadecimal del archivo que se encuentra en el mensaje citado (si se genera un archivo a partir del contenido, en un editor de hexadecimal, se creará una imagen visible).
		17	25 Temporalidad aplicada al mensaje citado.
			26 Fecha en la que se aplicó la temporalidad en el chat del mensaje citado en formato UTC Unix Epoch (segundos).
		20	Texto del mensaje citado.

Ilustración 268. Archivo protobuf del campo “ZMETADATA” de la tabla “ZWAMEDIAITEM”

Nota de voz o archivo de audio (8), Nota de voz de visualización única (59-1-8):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	8 (nota de voz o archivo de audio)	1	URL en la que se encuentra el archivo del mensaje citado.
		2	Tipo de MIME del archivo del mensaje citado.
		3	Hash SHA256 del archivo que se encuentra en el mensaje citado.
		4	Tamaño en bytes del archivo del mensaje citado.
		5	Duración en segundos del archivo.
		9	URL parcial en la que se encuentra el archivo del mensaje citado.
	59-1-8 (nota de voz de visualización única)	10	Fecha en la que se transmitió el mensaje citado en formato UTC Unix Epoch (segundos).
		17	25 Temporalidad aplicada al mensaje citado.
			26 Fecha en la que se aplicó la temporalidad en el chat del mensaje citado en formato UTC Unix Epoch (segundos).

Ilustración 269. Archivo protobuf del campo “ZMETADATA” de la tabla “ZWAMEDIAITEM”

Vídeo (9), nota de vídeo (66), vídeo de visualización única (55-1-9):

Campo	Campo	Campo	Descripción	
19 (mensaje citado)	9 (vídeo)	1	URL en la que se encuentra el archivo del mensaje citado.	
		2	Tipo de MIME del archivo del mensaje citado.	
		3	Hash SHA256 del archivo que se encuentra en el mensaje citado.	
	66 (nota de vídeo)	4	Tamaño en bytes del archivo del mensaje citado.	
		5	Duración en segundos del archivo.	
		7	Texto del mensaje citado.	
		9	Resolución horizontal (píxeles) imagen o vídeo del mensaje citado.	
	55-1-9 (vídeo de visualización única)	10	Resolución vertical (píxeles) de la imagen o vídeo del mensaje citado.	
		13	URL parcial en la que se encuentra el archivo del mensaje citado.	
		14	Fecha en la que se transmitió el mensaje citado en formato UTC Unix Epoch (segundos).	
		16	Thumbnail o miniatura en hexadecimal del archivo que se encuentra en el mensaje citado (si se genera un archivo a partir del contenido, en un editor de hexadecimal, se creará una imagen visible).	
		17	25	Temporalidad aplicada al mensaje citado.
			26	Fecha en la que se aplicó la temporalidad en el chat del mensaje citado en formato UTC Unix Epoch (segundos).

Ilustración 270. Archivo protobuf del campo “ZMETADATA” de la tabla “ZWAMEDIAITEM”

Ubicación en tiempo real (18):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	18 (ubicación dinámica)	1	Latitud geográfica del dispositivo.
		2	Longitud geográfica del dispositivo.
		6	Texto del mensaje.
		7	Fecha en la que se compartió la ubicación en el mensaje citado en formato UTC Unix Epoch (milisegundos).
		16	Thumbnail o miniatura en hexadecimal del archivo que se encuentra en el mensaje citado (si se genera un archivo a partir del contenido, en un editor de hexadecimal, se creará una imagen visible).
		17	25 Temporalidad aplicada al mensaje citado. 26 Fecha en la que se aplicó la temporalidad en el chat del mensaje citado en formato UTC Unix Epoch (segundos).

Ilustración 271. Archivo protobuf del campo **"ZMETADATA"** de la tabla **"ZWAMEDIAITEM"**

Sticker o avatar (26):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	26 (sticker)	1	URL en la que se encuentra el archivo del mensaje citado.
		2	Hash SHA256 del archivo que se encuentra en el mensaje citado.
		5	Tipo de MIME del archivo del mensaje citado.
		6	Resolución horizontal (píxeles) imagen o vídeo del mensaje citado.
		7	Resolución vertical (píxeles) de la imagen o vídeo del mensaje citado.
		8	URL parcial en la que se encuentra el archivo del mensaje citado.
		9	Tamaño en bytes del sticker citado.

Campo	Campo	Campo	Descripción
19 (mensaje citado)	26 (sticker)	10	Fecha en la que se transmitió el mensaje citado en formato UTC Unix Epoch (segundos).
		17	25 Temporalidad aplicada al mensaje citado.
		18	Fecha en la que se aplicó la temporalidad en el chat del mensaje citado en formato UTC Unix Epoch (milisegundos).

Ilustración 272. Archivo protobuf del campo **“ZMETADATA”** de la tabla **“ZWAMEDIAITEM”**

Encuesta (64):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	64 (encuesta)	2	Texto de la encuesta citada.
		3	1 Opción de respuesta. Se mostrarán tantos campos 3-1 como opciones de respuesta tenga la encuesta.
		5	25 Temporalidad en segundos asignada a la encuesta citada.

Ilustración 273. Archivo protobuf del campo **“ZMETADATA”** de la tabla **“ZWAMEDIAITEM”**

Evento (75):

Campo	Campo	Campo	Descripción
19 (mensaje citado)	64 (evento)	1	25 Temporalidad en segundos asignada al mensaje del evento citada.
		3	Nombre del evento.

Ilustración 274. Archivo protobuf del campo **“ZMETADATA”** de la tabla **“ZWAMEDIAITEM”**

9.9. Mensaje fijado

Dentro de las posibilidades que ofrece WhatsApp se encuentra la de fijar un mensaje al inicio de un chat para facilitar su consulta. El mensaje se mantendrá fijado por un tiempo limitado, debiendo seleccionar entre tres posibilidades, 24 horas, 7 días o 30 días, tiempo tras el cual dejará de estar fijado.

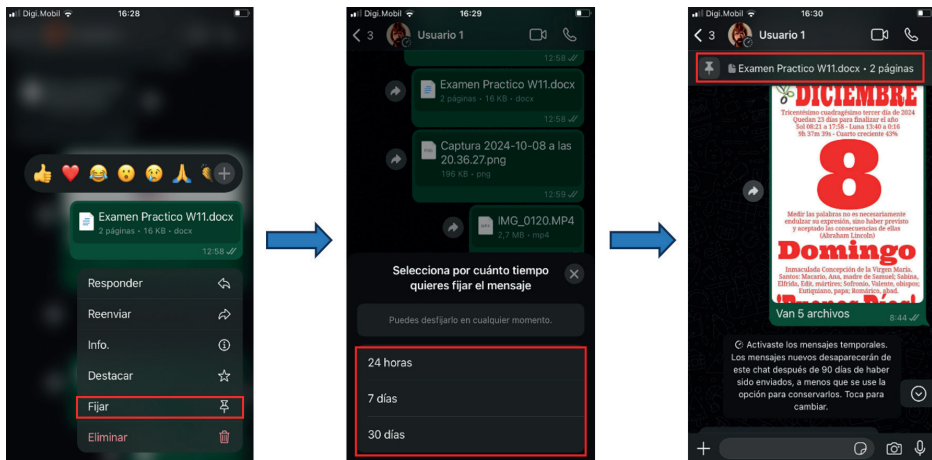


Ilustración 275. "Fijar" un mensaje en la versión de iOS (similar en Android)

Android

Para determinar los mensajes que han sido fijados hay que consultar las tablas **"message"**, **"message_add_on"** y **"message_add_on_pin_in_chat"**, que registran el tiempo que permanecerá fijado el mensaje y la fecha prevista de desanclaje. El dato característico de un mensaje fijado se encuentra en el campo **"message_add_on_type"** de la tabla **"message_add_on"**, cuyo valor será **"79"**.

iOS

El campo **"ZRECEIPTINFO"** de la tabla **"ZWMESSAGEINFO"** contiene el archivo protobuf con información relativa a la característica de fijar un mensaje, entre otras. Es necesario vincular esta tabla con la tabla **"ZWMESSAGE"** a través de campo **"ZMESSAGEINFO"** para obtener la información relevante del mensaje. Retomando el archivo protobuf, el campo que indica, por su mera existencia, que el mensaje está fijado en el chat es el número **"11"**. A continuación, se describe este campo **"11"**, que difiere si el usuario ha fijado el mensaje o un contacto. El resto de los campos que puede contener el archivo protobuf están descritos en el apartado dedicado a las bases de datos de la versión de iOS, concretamente en la tabla **"ZWMESSAGEINFO"**.

Contacto fija el mensaje

Campo	Campo	Campo	Descripción
11 (mensaje fijado)	1 (un contacto fija el mensaje en el chat)	1	Identificador del mensaje que fija el otro mensaje en el chat. Este identificador no está en ningún mensaje de la tabla "ZWMESSAGE" .
		2	Identificador "jid" del contacto que ha fijado el mensaje.
		3	Fecha en la que se fijó el mensaje en el chat en formato UTC Unix Epoch (milisegundos).
		6	Fecha en la que se fijó el mensaje en el chat en formato UTC Unix Epoch (milisegundos).
		7 1	Tiempo en segundos que se mantendrá fijado el mensaje en el chat. Se puede asignar 24 horas (86400), 7 días (604800) o 30 días (2292000).

*Ilustración 276. Archivo protobuf del campo **"ZRECEIPTINFO"** de la tabla **"ZWMESSAGEINFO"***

El usuario de esta cuenta fija el mensaje

Campo	Campo	Campo	Descripción
11 (mensaje fijado)	2 (el usuario de esta cuenta fija el mensaje en el chat)	1	Identificador del mensaje que fija el otro mensaje en el chat. Este identificador no está en ningún mensaje de la tabla "ZWA- MESSAGE ".
		2	Fecha en la que se fijó el mensaje en el chat en formato UTC Unix Epoch (milisegundos).
		3	Fecha en la que se fijó el mensaje en el chat en formato UTC Unix Epoch (milisegundos).
		61	Tiempo en segundos que se mantendrá fijado el mensaje en el chat. Se puede asignar 24 horas (86400), 7 días (604800) o 30 días (2292000).
		7	Fecha en la que se fijó el mensaje en el chat en formato UTC Unix Epoch (milisegundos).

Ilustración 277. Archivo protobuf del campo "ZRECEIPTINFO" de la tabla "ZWAMESSAGEINFO"

9.10. Estados

La funcionalidad "Estados", permite compartir actualizaciones de texto, emojis, notas de voz y archivos de imagen, vídeo o GIF con los contactos seleccionados en opciones de privacidad. La duración máxima de la nota de voz o del vídeo es de 90 segundos.

Una vez **transcurridas 24 horas** desde que se publica un estado (por el usuario o sus contactos), se elimina automáticamente. Esto tiene consecuencias drásticas; se elimina toda la información referente a los estados de la base de datos, así como los archivos asociados.

Cuando se publica un estado, es posible realizar una **mención privada** a uno o varios contactos mediante el carácter "@". Los contactos mencionados reciben una **notificación directa en sus respectivos chats**,

informándoles de que han sido citados en dicho estado. Al ser una mención privada, **únicamente el contacto señalado recibe la notificación.**

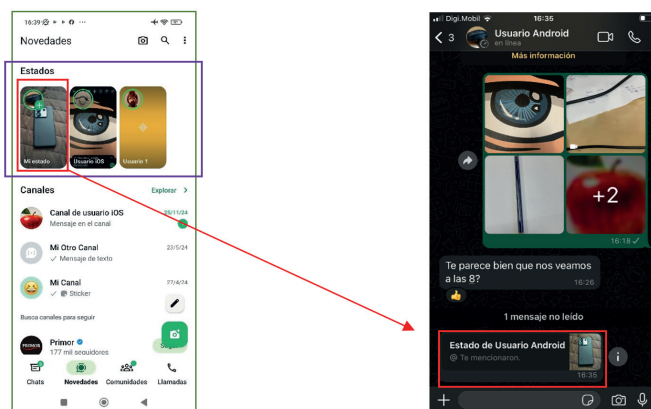


Ilustración 278. "Estados" en Android (izq.) y mención del usuario en el "Estado" de un contacto en iOS (dcha.)

Android

Por cada una de las actualizaciones de estado se grabará un registro en las tablas "**message**" y "**status_message_info**", y si el estado es un archivo multimedia o nota de voz, se registrará dicha información en la tabla "**message_media**". La tabla "**status**" aporta información del estado de un contacto o del propio usuario de esta cuenta.

Cuando el usuario añade un archivo multimedia a su estado, dicho archivo se guardará en una de las rutas habituales que dispone la aplicación para estos ficheros:

- /data/media/0/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Images/Sent
- /data/media/0/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Video/Sent
- /data/media/0/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Animated GIFs/Sent
- /data/media/0/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Voice Notes

Los estados compartidos por el usuario de la cuenta analizada son fácilmente localizables entre los registros de la tabla **"message"**, ya que el campo **"participant_hash"** contendrá un valor, a diferencia del resto de mensajes en los cuales este campo se encontrará vacío.

Cuando el usuario recibe estados de alguno de sus contactos, los archivos se descargan en la ruta:

- **/data/media/0/Android/media/com.whatsapp/WhatsApp/Media/.Statuses**

Esta carpeta está oculta para el usuario, debido a que el sistema operativo la reconoce con esta característica al comenzar el nombre de la carpeta por un punto ".". Aunque el usuario navegue con un explorador de archivos, no la verá si el explorador oculta elementos ocultos.

Cuando el usuario menciona privadamente en su estado a un contacto o viceversa, además del registro que se genera en la tabla **"message"** por la transmisión del estado, se crea un registro por el mensaje de notificación que le llega al participante mencionado, con el valor **"103"** en el campo **"message_type"**. Además, se generará un registro en la tabla **"message_quoted"**.

iOS

Cada contacto, al igual que el usuario de esta cuenta, tiene su propia sesión de chat para registrar los mensajes enviados a sus respectivos estados. La tabla que registra las sesiones de chat **"ZWACHATSESSION"**, contendrá en el campo **"ZCONTACTJID"** el valor "status@broadcast" en el caso del usuario de esta cuenta, y el número de teléfono del contacto junto con el dominio "@status" en el caso de los estados publicados por los contactos:

ZCONTACTJID	ZETAG	ZLASTMESSAGE TEXT	ZPARTNERNAME
status@broadcast		YlQznRERUUSOS0xQ0JBLTQ3Q0YtOTNDQy05RTUxOUNEN0JBODhgF0NBQjY4ZQwOEI1QjZBQkI4M...	
34c[redacted]@status		YlQznRERUUSOS0xQ0JBLTQ3Q0YtOTNDQy05RTUxOUNEN0JBODJAAQA=	Usuario 1

Ilustración 279. Tabla **"ZWACHATSESSION"**

En la tabla **"ZWMESSAGE"** se registran los mensajes publicados en los estados. Cuando el usuario de esta cuenta envía un mensaje a su estado, se registrará en el campo **"ZTOJID"** el valor **"status@broadcast"** y el campo **"ZSPOTLIGHTSTATUS"** mostrará el valor **"3"**.

En el caso de que sea un contacto el que envíe un mensaje a su propio estado y lo reciba el usuario de esta cuenta, se registrará en el campo **"ZFROMJID"** el mismo valor **"status@broadcast"** y el campo **"ZSPOTLIGHTSTATUS"** mostrará el valor **"2"**.

En el campo **"ZFILTEREDRECIPIENTCOUNT"** de la tabla **"ZWMESSAGE"** se registra el número de usuarios que han recibido el estado del usuario, y en el campo **"ZCHILDMESSAGESPLAYEDCOUNT"** se almacena el número de contactos que han visualizado el estado (si ambos tienen activado la confirmación de lectura).

La información sobre los contactos que han recibido el estado del usuario de esta cuenta se almacena en un archivo protobuf en el campo **"ZRECEIPTINFO"** de la tabla **"ZWMESSAGEINFO"**.

Campo	Campo	Descripción
2 (tantos campos como contactos sean receptores del mensaje publicado por el usuario en su estado)	1	Número de teléfono del contacto que ha recibido el mensaje precedido del número "81" y finalizado con el carácter "f" . Ejemplo: 8134633456456f
	7	Nombre del contacto con el que está grabado en la agenda del usuario. Si se trata del mismo usuario, será referido como "Tú" .
3		Fecha del envío del mensaje en formato UTC Unix Epoch (segundos).

*Ilustración 280. Archivo protobuf del campo **"ZRECEIPTINFO"** de la tabla **"ZWMESSAGEINFO"***

Cuando el usuario menciona privadamente en su estado a un contacto o viceversa, además del registro que se genera en la **"ZWMESSAGE"** por la transmisión del estado, se crea un registro por el mensaje de notificación que le llega al participante mencionado, con el valor **"68"** en el campo **"ZMESSAGETYPE"**. Como cualquier otro tipo de mensaje citado, es conveniente analizar el archivo protobuf del campo **"ZMETADATA"** de la tabla **"ZWAMEDIAITEM"**, cuya interpretación se ha expuesto en el apartado 9.8 *CITAR UN MENSAJE*.

10. Eliminación de mensajes (Android – iOS)

La aplicación WhatsApp en su compromiso con la privacidad permite la eliminación de mensajes de los chats en los que participa el usuario. Atendiendo a las características del borrado de mensajes se pueden clasificar de dos formas diferentes:

- **Programado** en base al transcurso de un tiempo predeterminado desde su emisión (mensajes temporales) o tras la visualización del mensaje por el receptor (mensaje de visualización única).
- **Instantáneo** (eliminación de mensaje, vaciado de chat o eliminación de chat).

10.1. Mensajes temporales

Es una funcionalidad que proporciona mayor privacidad al chat. Consiste en la elección del tiempo que un mensaje permanecerá en el chat, tras el cual se borrará definitivamente. Las opciones de temporalidad elegibles son de 24 horas, 7 días o 90 días, y se pueden adoptar tanto en chats individuales como grupales y comunidades, haciendo efecto sobre los mensajes transmitidos después de activar esta preferencia.

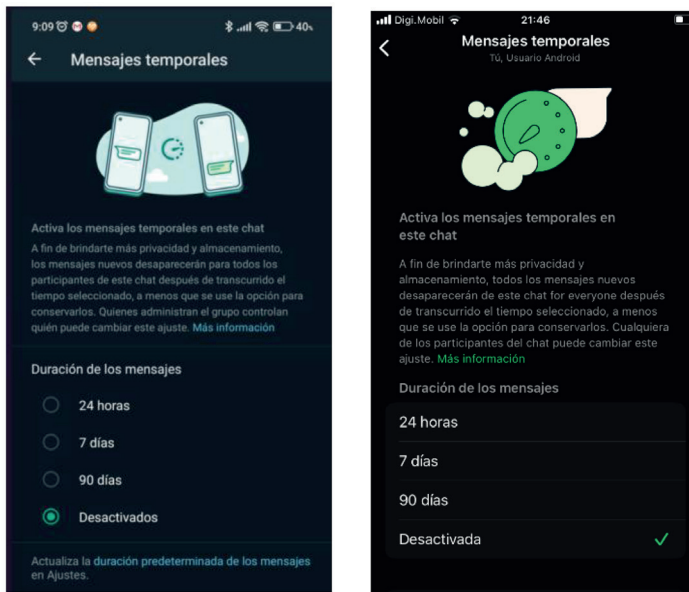


Ilustración 281. Opciones de duración de mensajes temporales en la versión de Android (izq.) e iOS (dcha.)

Cualquiera de los usuarios del chat puede aplicar esta opción a la comunicación, la cual afectará a todos los interlocutores del chat. La temporalidad de los mensajes será comunicada por un mensaje del sistema a todos los participantes.

Existen dos formas de activar los mensajes temporales:

1. Desde las opciones generales de la cuenta de WhatsApp se puede seleccionar que todos los chats de nueva creación cuenten con mensajes temporales. Esta opción tendrá efecto en los chats individuales que se inicien con fecha posterior a la selección, siendo indiferente si es el emisor o el receptor del mensaje quien tiene activada la temporalidad a los nuevos chats. Por motivos de privacidad, siempre tiene preferencia la temporalidad de un usuario sobre la no temporalidad de otro, independientemente de quién de los dos haya iniciado la conversación. Si ambos participantes la tienen activada, prevalece el tiempo asignado por el que inicia el chat. En este sentido, a los chats que estaban activos (iniciados) en la

bandeja de chats antes de seleccionar la temporalidad de mensajes no les afectará esta característica.

Un chat nuevo se puede crear porque no se ha mantenido nunca una conversación con el otro participante o porque eliminó el chat y se vuelve a crear cuando recibe o envía un mensaje. Pero en este último caso, para uno de los participantes será un chat nuevo (porque eliminó previamente en su cuenta el chat) y para el otro participante sólo será la continuación de un chat existente. Si el participante cuyo chat se crea de nuevo tiene dispuesto la temporalidad en los chats nuevos, cuando reciba o envíe un mensaje al otro participante, automáticamente se aplicará esa temporalidad al chat.

En los chats grupales, el creador decide si tendrá temporalidad el chat o no, en el momento de generarlo, siendo irrelevante el tipo de temporalidad que tengan asignada los demás participantes.

2. Otra alternativa es activar la temporalidad de los mensajes intercambiados en un chat activo que no tenía esta característica seleccionada cuando se inició. Tendrá efecto en los mensajes posteriores a la elección de esta opción. En este caso, la opción de mensajes temporales se encuentra en las preferencias del chat.

En cualquier momento uno de los participantes en el chat individual o grupal (si tiene los permisos) puede cambiar el tiempo que debe transcurrir hasta la eliminación de los mensajes o desactivar la temporalidad. En todos los casos, afectará a los mensajes transmitidos con posterioridad al cambio.

Cuando un mensaje temporal es citado en otro mensaje, el mensaje citado permanecerá en el chat hasta que se cumpla el tiempo establecido para el segundo mensaje. De la misma forma, si se reenvía el mensaje a un chat en el que no tiene activado los mensajes temporales, el mensaje reenviado no se eliminará.

Android

Cuando se tiene activada la *temporalidad aplicada a nuevos chats*, se registra la información en el archivo de preferencias que se encuentra localizado en la ruta `/data/data/com.whatsapp/shared_prefs/disappearing_mode_prefs.xml`:

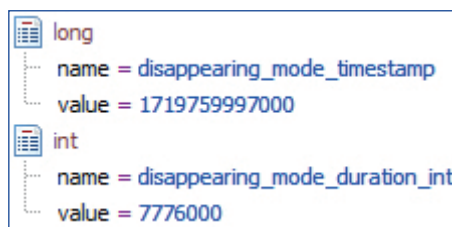


Ilustración 282. Archivo *disappearing_mode_prefs.xml*

El campo **"disappearing_mode_timestamp"** contiene la fecha UTC en formato Unix Epoch (milisegundos) en la que se activó o cambió la temporalidad en los mensajes de los nuevos chats.

El campo **"disappearing_mode_duration_int"** contiene el valor en segundos del tiempo que permanecerá el mensaje en el chat hasta que se elimine automáticamente. Las opciones son **86400** (24 horas), **604800** (7 días) o **7776000** (90 días).

Para determinar si un chat tiene aplicada la temporalidad de sus mensajes, independientemente del método utilizado para activar o desactivar esta característica hay que analizar la base de datos **"msgstore.db"**, donde se puede determinar numerosos extremos de los explicados consultando la tabla **"chat"**:

_id	jid_row_id	ephemeral_expiration	ephemeral_setting_timestamp
94	125	7776000	29/04/2024 17:42:02
97	59	7776000	18/07/2024 10:16:14
160	14	7776000	08/12/2024 17:26:06
238	33	0	08/12/2024 17:31:06
242	281	86400	25/01/2025 12:31:51

Ilustración 283. Tabla *chat*

A partir del valor del campo "**jid_row_id**" se determinan los participantes; el valor del campo "**ephemeral_expiration**" es el tiempo en segundos que transcurrirá hasta que se elimine el mensaje y el valor del campo "**ephemeral_setting_timestamp**" es la fecha UTC en formato Unix Epoch (milisegundos) en la que se aplicó esta opción. En el caso que exista un valor distinto a "**0**" en el campo "**ephemeral_setting_timestamp**" y el valor del campo "**ephemeral_expiration**" sea "**0**", significa que ese chat tuvo activado los mensajes temporales y en esa fecha se desactivaron.

La tabla "**message_ephemeral_setting**" registra el último mensaje que se ha generado en un chat por aplicar/cambiar la opción de mensaje temporal en dicho chat. Aunque pueda parecer una duplicación de los datos registrados en la tabla anterior, realmente amplía la información:

message_row_id	setting_duration	setting_reason
37	86400	0
116	604800	0
123	604800	1
922	86400	2
928	604800	1

*Ilustración 284. Tabla **message_ephemeral_setting***

A partir del valor de "**message_row_id**" se determina el registro del mensaje en la tabla "**message**" al corresponderse con el valor del campo "**_id**". El valor "**setting_duration**" es el tiempo en segundos que transcurrirá hasta que se elimine el mensaje y los valores asignados al campo "**setting_reason**" pueden ser de gran interés para discriminar quién ha elegido la opción de temporalidad. Si el valor es "**0**", uno de los participantes ha activado manualmente en este chat la temporalidad en chats individuales. Si el valor es "**1**", el usuario de este dispositivo tiene predeterminado (automatizado) la temporalidad de los mensajes en sus chats nuevos. Si el valor es "**2**", es el otro participante quien tiene esta opción predeterminada (automatizada) para los chats nuevos. En el caso de grupos el valor del campo "**setting_reason**" es siempre "0" y no aporta esa información extra.

Confirmando la información proporcionada por esta tabla, se puede recurrir a la tabla "**message**", en la cual se generará un registro cuando

un usuario de un chat individual activa/desactiva/cambia la duración de mensajes temporales manualmente desde las opciones del chat. El registro tendrá el campo **"message_type"** el valor **"36"**.

En la tabla **"message_ephemeral"** podemos ver los mensajes que tienen temporalidad. Se mantendrán en esta tabla hasta el momento en el que finalmente sean eliminados del chat, una vez transcurra su vida programada marcada en el campo **"expire_timestamp"**, en formato UTC Unix Epoch (milisegundos)

message_row_id	duration	expire_timestamp	keep_in_chat
2313	604800	05/12/2024 16:32:27	1
2341	7776000	04/03/2025 08:29:21	1
2345	7776000	04/03/2025 08:40:03	1
3818	7776000	23/10/2025 13:41:33	0
3957	7776000	25/11/2025 11:00:14	0

Ilustración 285. Tabla **message_ephemeral**

No se borrará en la fecha prevista si se ha utilizado la opción "conservar" el mensaje, que se refleja en el campo **"keep_in_chat"** con el valor **"1"** y que se explica más adelante.

iOS

La información que proporciona la aplicación en la versión en iOS se basa principalmente en los datos registrados en el campo **"ZLASTMESSAGE-TEXT"** de la tabla **"ZWCHATSESSION"**. Como se ha explicado en el apartado 5.3.3 **ZWCHATSESSION**, el campo **"ZLASTMESSAGE-TEXT"** contiene un archivo protobuf codificado en Base64.

Tras decodificar el archivo, se puede determinar la temporalidad que tienen asignados actualmente los mensajes, y el momento en el que se estableció esa temporalidad. También se registran los cambios de elección de la duración de la temporalidad o su activación/desactivación:

Campo	Campo	Descripción
2		Temporalidad aplicada actualmente a los mensajes de este chat en segundos. Si no aparece este campo, actualmente no tienen temporalidad los mensajes.
3		Fecha en la que se estableció la temporalidad aplicada actualmente a los mensajes del chat en formato UTC Unix Epoch (segundos).
5 (tantos campos como diferentes temporalidades se hayan asignado a este chat. El primer campo será la temporalidad aplicada más antigua)	1	Temporalidad aplicada a los mensajes en segundos anteriormente.

Ilustración 286. Archivo protobuf del campo **"ZLASTMESSAGETEXT"** de la tabla **"ZWCHATSESSION"**

Cuando interesa averiguar si un mensaje concreto tiene asignado temporalidad, se debe examinar el campo **"ZMESSAGEERRORSTATUS"** de la tabla **"ZWMESSAGE"**. Este campo contiene la fecha en la que está programada la eliminación del mensaje en formato UTC OS X Epoch (cuando el valor es **"0"** significa que no tiene temporalidad aplicada y un valor negativo es un mensaje "conservado").

ZMESSAGEERRORSTATUS	ZMESSAGEDATE	ZSENTDATE	ZTEXT
01/01/2026 18:54:18	03/10/2025 18:54:18	03/10/2025 18:54:18	Hola 🗨️

Ilustración 287. Tabla **ZWMESSAGE**
(mensaje con una temporalidad de 90 días)

10.1.1. Mensajes conservados

Si se quiere preservar un mensaje temporal que va a ser eliminado al cumplirse su plazo, se puede utilizar la opción "conservar". El mensaje se 🗨️ guardará para todos los usuarios del chat, aunque el emisor del

mensaje tiene la opción de revocar esa conservación para impedir que nadie lo conserve posteriormente.

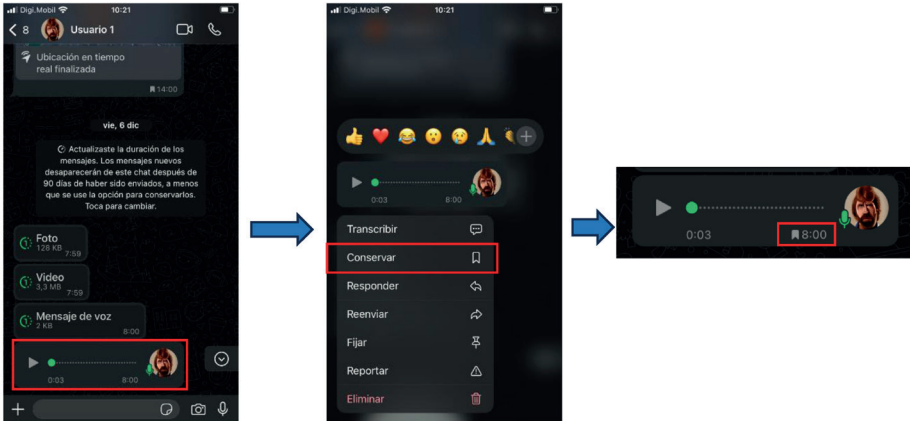


Ilustración 288. Selección de un mensaje temporal para conservarlo en el chat en la versión de iOS

Android

La información de la conservación de un mensaje se registra de forma sencilla. El campo "**keep_in_chat**" de la tabla "**message_ephemeral**" se registra con el valor "**1**" en caso de que el mensaje temporal al que se hace referencia en el campo "**message_row_id**" se conserva y se suspenda su eliminación tras cumplirse la temporalidad que tenía asignado:

message_row_id	duration	expire_timestamp	keep_in_chat	ephemeral_trigger	ephemeral_initiated_by_me
622	7776000	08/07/2024 21:20:51	1	1	1

Tabla **message_ephemeral**

_id	chat_row_id	from_me	key_id	timestamp	received_timestamp	receipt_server_timestamp	message_type
622	26	1	EF0B57D844DC0296817D5447C8B49542	09/04/2024 21:20:50	09/04/2024 21:20:51	09/04/2024 21:20:51	1

Tabla **message**

Ilustración 289. Relación entre tablas en los mensajes conservados en Android

Para ampliar la información sobre quién ha optado por conservar el mensaje, se debe consultar las tablas **"message_add_on"** y **"message_add_on_keep_in_chat"**.

iOS

Para comprobar si un mensaje temporal se conservará como resultado de seleccionar la opción "conservar", primero se debe consultar el valor del campo **"ZMESSAGEERRORSTATUS"** de la tabla **"ZWMESSAGE"**. Si el valor es *negativo*, se trata de un mensaje conservado. Transformando el valor en positivo se obtiene la fecha en la que estaba prevista la eliminación del mensaje, antes de ser conservado, en formato UTC OS X Epoch.

Partiendo del mensaje que interesa en la tabla **"ZWMESSAGE"**, se examina el valor del campo **"ZMEDIAITEM"**, el cual se vincula con el mismo valor del campo **"Z_PK"** de la tabla **"ZWAMEDIAITEM"**. En esta última tabla se encuentra la información que determina la conservación del mensaje (campo **"ZMETADATA"**).

En dicho campo se almacena un archivo protobuf con la información indicada. Una vez decodificado el archivo desde la información en hexadecimal, la presencia del campo **"66"** significa que el mensaje temporal será conservado:

Z_PK	ZISFROMME	ZMESSAGEERRORSTATUS	ZMESSAGEDATE	ZSENTDATE	ZMEDIAITEM	ZMESSAGEINFO	ZTEXT
557	1	-750494115	06/10/2024 6:35:14	06/10/2024 6:35:14	438	526	Texto grupo

Tabla **ZWMESSAGE**

Z_PK	ZMETADATA
438	è ò\$ 3Y/EA C àóú-2 1 120363337863331165@qq.us 3A6860317F6D489D67E9 Óúú-2 € ÓDÓNÍ*±

Tabla **ZWAMEDIAITEM**

00000000:	E8 01 80 F5 24 89 02 00	00 80 91 33 59 C6 41 92	è.è0\$%...è'3YEA'
00000010:	04 43 08 E0 F3 FC AD A6	32 12 31 0A 17 31 32 30	.C.àóúú2.1..120
00000020:	33 36 33 33 33 37 38 36	33 33 33 31 31 36 35 40	363337863331165è
00000030:	67 2E 75 73 10 01 1A 14	33 41 36 38 36 30 33 31	g.us....3A686031
00000040:	37 46 36 44 34 38 39 44	36 37 45 39 18 D2 FA FC	7F6D489D67E9.Óúú
00000050:	AD A6 32 20 01 A2 04 20	D6 44 D6 4E CF 2A B1 7D	Ú2 .€. ÓDÓNÍ*±
00000060:	09 C8 28 08 9E 48 88 C2	8B F1 07 E3 CF AC 17 FF	.È(.ÈH'À<À.ÀI-.y
00000070:	EB 19 5B D3 B4 34 20 D3	C8 06 01 90 07 00 A8 07	è.[Ó'4 ÓÈ..Ú..'
00000080:	01 B0 07 00 E8 07 01		.°.è...

Archivo protobuf en hexadecimal

Ilustración 290. Relación entre las diferentes tablas en los mensajes conservados en iOS

Archivo protobuf del campo “ZMETADATA” de la Tabla “ZWAMEDIAITEM” decodificado

Campos comunes:

Campo	Campo	Descripción
4		URL parcial en la que se encuentra el archivo del mensaje.
29		Temporalidad aplicada al mensaje.
33		Fecha en la que se envió el mensaje en formato UTC OS X Epoch.
35		Fecha en la que se cambió la temporalidad de los mensajes en el chat en formato UTC Unix Epoch (segundos)
47	3	Resolución horizontal (píxeles) del thumbnail señalado en el campo “47-8”.
	4	Resolución vertical (píxeles) del thumbnail señalado en el campo “47-8”.
	6	Hash SHA256 del thumbnail señalado en el campo “47-8”.
	8	Ruta parcial en el dispositivo en el que se encuentra el thumbnail del archivo pdf.

Ilustración 291. Archivo protobuf del campo “ZMETADATA” de la tabla “ZWAMEDIAITEM”

Campo “66” determina que se trata de un mensaje conservado:

Campo	Campo	Campo	Descripción
66 (mensaje conservado)	1		Fecha en la que se optó por conservar el mensaje en formato UTC Unix Epoch (mili-segundos).
	2	1	Identificador “jid” del contacto o del grupo del chat en el que se ha conservado el mensaje.
		2	Quién ha optado por conservar el mensaje: 0 : un contacto. 1 : el usuario de esta cuenta.
		3	Identificación del mensaje generado al conservar el mensaje
	3		Fecha en la que se optó por conservar el mensaje en formato UTC Unix Epoch (mili-segundos)

Ilustración 292. Archivo protobuf del campo “ZMETADATA” de la tabla “ZWAMEDIAITEM”

10.2. Mensajes de visualización única

Es una funcionalidad que permite enviar imágenes, vídeos o notas de voz que solo se pueden abrir en una ocasión, necesariamente en el dispositivo principal (no es posible su reproducción en dispositivos vinculados).

Una vez abierto, el receptor puede reproducir el archivo (vídeos o notas de voz) tantas veces como desee, pero tras el cierre del archivo, se elimina de la aplicación y, por tanto, del dispositivo. El emisor nunca podrá visualizar en el chat de WhatsApp el archivo que ha enviado, ni siquiera antes de que el receptor reproduzca el archivo que ha recibido.

Cuando se envía un mensaje de visualización única, solamente se recibirá la confirmación de que ha sido "Abierto" por el receptor, si ambos usuarios tienen activada la confirmación de lectura en su configuración de privacidad.

Esta funcionalidad no admite que se reenvíe, guarde o se realicen capturas de pantalla del archivo de visualización única. Tampoco se guardará o mostrará en la sección de fotos o galería del destinatario.

Otra de las diferencias más significativas respecto a un envío normal es que, si se genera la imagen o el vídeo con la aplicación, solo se grabará el archivo comprimido enviado y *el archivo original no se almacenará en el dispositivo*. Por el contrario, si se envía una imagen o vídeo adjuntándolo desde la galería o el explorador de archivos, el fichero original a partir del cual se genera el enviado (comprimido) permanecerá en su ubicación original.

Android

Lo cierto es que el archivo recibido por el destinatario se podrá descargar (automática o manualmente, dependiendo de las opciones elegidas por el usuario) en la carpeta ubicada en la ruta **/data/data/com.whatsapp/files/ViewOnce/**, hasta que se visualice a través de la aplicación, momento en el que se borrará. Si no se reproduce el archivo

en el transcurso de 14 días desde que se recibió, se eliminará automáticamente. A dicha carpeta no puede acceder un usuario normal a través del explorador de archivos al encontrarse en una ubicación protegida. Únicamente se podría evadir esta protección si el usuario obtuviera permisos de administrador (root).

Conviene recordar que los archivos de visualización única recibidos tienen una nomenclatura propia, iniciada por IMG (imagen), VID (vídeos) o AUD (notas de voz), seguido por ocho caracteres y la extensión del tipo de archivo. Ejemplos de nombres de este tipo de ficheros:

- **IMG-lqn09qmy.jpg** (imagen de visualización única)
- **VID-lqmzz7hh.mp4** (vídeo de visualización única)
- **AUD-lqn05ag5k.opus** (nota de voz de visualización única)

Los archivos enviados de visualización única se almacenan temporalmente en el dispositivo hasta que son entregados al servidor, momento en el que son eliminados.

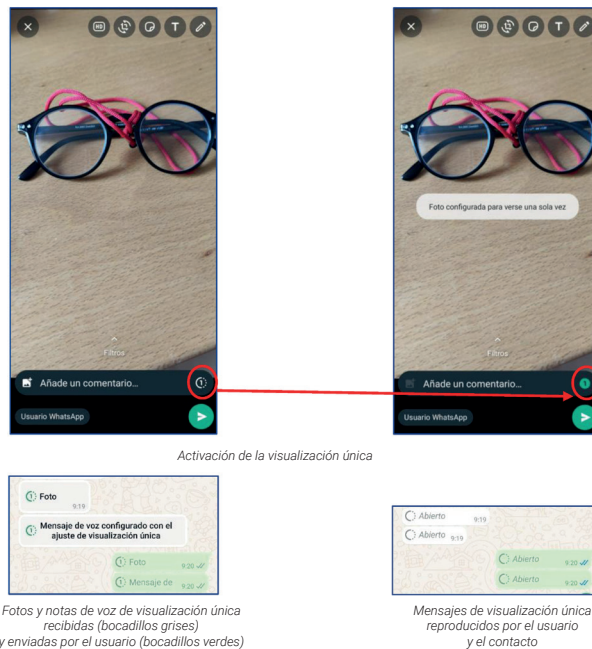


Ilustración 293. Envío, recepción y reproducción de archivos de visualización única en Android (similar en iOS)

Análisis de los mensajes de visualización única:

Los pasos que se pueden seguir para el análisis de este tipo de mensajes serán los mismos en el teléfono que envía y en el que recibe el mensaje, si bien los resultados serán más limitados en este último dispositivo.

Aunque el archivo se elimina automáticamente, no ocurre lo mismo con toda la información que registra la aplicación sobre el mensaje transmitido, tanto en el emisor como en el receptor. La aplicación WhatsApp siempre que se envía/recibe un archivo de vídeo o imagen genera una miniatura o thumbnail que se guarda en la base de datos "**msgstore.db**", cuya finalidad es mostrarla en el chat como representación en baja calidad del archivo original. En este caso, la aplicación no se comporta de forma diferente, genera el thumbnail que se almacena en la base de datos, pero con la diferencia de que no se muestra a ninguno de los usuarios (ni el emisor ni receptor). Lógicamente, en las notas de voz de visualización única no se genera thumbnail y no se dispondrá de ese indicio de la transmisión del mensaje.

Por lo tanto, cuando se realiza un análisis y se observa la existencia de un thumbnail y que el archivo transmitido no se encuentra en el dispositivo, es un indicio (no determinante) de que pudiera tratarse de un mensaje de visualización única.

Si se quiere profundizar en este tipo de mensaje, hay que enfocarse en las bases de datos, concretamente dos tablas son fundamentales para interpretar estos mensajes:

La primera, es la tabla "**message**", específicamente las filas o registros en las que se muestre el campo "**message_type**" con los valores "**42**" (imagen de visualización única), "**43**" (vídeo de visualización única) o "**82**" (nota de voz de visualización única), de las que se podrá obtener el campo "**_id**" así como el chat al que pertenece, quién lo envió y las marcas de tiempo, etc.

La segunda tabla que hay que consultar es "**message_view_once_media**", la cual sólo recoge datos de este tipo de mensajes, conectando los mensajes de la tabla "**message**" de visualización única y el estado

de visualización del mensaje. Si ambos participantes tienen activada la confirmación de lectura, se podrá confirmar si el contacto que ha recibido el archivo de visualización única enviado desde esta cuenta ha sido reproducido, no ha sido reproducido o ha sido eliminado por haber transcurrido 14 días sin ser reproducido.

Tal y como se ha indicado en el apartado 8.3 *CONFIRMACIÓN DE RECEPCIÓN Y LECTURA DE MENSAJES*, se observa que en los mensajes recibidos por el usuario de la cuenta no resulta relevante que la opción de confirmación de lectura esté activada. Esto se debe a que en el campo "**status**" de la tabla "**message**" queda igualmente registrada la reproducción de este tipo de archivo, reflejándose con el valor "**status**" = "**10**".

Por el contrario, en los mensajes enviados en chats individuales, resulta imprescindible que **ambos usuarios** tengan habilitada la confirmación de lectura, pues únicamente en ese caso el emisor podrá recibir el indicador de "**Abierto**" cuando el contacto abra el mensaje.

En tal caso, será posible consultar la tabla "**message**" para ver el estado del envío en el campo "**status**", y la tabla "**receipt_user**" para verificar la recepción del mensaje, la apertura del chat y la reproducción del mensaje. Cuando es un grupo, las opciones de confirmación de lectura no le afectan y se comporta como si todos los componentes la tuvieran activada. Por ello, el estado de recepción, apertura del chat y reproducción de un mensaje de visualización única enviado por el usuario de la cuenta analizada podrá consultarse en las mismas tablas.

A partir del campo "**_id**" de la tabla "**message**" se conecta por un lado a la tabla "**message_media**", obteniendo un dato tan relevante como es el hash SHA-256 (codificado en Base64) del archivo transmitido, y por otro, se obtiene el **thumbnail** de la tabla "**message_thumbnail**".

Cuando el emisor del mensaje toma una imagen o un vídeo de la galería del teléfono, el archivo enviado será una copia generada y comprimida por WhatsApp. El archivo que se borrará será la copia generada, siendo probable que se pueda localizar el original en el dispositivo emisor, a no ser que el usuario lo elimine manualmente.

Se deberían comparar los hashes obtenidos de la tabla "**message_media**" contra todos los archivos del dispositivo. Es importante recordar que, si el archivo ha sido comprimido por la aplicación para enviarlo, tendremos dos hashes con los que enfrenar los hashes de los archivos del dispositivo, el hash del archivo comprimido y enviado, registrado en el campo "**file_hash**", y el hash del archivo original del cual se obtuvo el comprimido registrado en el campo "**original_file_hash**".

En el caso de que el archivo de imagen o vídeo se *genere* a través de la aplicación WhatsApp (seleccionando la cámara del dispositivo) y se envíe con la configuración de visualización única, **no se guardará el archivo original en los correspondientes subdirectorios** en los que se almacenarían si no se hiciera uso de dicha configuración. De la misma forma, el archivo enviado será eliminado del dispositivo en el momento en que sea entregado al servidor.

Se puede verificar si el archivo se generó con la aplicación, examinando que el valor del campo "**origin**" de la tabla "**message**" es "**1**".

Si la imagen o vídeo enviado *no se ha generado* a través de la cámara de la aplicación, el archivo comprimido transmitido será eliminado, pero el original continuará en la ubicación en la que se encontraba inicialmente, siendo posible por medio del hash registrado en la tabla "**message_media**" localizar este archivo original.

En las notas de voz de visualización única, una vez recibidas y reproducidas serán eliminadas del dispositivo receptor, sin posibilidad de recuperación del archivo. Sin embargo, en el caso de que la nota de voz haya sido transcrita por la funcionalidad de WhatsApp, el **texto se mantendrá** en el campo "**raw_transcription_text**" de la tabla "**message_media**".

Es probable que, en un futuro cercano, los desarrolladores eviten que se almacenen las transcripciones de notas de voz de visualización única. Esta implementación ya se ha observado en las versiones de iOS, en las cuales también se grababan pero que en la última analizada (2.25.33.77) no registra esta información.

iOS

Debido a su propio funcionamiento interno, el sistema operativo iOS es más opaco; cuando se implementa un plus de privacidad a determinados mensajes complica mucho su análisis. Los archivos adjuntados en mensajes de visualización única no se obtienen en una extracción de tipo iTunes Backup, aun cuando se encuentren en el dispositivo.

El único caso que se ha concretado en el estudio en el que se puede recuperar un mensaje de visualización única, es cuando el usuario de la cuenta analizada recibe un archivo, se descarga en el dispositivo (dependiendo de la configuración que tenga aplicada se efectuará automática o manualmente) y no lo reproduce. La ventana de tiempo para la adquisición del archivo es de 14 días desde que fue enviado, tras los cuales la aplicación lo eliminará automáticamente.

La ruta en la que se almacena el archivo es la misma que para el resto de los archivos multimedia en una extracción FFS (Full File System):

- /private/var/mobile/Containers/Shared/AppGroup/<GUID>/Message/Media/34xxxxxxxx@s.whatsapp.net/

Cuando un archivo de visualización única es una imagen o un vídeo, se genera una miniatura (thumbnail) con el mismo nombre que el archivo original, pero con la extensión ".thumb". Para localizar el mensaje de visualización única en la tabla "**ZWAMESSAGE**", se debe buscar el campo "**ZMESSAGETYPE**" con los valores "**38**" (imagen de visualización única) o "**39**" (vídeo de visualización única). Este mensaje se vincula con la tabla "**ZWAMEDIAITEM**", que contiene en el campo "**ZXMPPTHUMB-PATH**" la ruta parcial y el nombre de la miniatura.

En contraposición a las técnicas de análisis que son utilizadas en la versión de Android, el único hash que se registra en el envío del mensaje es el del archivo comprimido y transmitido por la aplicación. Aunque el archivo original se encontrase en la aplicación "FOTOS" u otra ubicación previa a ese tratamiento, los hashes de ambos archivos serán completamente diferentes y no se podrán vincular.

10.3. Mensajes eliminados por el usuario

La aplicación permite el borrado de los diferentes tipos de mensajes por parte del usuario. Hay varias opciones en función del tipo de chat y el tiempo transcurrido desde el envío del mensaje:

10.3.1. Eliminar para mí

El usuario elimina un mensaje que ha enviado/recibido, pero se conserva en el chat del otro usuario (chat individual) u otros usuarios (chat grupal). El mensaje se eliminará sin dejar rastro en el chat.

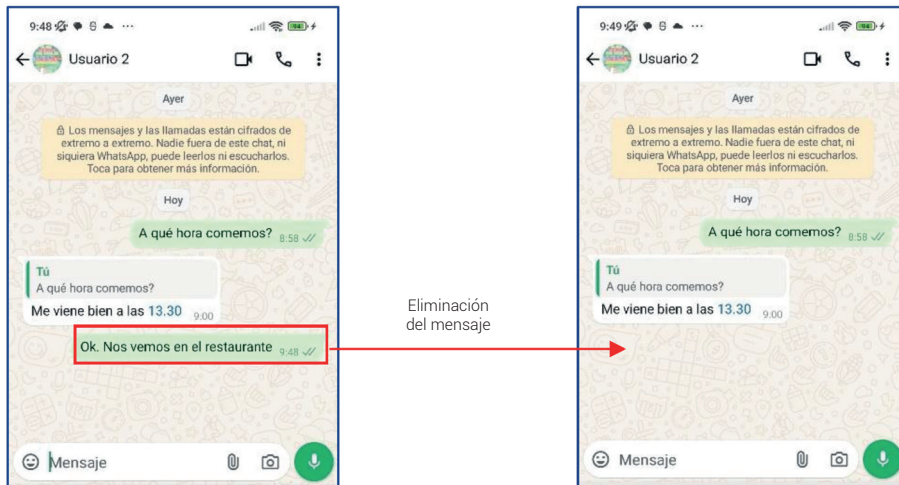


Ilustración 294. Eliminación de un mensaje por el usuario en Android (similar en iOS)

Android

Si el mensaje se eliminó pocos días después de su transmisión, se registrará el momento de su borrado en los logs, pero únicamente aportará información de que se eliminó un mensaje de un chat con un contacto

(4 últimos dígitos de su identificador "jid") o un grupo (identificador "jid" completo):

```
2025-11-21 07:18:15.614 LL_I W [1633:WhatsApp Worker #169] UserActions/userActionDeleteMessages 1
2025-11-21 07:18:15.615 LL_I W [1633:WhatsApp Worker #169] UserActions/userActionDeleteMessages
messagesToDeleteIncludingAssociatedMessages=1
2025-11-21 07:18:19.662 LL_I W [395:androidx.work-1] msgstore/countmessagestodelete/count: 1
2025-11-21 07:18:19.669 LL_I W [395:androidx.work-1] msgstore/countmessagestodelete/count: 1
2025-11-21 07:18:19.682 LL_I W [395:androidx.work-1] msgstore/deletemedia/batch/files/timer/stop: 0
2025-11-21 07:18:19.682 LL_I W [395:androidx.work-1] CoreMessageStore/deletemedia/batch/files
2295@s.whatsapp.net timeSpent:0
2025-11-21 07:18:19.716 LL_I W [395:androidx.work-1] msgstore/deleteMessageThumbnailsFor-jid/0
2025-11-21 07:18:19.716 LL_I W [395:androidx.work-1] msgstore/deletemsgs/batches/timer/elapsed: 69
2025-11-21 07:18:19.734 LL_I W [395:androidx.work-1] msgstore/deletemsgs/batches/timer/stop: 86
2025-11-21 07:18:19.734 LL_I W [395:androidx.work-1] CoreMessageStore/deletemsgs/batches 2295@s.
whatsapp.net haveMessagesToDelete:false timeSpent:86 currentMessages:1 totalMessages:1
2025-11-21 07:18:19.735 LL_I W [395:androidx.work-1] msgstore/deletemsgs/unmark jid:2295@s.what-
sapp.net
```

Cuando se selecciona eliminar un mensaje, aparece una ventana emergente con la posibilidad de eliminar "los archivos multimedia recibidos". En realidad, si se selecciona esta opción que viene activada por defecto, se pueden eliminar tanto los archivos recibidos como los enviados seleccionados:

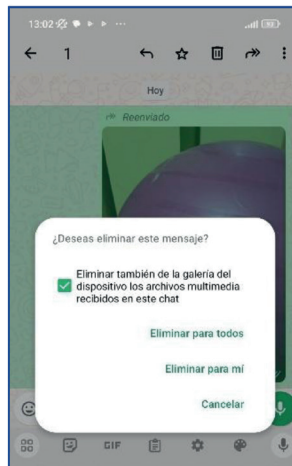


Ilustración 295. Opciones de eliminación del archivo multimedia en Android

Hay que recordar que cuando se envía una fotografía o un vídeo, generalmente procede de un archivo obtenido desde la aplicación o de

la galería, y es comprimido por la aplicación. Con esta opción de borrado de archivos se elimina el enviado, pero no el archivo origen sin comprimir. Cuando se opta por no eliminar el archivo, se mantendrá en su ubicación, pero no habrá información en las bases de datos de esa transmisión, por lo que no será posible determinar cuál fue su destino.

iOS

El registro de la eliminación de un mensaje mediante la opción “eliminar para mí” queda almacenado por un tiempo limitado en los logs de la aplicación, concretamente en la ruta /private/var/mobile/Containers/Shared/AppGroup/<GUI>/Logs/WhatsApp_2/whatsapp-AAAA-MM-DD-hh-mm-ss-mss-WhatsApp-xxx.log. Se puede determinar la eliminación por la orden “deleteMessageForMe”, además aporta información del identificador parcial “jid” del chat en el que se transmitió el mensaje “2387@s.whatsapp.net” en este ejemplo y la identificación del mensaje “3A63BFC06BFBA9D4590D”:

```
12:33:36.224 [ 3394] [service ] [F] LL_A app-state-store/savePendingMutations state: Optional(WAAppS-
tateSync.AppStatePendingMutationEntityState), actions: deleteMessageForMe
12:33:36.239 [ 3394] [NSManaged...c680] [F] LL_A storage//save/success [AppStateStore in 0.01s with
changes]
12:33:36.241 [ 4527] [message-delete] [F] LL_A message/report-token-store/reporting-tag deleting repor-
ting tags for message IDs: <*****2387@s.whatsapp.net>-3A63BFC06BFBA9D4590D_1_0
12:33:36.251 [ 3433] [searchengine ] [F] LL_E searchengine/delete/error [count: 1, first: 0]
12:33:36.260 [ 3394] [main-thread ] [F] LL_W chatsessions//controller-will-change-content _selectedChat-
SessionBeforeFetchedResultsControllerUpdate: *****2387@s.whatsapp.net
12:33:36.264 [ 3394] [main-thread ] [F] LL_W chatsessions/can-edit-row/index path not found: <NSIndex-
Path: 0x859071635c65963a> {length = 2, path = 4 - 0}
12:33:36.329 [ 3394] [main-thread ] [F] LL_A chatsessions//will-begin-updating-tableview
12:33:36.333 [ 3394] [main-thread ] [F] LL_A chatsessions//controller-did-change-content
12:33:36.341 [ 3394] [main-thread ] [F] LL_W chatsessions/can-edit-row/index path not found: <NSIndex-
Path: 0x859071635c65963a> {length = 2, path = 4 - 0}
12:33:36.348 [ 3394] [main-thread ] [F] LL_A chatsessions//did-finish-updating-tableview
12:33:36.352 [ 3394] [main-thread ] [F] LL_A chatsessions//controller-did-change-content reset _selecte-
dChatSessionBeforeFetchedResultsControllerUpdate to nil
12:33:36.355 [ 3551] [message-delete] [F] LL_A message/report-token-store/reporting-token deleting re-
porting tokens for message IDs: <*****2387@s.whatsapp.net>-3A63BFC06BFBA9D4590D_1_0
```

Cuando los mensajes que contienen archivos multimedia son borrados, el archivo también es eliminado de los directorios de WhatsApp. Sin embargo, si el usuario tiene activada la opción de “Guardar en Fotos”, quedará una copia del archivo eliminado en el dispositivo, pero sin ninguna opción de vincularlo con el mensaje en el que se transmitió.

10.3.2. Eliminar para todos

El emisor de un mensaje puede eliminarlo de su propio chat y del chat del otro usuario (chat individual) u otros usuarios (chat grupal). Esta acción debe realizarse dentro de las **60 horas** posteriores al envío del mensaje. Los mensajes eliminados se reemplazarán con los textos del sistema:

- **“Eliminaste este mensaje.”** en el chat del emisor del mensaje, siendo quien lo elimina.
- **“Se eliminó este mensaje.”** en el chat o chats del/os otro/s participante/s.

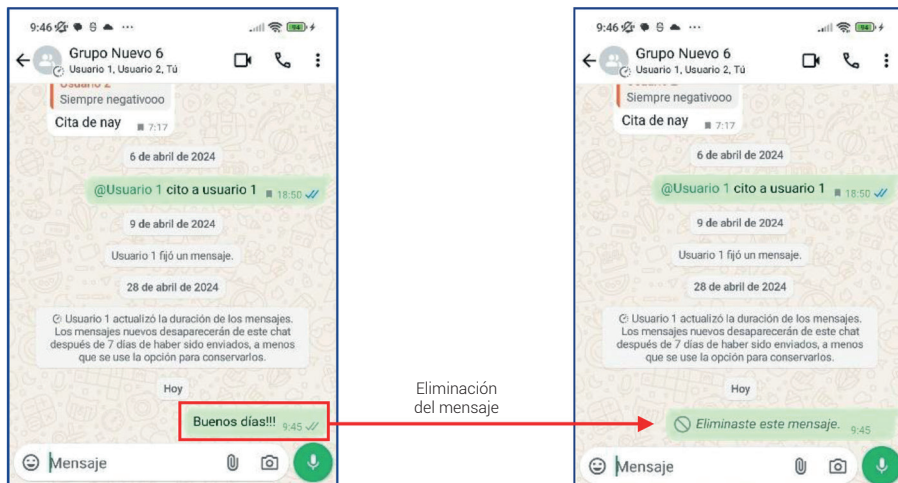


Ilustración 296. Eliminación de un mensaje “para todos” por el emisor.

Android

Cuando el emisor del mensaje lo elimina **“para todos”**, se producen tres cambios relevantes en la base de datos **“msgstore.db”**.

En primer lugar, en la tabla **“message”** se actualiza el tipo de mensaje: el valor inicial del campo **“message_type”** se sustituye por **“15”**, y el identificador del mensaje (**“key_id”**) es reemplazado por uno nuevo.

En segundo lugar, se crea un registro en la tabla **"message_revoked"**, donde se almacena el mismo número de fila del mensaje (correspondencia entre los campos **"_id"** y **"message_row_id"**), el identificador anterior del mensaje (**"revoked_key_id"**) y la fecha en la que se efectuó la eliminación, en formato UTC Unix Epoch.

Finalmente, si el mensaje contenía un archivo multimedia, se elimina todo rastro del archivo en la base de datos **"msgstore.db"**, suprimiéndose tanto su referencia en la tabla **"message_media"** como cualquier otro dato asociado.

_id	chat_row_id	from_me	key_id	timestamp	received_timestamp	message_type
5032	322	1	ACE2BA8B9A82F735BABFF6C017EFD5A0	30/11/2025 19:13:11	01/01/1970 00:00:00	15

Tabla **message** (después de la eliminación del mensaje)

message_row_id	revoked_key_id	admin_jid_row_id	revoke_timestamp
5032	ACA453B896D3081C4C2FBBAA1A4C698C		30/11/2025 19:13:24

Tabla **message_revoked** (después de la eliminación del mensaje)

Ilustración 297. Relación entre tablas en la eliminación de un mensaje en Android

Se puede obtener información del fichero de logs siempre que la eliminación del mensaje se haya producido dentro del periodo para el que existen registros auditables (aproximadamente, los últimos cuatro días).

Si el envío del mensaje tuvo lugar dentro del intervalo cubierto por alguno de los archivos de logs, será posible recuperar datos relevantes a partir del valor del campo **"revoked_key_id"** (en este ejemplo, **ACA453B896D3081C4C2FBBAA1A4C698C**) registrado en la tabla **"message_revoked"**.

En este caso, a las 19:13 horas del 30/11/2025, el usuario envió (is-FromMe=true) un mensaje al contacto con identificador "jid" parcial (chatJid=2295@s.whatsapp.net). El mensaje quedó almacenado en la tabla **"message"** con el número de registro (row_id=5032).

El contenido del mensaje es una imagen, circunstancia que puede determinarse por el tipo de mensaje, cuyo valor es **"1"** (messagesViewModel/addsent/skipped/fmsg/status:1/**type:1**/rmt-src). Asimismo, el nombre asignado a la imagen en este dispositivo es **IMG-20251130-WA0001**:

```
2025-11-30 19:13:11.619 LL_I W [2:main] messagesViewModel/observer/beforemsgadded/add ACA453B-896D3081C4C2FBBAA1A4C698C 1
2025-11-30 19:13:11.634 LL_I W [691:WhatsApp Worker #62] SendMediaMessageManager/attachMedia-JobCallbacks
2025-11-30 19:13:11.638 LL_I W [310:AsyncCommitThread] MainMessageStore/insertMainMessageRow/inserted/updated rowId=5032 key=Key(id=ACA453B896D3081C4C2FBBAA1A4C698C, isFromMe=true, chatJid=2295@s.whatsapp.net) chatRowId=null
2025-11-30 19:13:11.721 LL_I W [2:main] messagesViewModel/addsent/skipped/fmsg/status:1/type:1/rmt-src:null Key(id=ACA453B896D3081C4C2FBBAA1A4C698C, isFromMe=true, chatJid=2255@s.whatsapp.net) adapter-count:61 las-row-id:4959 cur-row-id:5032
2025-11-30 19:13:13.166 LL_I W [452:WhatsApp Worker #56] BaseMediaFileUtils/readablefilename IMG-20251130-WA0001
```

Del valor del campo **"key_id"** (ACE2BA8B9A82F735BABFF6C017EFD5A0) de la tabla **"message"** obtienen los datos de la eliminación del mensaje, en este caso, el archivo enviado (msgstore/edit/revoke send deleteMedia=true):

```
2025-11-30 19:13:24.686 LL_I W [310:AsyncCommitThread] msgstore/edit/revoke send deleteMedia=true key=Key(id=ACE2BA8B9A82F735BABFF6C017EFD5A0, isFromMe=true, chatJid=2295@s.whatsapp.net)
2025-11-30 19:13:24.724 LL_I W [310:AsyncCommitThread] MainMessageStore/insertMainMessageRow/inserted/updated rowId=5032 key=Key(id=ACE2BA8B9A82F735BABFF6C017EFD5A0, isFromMe=true, chatJid=2295@s.whatsapp.net) chatRowId=322
```

Cuando el mensaje enviado por el usuario contiene una imagen o vídeo, tendrá la opción de eliminarlo de su propia galería, con las repercusiones explicadas en el apartado 10.3.1 *Eliminar para mí*.

Si un contacto que ha enviado un mensaje con un archivo al usuario de esta cuenta lo elimina "para todos", la única copia del archivo almacenada en el directorio **/data/media/0/Android/media/com.whatsapp/WhatsApp/Media/** se eliminará.

iOS

La eliminación “para todos” de un mensaje produce cambios significativos en la tabla **“ZWMESSAGE”** de la base de datos **“ChatStorage.sqlite”**. El tipo de mensaje inicial (campo **“ZMESSAGETYPE”**) cambiará del que tuviera inicialmente a presentar el valor **“14”**. No es el único cambio que se produce en la tabla, el identificador del mensaje del campo **“ZSTANZAID”** cambia al haberse creado un mensaje que notifica la eliminación de mensaje de todos los participantes.

Z_PK	ZMESSAGETYPE	ZMESSAGEINFO	ZMESSAGEDATE	ZSENTDATE	ZSTANZAID
621	1		12/10/2024 8:15:38	12/10/2024 8:15:38	3A716FB7C26CB58D96E7

Tabla **ZWMESSAGE** (antes de la eliminación del mensaje)

Z_PK	ZMESSAGETYPE	ZMESSAGEINFO	ZMESSAGEDATE	ZSENTDATE	ZSTANZAID
621	14	642	12/10/2024 8:15:38	12/10/2024 12:03:31	3ACA085E32F6944CDE54

Tabla **ZWMESSAGE** (después de la eliminación del mensaje)

Ilustración 298. Relación entre tablas en la eliminación de un mensaje en iOS

Cuando es el usuario de esta cuenta quien elimina el mensaje “para todos”, se podrá determinar la fecha en la que se eliminó el mensaje; en caso de que la eliminación la haya realizado un contacto no se podrá obtener esa información. El primer lugar donde se puede localizar estos datos es en el campo **“ZSENTDATE”** de la tabla **“ZWMESSAGE”**. Este dato se duplica en el campo **“ZRECEIPTINFO”** de la tabla **“ZWMESSAGEINFO”** asociado al mensaje. Es un archivo protobuf, que una vez decodificado, en el campo **3** registra la fecha de eliminación en formato UTC Unix Epoch (segundos).

Z_PK	Z_ENT	Z_OPT	ZMESSAGE	ZRECEIPTINFO
642	11	4	621	4d O J R R 4g%r8 R É©

Archivo protobuf que se debe decodificar

Ilustración 299. Tabla **ZWMESSAGEINFO**

En el campo **“ZTITLE”** de la tabla **“ZWAMEDIAITEM”** vinculada al mensaje, se encuentra el valor del identificador del mensaje original, antes de ser eliminado.

Este tipo de eliminación del mensaje se registra con la orden “revoke” en los logs, señalando el cambio de identificador del mensaje inicial al mensaje de comunicación del borrado a los participantes. También registra el chat en el que se ha producido estos cambios y los dispositivos vinculados (de existir) en los que se eliminará también el mensaje:

```
21:03:23.322 [ 4660] [main-thread ] [F] LL_A revoke [3AD1A2DDE9306F73F783 -> 3A9DDFBFEAC7E-26066FD]
21:03:23.327 [ 35370] [message-delete] [F] LL_A message/report-token-store/reporting-token deleting reporting tokens for message IDs: <*****2295@s.whatsapp.net>_3AD1A2DDE9306F73F783_1_0
21:03:23.334 [ 34905] [searchengine ] [F] LL_A searchengine/delete [count: 1, first: 244]
21:03:23.342 [ 4660] [main-thread ] [F] LL_W chatsessions//controller-will-change-content _selectedChat-SessionBeforeFetchedResultsControllerUpdate: <*****2295@s.whatsapp.net>
21:03:23.343 [ 4660] [main-thread ] [F] LL_A chatsessions//will-begin-updating-tableview
21:03:23.343 [ 4660] [main-thread ] [F] LL_A chatsessions/did-change-object/jid:*****2295@s.whatsapp.net/last-message-stanzaId:3A9DDFBFEAC7E26066FD/last-message-objectID:0xa61d1aef8875f639<x-coredata://6B0BA179-DD9A-4FD4-8A6B-476C65BAD0A3/WAMessage/p555>/last-message-date:2025-11-30 21:02:23 +0000
21:03:23.424 [ 4660] [main-thread ] [F] LL_A messaging/request: OutboxItemEncryptionRequest {
  LL_A chat_jid: <*****2255@s.whatsapp.net>,
  LL_A stanza_id: 3A9DDFBFEAC7E26066FD,
  LL_A retry: n/a,
  LL_A directed: false,
  LL_A phash: n/a,
  LL_A recipients (6): [<*****8364:33@s.whatsapp.net>: v24, <*****8364:34@s.whatsapp.net>: v25, <*****2295:34@s.whatsapp.net>: v6, <*****2295:0@s.whatsapp.net>: v5, <*****8364:35@s.whatsapp.net>: v26, <*****8364:32@s.whatsapp.net>: v23]
```

La forma de registrar la eliminación de un mensaje “para todos” en los logs en sistemas iOS depende del miembro que elimina el mensaje, si es el usuario de esta cuenta (este apartado) o es un contacto el que elimina el mensaje (el ejemplo sería similar al apartado 10.3.3 *Eliminar para todos como administrador*).

En el borrado de mensajes que contienen archivos multimedia, los archivos también son eliminados de los directorios de WhatsApp. Sin embargo, si el usuario tiene activada la opción de “Guardar en Fotos”, quedará una copia de la fotografía o vídeo eliminado en el dispositivo, pero sin ninguna opción de vincularlo con el mensaje en el que se transmitió.

10.3.3. Eliminar para todos (como administrador)

En chats grupales, solo un administrador podrá borrar todo tipo de mensajes enviados por otros participantes, siempre que no haya transcurrido

más de 60 horas desde que se envió el mensaje. Como en el resto de los casos, tendrá la misma opción de borrarlo de su propia galería en el caso de que sea un archivo. Los mensajes eliminados se reemplazarán con el texto:

“Un admin., [nombre del admin.], eliminó este mensaje.”

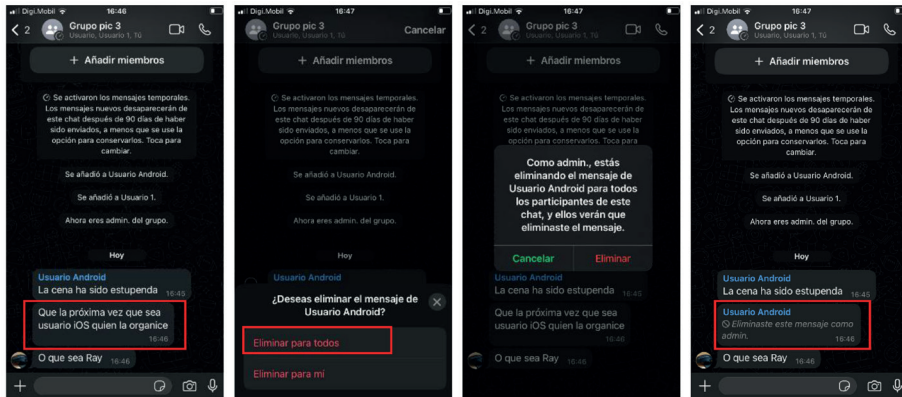


Ilustración 300. Eliminación de un mensaje “para todos” por el administrador del grupo en iOS (similar en Android)

Android

Cuando un administrador de un grupo elimina para todos, un mensaje enviado por otro participante, se generan tres cambios reseñables en la base de datos “**msgstore.db**”. El primero es en la tabla “**message**”, en el que se producirá un cambio del tipo de mensaje (“**message_type**”) del que tuviera inicialmente al valor “**64**” y también cambiará el identificador “**key_id**” del mensaje por uno nuevo. En segundo lugar, se creará un registro en la tabla “**message_revoked**” con el número de fila o registro del mensaje de la tabla “**message**” (campo “**message_row_id**”), el identificador del mensaje (“**key_id**”) previo a ser eliminado y la fecha de eliminación del mensaje en formato UTC Unix Epoch. Por último, en el caso de que se haya transmitido un archivo adjunto, se elimina todo rastro de éste de la base de datos “**msgstore.db**”.

El administrador que ha eliminado el mensaje es grabado en el campo **"admin_jid_row_id"** de la tabla **"message_revoked"**. En este ejemplo se debería consultar la fila o registro "3" de la tabla **"jid"** para determinar el identificador "jid" del administrador.

_id	chat_row_id	from_me	key_id	timestamp	received_timestamp	message_type
5033	224	0	AC4683C7D21FFE7C0F1FE1A80E093EA6	30/11/2025 19:16:45	30/11/2025 19:16:45	64

Tabla **message** (después de la eliminación del mensaje)

message_row_id	revoked_key_id	admin_jid_row_id	revoke_timestamp
5033	AC31B3AF1406534B1C501706C0BC8EE4	3	30/11/2025 19:18:06

Tabla **message_revoked** (después de la eliminación del mensaje)

_id	user	server	agent	device	type	raw_string
3	346	s.whatsapp.net	0	0	0	346@s.whatsapp.net

Tabla **jid**

Ilustración 301. Relación entre tablas en la eliminación de un mensaje por un admin. en Android

Como en el apartado anterior, se puede obtener información del fichero de logs, en el caso de que el borrado se haya producido en el periodo de tiempo que hay registros auditable (últimos 4 días aproximadamente).

Tomando como ejemplo los datos expuestos en la imagen anterior, si el envío del mensaje se produjo en el periodo de tiempo registrado por alguno de los archivos de logs, se obtendrá información del mensaje enviado a partir del valor campo **"revoked_key_id"** (AC31B3AF1406534B1C501706C0BC8EE4).

A las 19:16 horas del día 30/11/2025 el usuario recibió (isFromme=false) un mensaje en el grupo con jid (chatJid=363372714331345@g.us) que fue enviado por el contacto con jid parcial (participant=2295@s.whatsapp.net). El mensaje se grabó en el registro de la tabla "message" número (row_id=5033).

El mensaje contiene una fotografía, como se puede determinar por el tipo de mensaje es "1" (new=fmsg/status:0/**type:1**/rmt-src), aportando el hash SHA-256 codificado en Base64 parcialmente (message.mediaHash=*****qwqg=). También se registran datos de la descarga del archivo como es el tamaño en bytes,

el tipo de mime y el nombre del archivo con el que se almacenó en el dispositivo:

```
2025-11-30 19:16:46.160 LLI W [285:XmppMessageRouter] MessageForMeXmppHandler/
onMessageForMe key=Key(id=AC31B3AF1406534B1C501706C0BC8EE4, isFromMe=false, chatJi-
d=363372714331345@g.us)/onMessageForMe participant=2295@s.whatsapp.net t=1764530205000
now=1764530206159 retry=0 offline=null edit=0 stanzaAttrshash=831574516
2025-11-30 19:16:46.256 LLI W [697:SignalExecutor] MainMessageStore/insertMainMessageRow/
inserted/updated rowId=5033 key=Key(id=AC31B3AF1406534B1C501706C0BC8EE4, isFromMe=false, cha-
tJid=363372714331345@g.us) chatRowId=null
2025-11-30 19:16:46.261 LLI W [697:SignalExecutor] MessageSecretInserterPostProcessor/processing/
row_id=5033,hasSecret=true
2025-11-30 19:16:46.281 LLI W [762:WhatsApp Worker #95] MediaDownloadManager/queue-
Download auto download Key(id=AC31B3AF1406534B1C501706C0BC8EE4, isFromMe=false,
chatJid=363372714331345@g.us), message.mediaHash=*****qwg=
2025-11-30 19:16:46.426 LLI W [293:Notifications] messagenotification/ new=fmsg/status:0/type:1/
rmt-src:2255@s.whatsapp.net Key(id=AC31B3AF1406534B1C501706C0BC8EE4, isFromMe=false, chatJi-
d=363372714331345@g.us) isNotificationSilent=false
2025-11-30 19:17:49.777 LLI W [884:WhatsApp Worker #116] MediaDownload/call/download/mediaHas-
h=*****qwg= 2025-11-30 19:17:49.969 LLI W [884:WhatsApp Worker
#116] WhatsAppRust/libwaimageoperations_rs:jpeg::topology: Input file length = 56440 bytes
```

Del valor del campo **“key_id”** de la tabla **“message”** (AC4683C7D-21FFE7C0F1FE1A80E093EA6) se obtiene la información relativa a la eliminación del mensaje. A las 19:18 horas del día 30/11/2025, el participante con identificador “lid” parcial 8186@lid (SignalSenderKeyStore/getSenderKey 363372714331345@g.us::8186) ha eliminado el mensaje (msgstore/edit/revoke) que había sido enviado por el contacto con “jid” parcial parcial (2295@s.whatsapp.net) al grupo (chatJid=363372714331345@g.us).

Aunque puedan aparecer numerosas líneas de registro indicando que el mensaje de eliminación no ha sido generado por el usuario de esta cuenta (isFromMe=false), es el “lid” parcial consignado en el registro (SignalSenderKeyStore/getSenderKey) el que ofrece el dato correcto. En este ejemplo, el usuario de esta cuenta - que es administrador del grupo - ha eliminado el mensaje. Aunque el log no muestra su identificador completo, se conoce que su **“lid”** es 262074978558186@lid.

La confirmación de que un mensaje ha sido eliminado por un administrador del grupo (que no fue el emisor el mensaje) se encuentra en el valor del tipo de mensaje que pasa a ser **“64”** (messagesViewModel/ adreceived/skip/fmsg/status:0/type:64):


```
2025-11-30 19:18:06.622 LL_I W [310:AsyncCommitThread] msgstore/edit/revoke recv key=Key(id=AC4683C7D21FFE7C0F1FE1A80E093EA6, isFromMe=false, chatJid=363372714331345@g.us)
2025-11-30 19:18:06.678 LL_I W [310:AsyncCommitThread] MainMessageStore/insertMainMessageRow/inserted/updated rowId=5033 key=Key(id=AC4683C7D21FFE7C0F1FE1A80E093EA6, isFromMe=false, chatJid=363372714331345@g.us) chatRowId=224
2025-11-30 19:18:06.705 LL_I W [2:main] messagesViewModel/addressReceived/skip/fmsg/status:0/type:64/rmt-src:2295@s.whatsapp.net Key(id=AC4683C7D21FFE7C0F1FE1A80E093EA6, isFromMe=false, chatJid=363372714331345@g.us)
2025-11-30 19:18:07.139 LL_I W [310:AsyncCommitThread] ParticipantUserStore/getGroupParticipantsWithCaching 363372714331345@g.us size: 2
2025-11-30 19:18:07.141 LL_I W [694:JobRunner #2] SignalSenderKeyStore/getSenderKey 363372714331345@g.us::8186:0:1:REGULAR & translated = 363372714331345@g.us::8186:0:1:REGULAR
2025-11-30 19:18:07.142 LL_I W [694:JobRunner #2] ParticipantUserStore/markParticipantsAsHavingSenderKey [5945:0@lid, 5945:34@lid, 8186:41@lid]
2025-11-30 19:18:07.142 LL_I W [694:JobRunner #2] ParticipantUserStore/getGroupParticipantsWithCaching 363372714331345@g.us size: 2
2025-11-30 19:18:07.142 LL_I W [694:JobRunner #2] ParticipantDeviceStore/markDevicesAsHavingSenderKey 363372714331345@g.us [5945:0@lid, 5945:34@lid, 8186:41@lid]
2025-11-30 19:18:07.145 LL_I W [694:JobRunner #2] SendE2EMessageJob/ e2e message send job finished result = true ; id=AC4683C7D21FFE7C0F1FE1A80E093EA6; jid=363372714331345@g.us; participant=null; retryCount=0; targetDevices=[]; groupParticipantHash=2:3df2rLJo; includeSenderKeysInMessage=true; useOneOneEncryptionOnPHashMismatch=true; forceSenderKeyDistribution=false; useParticipantUserHash=true; persistentId=1
```

Cuando es el usuario de la cuenta analizada quien elimina el mensaje como administrador y el mensaje contiene una imagen o vídeo, tendrá la opción de eliminarlo de su propia galería, con las consecuencias explicadas en el apartado *10.3.1 Eliminar para mí*.

Si un administrador de un grupo elimina un mensaje que contenía un archivo enviado por cualquier contacto (excepto el usuario de esta cuenta), la única copia del archivo almacenada en el directorio **/data/media/0/Android/media/com.whatsapp/WhatsApp/Media/** de usuario de esta cuenta se eliminará.

iOS

Un administrador de un grupo tiene la capacidad de eliminar un mensaje para todos los participantes, aunque no haya enviado dicho mensaje. Los cambios que se producen en la tabla **"ZWAMESSAGE"** de la base de datos **"ChatStorage.sqlite"** son muy similares a los explicados en el anterior tipo de borrado. El tipo de mensaje inicial (**"ZMESSAGETYPE"**) pasaría a mostrar el valor **"14"**. No es el único cambio que se produce en la tabla, el identificador del mensaje del campo **"ZSTANZAID"** cambia al haberse creado un mensaje que notifica la eliminación de mensaje de todos los participantes. El identificador "jid" del administrador que

ha eliminado el mensaje se muestra en el campo **"ZTEXT"** (la diferencia entre un mensaje eliminado "para todos" por un administrador que no lo ha enviado, con uno eliminado por el propio emisor del mensaje, es que en el segundo caso campo **"ZTEXT"** se encuentra vacío).

Z_PK	ZMESSAGEID	ZMESSAGEDATE	ZSENTDATE	ZSTANZID	ZTEXT
639	3	12/10/2024 8:35:52	12/10/2024 8:35:52	3AFCBD3E3FF63722B334	

Tabla **ZWAMESSAGE** (antes de la eliminación del mensaje)

Z_PK	ZMESSAGEID	ZMEDIAITEM	ZMESSAGEDATE	ZSENTDATE	ZSTANZID	ZTEXT
639	14	533	12/10/2024 8:35:52	12/10/2024 8:35:52	C334D667395BA3601F9BA44C24B1B260	34 [redacted]@s.whatsapp.net

Tabla **ZWAMESSAGE** (después de la eliminación del mensaje)

Ilustración 302. Relación entre tablas en la eliminación de un mensaje por un admin. en iOS

En el campo **"ZTITLE"** de la tabla **"ZWAMEDIAITEM"** vinculada al mensaje, se encuentra el valor del identificador del mensaje original, antes de ser eliminado.

Z_PK	ZTITLE
533	3AFCBD3E3FF63722B334

*Ilustración 303. Tabla **ZWAMEDIAITEM***

En este ejemplo no se almacena información de la fecha del borrado porque el mensaje lo eliminó un administrador que no era el usuario de esta cuenta. Pero en el caso de que el administrador que elimina un mensaje sea el usuario de esta cuenta, se podrá localizar esa información en el campo **"ZSENTDATE"** de la tabla **"ZWAMESSAGE"**. Este dato se duplica en el campo **"ZRECEIPTINFO"** de la tabla **"ZWAMESAGEINFO"** asociado al mensaje. Es un archivo protobuf, que una vez decodificado, en el campo 3 registra la fecha del borrado en formato UTC Unix Epoch (segundos).

Cuando no ha transcurrido más de unos pocos días y se extrae la información del archivo de logs, se observará que el borrado se registra con la orden "revoke", añadiendo el identificador "jid" parcial del grupo (*****2951@g.us). El mensaje inicial procede del usuario de esta cuenta ("fromMe: 1") y señala el cambio de identificador del

mensaje inicial (3AFCBD3E3FF63722B334) al identificador del mensaje de comunicación del borrado a los participantes (C334D667395BA-3601F9BA44C24B1B260).

Además del identificador del mensaje, puede aparecer también el identificador **"lid"** parcial del emisor que ejecuta la acción. En este ejemplo (C334D667395BA3601F9BA44C24B1B260_0_<****5945@lid), el identificador **"lid"** corresponde a un contacto (contrastado en la base de datos **"LID.sqlite"**).

Dado que el mensaje fue enviado por el usuario de esta cuenta al grupo, y que la eliminación ha sido ejecutada por un tercero, la única posibilidad coherente es que el borrado haya sido realizado por un **administrador del grupo**:

```
13:10:06.442 [ 8172] [main-thread ] [F] LL_A connection/revoke/incoming/received-revocation-signal/
[WAMessageID: remote: <*****2951@g.us>, participant: (null), fromMe: 1, stanza: 3AFCBD3E-
3FF63722B334]/C334D667395BA3601F9BA44C24B1B260
13:10:06.443 [ 8172] [main-thread ] [F] LL_A connection/revoke/incoming/3AFCBD3E3FF63722B334/
C334D667395BA3601F9BA44C24B1B260
13:10:06.447 [ 8172] [NSManaged...2a40] [F] LL_A storage//save/success [KVStore-BackedUpKeyValue.
sqlite in 0.00s with changes]
13:10:06.448 [ 8172] [main-thread ] [F] LL_W messaging//fail/missing send task
13:10:06.448 [ 8172] [main-thread ] [F] LL_A revoke [3AFCBD3E3FF63722B334 -> C334D667395BA-
3601F9BA44C24B1B260]
13:10:06.448 [ 356410] [searchengine ] [F] LL_E searchengine/delete/error [count: 1, first: 0]
13:10:06.573 [ 356497] [message-delete] [F] LL_A message/report-token-store/reporting-tag
deleting reporting tags for message IDs: <*****2951@g.us>_ C334D667395BA3601F9BA44C-
24B1B260_0_<*****5945@lid >
13:10:06.575 [ 356497] [message-delete] [F] LL_A message/report-token-store/reporting-token
deleting reporting tokens for message IDs: <*****2951@g.us>_ C334D667395BA3601F9BA44C-
24B1B260_0_<*****5945@lid >
```

La forma de registrar la eliminación de un mensaje "para todos" en los logs en sistemas iOS depende del miembro que elimina el mensaje, si es el usuario de esta cuenta (el ejemplo sería similar al apartado 10.3.2 *Eliminar para todos*) o es un contacto el que elimina el mensaje (este apartado).

Cuando los mensajes que contienen archivos multimedia, el archivo también es eliminado de los directorios de WhatsApp. Sin embargo, si el usuario tiene activada la opción de "Guardar en Fotos", quedará una copia de la fotografía o vídeo eliminado en el dispositivo, pero sin ninguna opción de vincularlo con el mensaje en el que se transmitió.

10.4. Vaciado de chat

Funcionalidad que permite eliminar todos los mensajes de un chat, ofreciendo la opción de eliminar de la galería del dispositivo los archivos multimedia del chat. Tras el vaciado, el chat (sin mensajes) continuará apareciendo en la lista de chats.

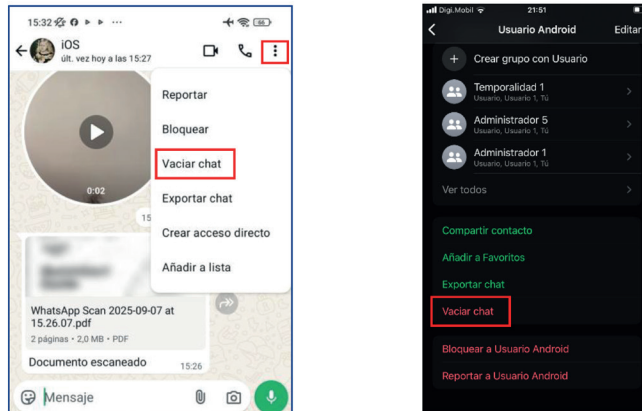


Ilustración 304. "Vaciar chat" en la versión Android (izq.) e iOS (dcha.)

Android

El vaciado de un chat en el dispositivo queda registrado en el fichero dedicado al almacenamiento de logs denominado "whatsapp.log", pero con la limitación temporal que supone que se almacenen los cambios de los últimos 4 días aproximadamente. El primer indicio del vaciado es el registro de la eliminación de las conversaciones del contacto "clear-msgs", los últimos cuatro dígitos del número de teléfono asociado a la cuenta de WhatsApp (jid) eliminada cuando es un contacto y la identificación (campo "_id") del último mensaje del chat que se encontraba grabado en la tabla "**message**" de la base de datos "**msgstore.db**". Se puede identificar el borrado de archivos multimedia "/deletemedia/" y el número total de mensajes eliminados "totalMessages:", que en este ejemplo son **8**:

```
2025-11-25 11:59:39.441 LL_I D [103:WhatsApp Worker #16] CoreMessageStore/clearmsgs/service/jid 2292@s.whatsapp.net excludeStarred:false
2025-11-25 11:59:39.446 LL_I D [103:WhatsApp Worker #16] msgstore/deletemsgs/mark jid:2292@s.whatsapp.net lastDeletedMessageSortId:2782 lastDeletedStarredMessageSortId:2782 jobId: 67
2025-11-25 11:59:39.449 LL_I D [103:WhatsApp Worker #16] msgstore/lastmsgid/count 0
2025-11-25 11:59:39.455 LL_I D [103:WhatsApp Worker #16] CoreMessageStore/updateChatTable/updated:1
2025-11-25 11:59:39.455 LL_I D [103:WhatsApp Worker #16] CoreMessageStore/clearmsgs/service/ adding plaintext disabled message
2025-11-25 11:59:39.455 LL_I D [103:WhatsApp Worker #16] VerifiedNameManager/getVerifiedNameDeprecated, jid: 2292@s.whatsapp.net, vlevel:0
2025-11-25 11:59:39.592 LL_I D [129:androidx.work-1] msgstore/deletemsgs/batches/timer/start
2025-11-25 11:59:39.593 LL_I D [129:androidx.work-1] msgstore/countmessagesdelete/count: 8
2025-11-25 11:59:39.595 LL_I D [129:androidx.work-1] msgstore/deletemedia/batch/files/timer/start
2025-11-25 11:59:39.650 LL_I D [129:androidx.work-1] msgstore/deletemedia/batch/files/timer/stop: 56
2025-11-25 11:59:39.654 LL_I D [129:androidx.work-1] CoreMessageStore/deletemedia/batch/files 2292@s.whatsapp.net timeSpent:56
2025-11-25 11:59:39.698 LL_I D [129:androidx.work-1] msgstore/deleteMessageThumbnailsFor-jid/0
2025-11-25 11:59:39.698 LL_I D [129:androidx.work-1] msgstore/deletemsgs/batches/timer/elapsed: 106
2025-11-25 11:59:39.733 LL_I D [129:androidx.work-1] msgstore/deletemsgs/batches/timer/stop: 141
2025-11-25 11:59:39.733 LL_I D [129:androidx.work-1] CoreMessageStore/deletemsgs/batches 2292@s.whatsapp.net haveMessagesToDelete:false timeSpent:141 currentMessages:8 totalMessages:8
2025-11-25 11:59:39.734 LL_I D [129:androidx.work-1] msgstore/deletemsgs/unmark jid:2292@s.whatsapp.net
```

A diferencia del caso del vaciado de chats individuales, cuando se vacía un grupo, WhatsApp muestra el identificador “jid” completo.

ios

La posibilidad de obtener información del vaciado de un chat es muy limitada puesto que únicamente se almacenan esos datos en los archivos de logs, los cuales permanecen unos pocos días en el sistema. Además, está el inconveniente de que para obtenerlos de un iPhone es necesario una extracción de sistema de archivos completo (FFS).

El vaciado se puede determinar por el registro del texto “chatsession/delete” y el identificador parcial “jid” del contacto con el que se mantenía el chat. También se informa de la cantidad de mensajes que son eliminados “delete-messages; count:”, que en este ejemplo son **37**:

```
12:59:24.933 [ 8172] [main-thread ] [F] LL_A chatsession/delete [<*****2522@s.whatsapp.net>]
12:59:24.940 [ 8172] [main-thread ] [F] LL_A chatsession/<*****2522@s.whatsapp.net>/counter/2
12:59:24.955 [ 8172] [NSManaged...8820] [F] LL_A storage//save/success [AppStateStore in 0.00s with changes]
12:59:24.956 [ 8172] [main-thread ] [F] LL_W chatsessions//controller-will-change-content _selectedChatSessionBeforeFetchResultsControllerUpdate: *****2595@s.whatsapp.net
12:59:24.956 [ 8172] [main-thread ] [F] LL_A chatsessions//controller-did-change-content
12:59:24.959 [ 8172] [main-thread ] [F] LL_A chatsessions//reload-tableview/preserving-selected-chatsession chatSession:*****2522@s.whatsapp.net
12:59:24.959 [ 8172] [main-thread ] [F] LL_A chatlist//select-row/ chatJID: *****2522@s.whatsapp.net
12:59:24.959 [ 8172] [main-thread ] [F] LL_A chatsessions//select-row chatSession:*****2522@s.whatsapp.net
12:59:24.959 [ 8172] [main-thread ] [F] LL_A chatsessions//did-finish-updating-tableview
12:59:25.020 [ 8172] [main-thread ] [F] LL_A messages-by-session//by-session [id: delete-messages; count: 37; has-more: 0]
```

A diferencia del caso del vaciado de chats individuales, cuando se vacía un grupo, WhatsApp muestra el identificador "jid" completo.

Otra fuente de información en una extracción FFS, si está presente, puede ser la base de datos "**AppState.sqlite**". La tabla "**ZAPPSTATE-CONFIRMEDMUTATIONENTITY**" registrará los chats vaciados, los cuales presentarán el valor "**clearChat**" en el campo "**ZACTIONNAME**", y el identificador "jid" del chat en el campo "**ZTARGETID**".

10.5. Eliminación de chat

Con la funcionalidad "eliminación de chat" se borra por completo el chat, y a diferencia del vaciado, no aparecerá en la lista de chats abiertos con otros contactos. Para eliminar un chat de grupo, previamente hay que salir del chat.

Al igual que en el vaciado, la aplicación ofrece el borrado de los archivos multimedia asociados al chat.

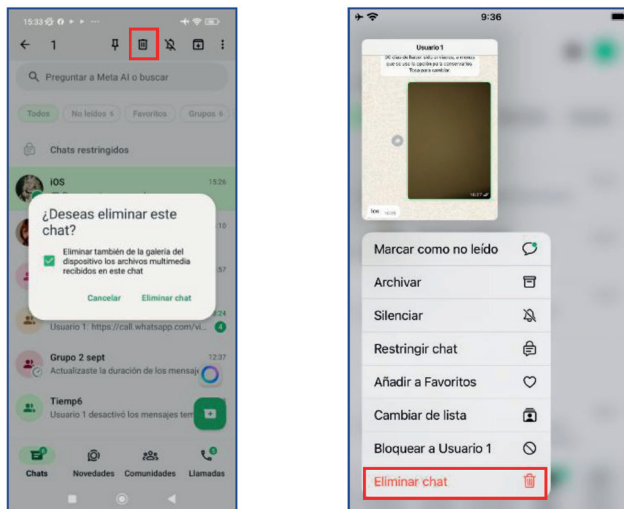


Ilustración 305. "Eliminar chat" en la versión Android (izq.) e iOS (dcha.)

Android

El rastro que deja la eliminación de chat en el dispositivo hay que buscarlo en el fichero dedicado al almacenamiento de logs denominado whatsapp.log. Lo primero que se detecta en este log es la eliminación del contacto `"/delete-contact"` y las conversaciones del contacto, los últimos cuatro dígitos del identificador `"jid"` del contacto con el que se mantenía el chat eliminado y la identificación (campo `_id`) del último mensaje del chat que se encontraba grabado en la tabla **"message"** de la base de datos **"msgstore.db"**. Se puede identificar el borrado de archivos multimedia `"/deletemedia/"` y el número total de mensajes eliminados `"totalMessages:"`, que en este ejemplo son **207**:

```
2025-11-13 09:16:10.447 LL_I W [2:main] conversations/delete-contact
2025-11-13 09:16:10.514 LL_I W [812:WhatsApp Worker #150] CoreMessageStore/deletemsgs/service/jid 5824@s.whatsapp.net
2025-11-13 09:16:10.516 LL_I W [812:WhatsApp Worker #150] msgstore/deletemsgs/mark jid:5824@s.whatsapp.net lastDeletedMessageSortId:3404 lastDeletedStarredMessageSortId:3404 jobId: 75
2025-11-13 09:16:10.574 LL_I W [814:androidx.work-4] msgstore/deletemsgs/batches/timer/start
2025-11-13 09:16:10.574 LL_I W [814:androidx.work-4] msgstore/countmessagestodelete/count: 207
2025-11-13 09:16:10.596 LL_I W [455:WhatsApp Worker #126] ReferenceCountedFileManager/deleteManagedFile actually deleting file
2025-11-13 09:16:10.598 LL_I W [815:WhatsApp Worker #151] ReferenceCountedFileManager/deleteManagedFile actually deleting file
2025-11-13 09:16:11.483 LL_I W [814:androidx.work-4] msgstore/deletemedia/batch/files/timer/stop: 41
2025-11-13 09:16:11.483 LL_I W [814:androidx.work-4] CoreMessageStore/deletemedia/batch/files 5824@s.whatsapp.net timeSpent:41
2025-11-13 09:16:11.484 LL_I W [814:androidx.work-4] msgstore/deleteMessageThumbnailsFor-jid/0
2025-11-13 09:16:11.484 LL_I W [814:androidx.work-4] msgstore/deletemsgs/batches/timer/elapsed: 909
2025-11-13 09:16:11.489 LL_I W [814:androidx.work-4] msgstore/deletemsgs/batches/timer/stop: 916
2025-11-13 09:16:11.489 LL_I W [814:androidx.work-4] CoreMessageStore/deletemsgs/batches 5824@s.whatsapp.net haveMessagesToDelete:false timeSpent:916 currentMessages:207 totalMessages:207
2025-11-13 09:16:11.490 LL_I W [814:androidx.work-4] msgstore/deletemsgs/unmark jid:5824@s.whatsapp.net
```

A diferencia del caso de la eliminación de chats individuales, cuando se elimina un grupo, WhatsApp registra el identificador `"jid"` completo:

```
2025-11-13 09:14:37.861 LL_I W [2:main] conversations/delete/group.row_id=254 jid=363392539990697@g.us key=(null) phone=0 iswa=true status=null
2025-11-13 09:15:01.440 LL_I W [2:main] conversations/user-deleteGroup
2025-11-13 09:15:01.554 LL_I W [690:WhatsApp Worker #141] CoreMessageStore/deletemsgs/service/jid 363392539990697@g.us
2025-11-13 09:15:01.559 LL_I W [690:WhatsApp Worker #141] msgstore/deletemsgs/mark jid:363392539990697@g.us lastDeletedMessageSortId:3435 lastDeletedStarredMessageSortId:3435 jobId: 74
2025-11-13 09:15:01.654 LL_I W [695:androidx.work-3] msgstore/countmessagestodelete/count: 38
2025-11-13 09:15:01.774 LL_I W [695:androidx.work-3] msgstore/deletemedia/batch/files/timer/stop: 118
2025-11-13 09:15:01.774 LL_I W [695:androidx.work-3] CoreMessageStore/deletemedia/batch/files 363392539990697@g.us timeSpent:118
2025-11-13 09:15:01.804 LL_I W [695:androidx.work-3] msgstore/deleteMessageThumbnailsFor-jid/0
2025-11-13 09:15:01.824 LL_I W [695:androidx.work-3] msgstore/deletemsgs/batches/timer/stop: 171
2025-11-13 09:15:01.825 LL_I W [695:androidx.work-3] CoreMessageStore/deletemsgs/batches 363392539990697@g.us haveMessagesToDelete:false timeSpent:171 currentMessages:38 totalMessages:38
2025-11-13 09:15:01.825 LL_I W [695:androidx.work-3] msgstore/deletemsgs/unmark jid:363392539990697@g.us
2025-11-13 09:15:01.825 LL_I W [695:androidx.work-3] ParticipantUserStore/updateGroupParticipants/deleteParticipants 363392539990697@g.us
```

iOS

Como en los apartados anteriores, el archivo que puede contener información sobre la eliminación de un chat es el archivo que almacena los logs, denominado "whatsapp-AAAA-MM-DD-hh-mm-ss-mss-WhatsApp-xxx.log". Se registra tanto la eliminación del chat de la lista de chats "chatlist/delete", como el de la sesión del chat "chatsession/delete", añadiendo en ambos registros el identificador parcial "jid" del contacto con el que se mantenía el chat. Lo último que registra es el número de mensajes eliminados ("count: **25**"):

```
12:25:28.638 [ 4860] [main-thread ] [F] LL_A chatlist/delete/confirmed [<*****2295@s.whatsapp.net>]
12:25:28.650 [ 4860] [main-thread ] [F] LL_A chatsession/delete [<*****2295@s.whatsapp.net>]
12:25:28.795 [ 6284] [message-delete] [F] LL_A message/report-token-store/reporting-tag deleting repor-
ting tags for message IDs:
<*****2295@s.whatsapp.net>_3AFD46199F2A8D225E3E_1_0
<*****2295@s.whatsapp.net>_29EB01E5778CAB5743DB5D3B8F50F593_0_0
<*****2295@s.whatsapp.net>_B3976855E6A1B256E0A050BD15F81EE8_0_0
<*****2295@s.whatsapp.net>_8E669912BF59C315F70716519AB36433_0_0
<*****2295@s.whatsapp.net>_3A21671978D4EEF4DFA7_1_0
<*****2295@s.whatsapp.net>_3AA75C8054BF6DA1FFD5_0_0
<*****2295@s.whatsapp.net>_24CAEBBCFC7F2564209FF0F22785278A_0_0
<*****2295@s.whatsapp.net>_3A3983BDA68295BD60A4_0_0
<*****2295@s.whatsapp.net>_3A3983BDA68295BD60A4_0_0
12:25:28.798 [ 5379] [network-normal] [F] LL_N stream//> send > [iq/set ns=w:sync:app:state t=s.whatsapp.
net id=1739449360-25]
12:25:28.804 [ 6284] [message-delete] [F] LL_A message/report-token-store/reporting-token deleting re-
porting tokens for message IDs:
<*****2295@s.whatsapp.net>_3AFD46199F2A8D225E3E_1_0
<*****2295@s.whatsapp.net>_29EB01E5778CAB5743DB5D3B8F50F593_0_0
<*****2295@s.whatsapp.net>_B3976855E6A1B256E0A050BD15F81EE8_0_0
<*****2295@s.whatsapp.net>_8E669912BF59C315F70716519AB36433_0_0
<*****2295@s.whatsapp.net>_3A21671978D4EEF4DFA7_1_0 <*****2295@s.whatsapp.net>_3AA75C8054BF6DA1FFD5_0_0
<*****2295@s.whatsapp.net>_24CAEBBCFC7F2564209FF0F22785278A_0_0
<*****2295@s.whatsapp.net>_3A3983BDA68295BD60A4_0_0
<*****2295@s.whatsapp.net>_3A3983BDA68295BD60A4_0_0
12:25:28.807 [ 6052] [searchengine ] [F] LL_A searchengine/delete [count: 25, first: 1279]
```

En las eliminaciones de grupo, WhatsApp registra la eliminación del chat de la lista de chats "chatlist/delete", y de la sesión del chat "chatsession/delete", añadiendo en ambos registros el identificador parcial "jid" del grupo. Lo último que registra es el número de mensajes eliminados ("count: **39**"):


```
09:37:05.965 [ 3494] [main-thread ] [F] LL_A chatlist/delete/confirmed [<*****0697@g.us>]
09:37:05.975 [ 3494] [main-thread ] [F] LL_A chatsession/delete [<*****0697@g.us>]
09:37:06.132 [ 5849] [NSManaged...4ea0] [F] LL_E internal-participantJID/group-member-nil
09:37:06.134 [ 5583] [message-delete] [F] LL_A message/report-token-store/reporting-tag deleting repor-
ting tags for message IDs:
<*****0697@g.us>_3ADF13C44FB5275AFAD5_1_0
<*****0697@g.us>_D050D84543D62AA37BF93AF3AC705029_0_<*****2387@s.whatsapp.net>
<*****0697@g.us>_D06C5122CE8BF85DE0CF98387C9B8C08_0_<*****9955@s.whatsapp.net>
<*****0697@g.us>_3A1469AA9EB850DAE16A_0_0
<*****0697@g.us>_3A1D82E64AB24EAA7AC4_1_0
<*****0697@g.us>_EFEECD86F723CD394DA88991804D011B_0_<*****2387@s.whatsapp.net>
<*****0697@g.us>_3AB9E732FB38C2BB6B1F_0_<*****5824@s.whatsapp.net>
<*****0697@g.us>_2FD107AFE4705965F2D550ED...
09:37:06.136 [ 5796] [network-normal] [F] LL_N stream//> send > [iq/set ns=w:sync:app:state t=s.whatsapp.
net id=1739439219-26]
09:37:06.154 [ 5583] [message-delete] [F] LL_A message/report-token-store/reporting-token deleting re-
porting tokens for message IDs:
<*****0697@g.us>_D050D84543D62AA37BF93AF3AC705029_0_<*****2387@s.whatsapp.net>
<*****0697@g.us>_3ADF13C44FB5275AFAD5_1_0
<*****0697@g.us>_3A1D82E64AB24EAA7AC4_1_0
<*****0697@g.us>_D06C5122CE8BF85DE0CF98387C9B8C08_0_<*****9955@s.whatsapp.net>
<*****0697@g.us>_3A1469AA9EB850DAE16A_0_0
<*****0697@g.us>_EFEECD86F723CD394DA88991804D011B_0_<*****2387@s.whatsapp.net>
<*****0697@g.us>_17ACB07EC852A76C6AF51CA0A447715D_0_<*****9955@s.whatsapp.net>
<*****0697@g.us>_3AB9E732...
09:37:06.157 [ 5852] [searchengine ] [F] LL_A searchengine/delete [count: 39, first: 1279]
```

De forma análoga a lo que ocurre en el vaciado de chat, en una extracción FFS la base de datos **“AppState.sqlite”** puede aportar información relevante. En particular, la tabla **“ZAPPSTATECONFIRMEDMUTATIONENTITY”** registra los chats eliminados, presentando el valor **“deleteChat”** en el campo **“ZACTIONNAME”**, junto con el identificador **“jid”** del chat correspondiente en el campo **“ZTARGETID”**.

Apéndice: recuperación de datos

La recuperación de información eliminada es siempre una de las prioridades de un analista forense, aunque por desgracia la tecnología implementada actualmente en los teléfonos móviles impide prácticamente por completo esta posibilidad. Las pruebas realizadas sobre los dispositivos con los dos sistemas operativos han dado como resultado que la recuperación de información eliminada de las bases de datos es sumamente limitada en Android e inexistente en iOS.

Aunque pueda parecer desilusionante el panorama, se puede seguir numerosas estrategias exitosas para recuperar información y/o interpretar lo sucedido. Es el analista el que tiene que decidir en qué bases de datos, archivos de configuración, directorios de almacenamiento de archivos, etc., profundizar dependiendo de la investigación y el sistema operativo del teléfono. Puede parecer que la información en la versión para Android es más prolífica, pero lo cierto es que a partir de una extracción FFS de un iPhone se puede obtener muchísima información, si bien, el análisis e interpretación es más compleja debido a su codificación, como puede ser con archivos protobuf.

Hay que recordar que aun cuando se elimina un archivo multimedia (no el mensaje en el que fue transmitido), es posible que existan copias en el dispositivo y que se puedan vincular con el envío de un mensaje por

medio de su hash SHA-256 codificado en Base64. En Android también es posible vincular una imagen o un vídeo original, a partir del cual se ha generado una versión comprimida para su envío con el mensaje en el que se ha adjuntado. Técnica que puede proporcionar evidencia indirecta en el análisis.

Como ejemplo, en la versión de WhatsApp para Android, interesa recuperar la información de la tabla **"message"**, en la base de datos **"msgstore.db"**, que es donde se registran todos los mensajes transmitidos. Al tratarse de una base de datos SQLite v.3 con "WAL", los cambios que se vaya a producir en la base de datos se graban temporalmente en el archivo "WAL". Esto tiene unas implicaciones importantes en cuanto a la recuperación de información se refiere, debido a que, si ha transcurrido muy poco tiempo desde el borrado del mensaje y la extracción de la base de datos del dispositivo, es posible que se pueda recuperar su contenido. Pero dicha posibilidad disminuye con el paso del tiempo. Actualmente, la mayoría de las herramientas comerciales de análisis forense de dispositivos móviles automatizan este proceso, combinando la información almacenada en la base de datos principal y el archivo "WAL", lo que facilita la recuperación en estos casos.

Otra técnica de recuperación implica analizar directamente la base de datos en bruto, que puede contener información eliminada durante un período de tiempo limitado. Sin embargo, estos datos suelen estar parcialmente corruptos, lo que requiere un análisis manual detallado y conocimiento técnico profundo sobre el funcionamiento interno de bases de datos SQLite v.3. Estas técnicas avanzadas están fuera del alcance y objetivo de este estudio.

En las pruebas realizadas, los datos de los mensajes eliminados no han permanecido más de uno o dos días en las bases de datos y el archivo WAL. Con un uso intensivo de la aplicación, es probable que los datos se mantengan solo unas horas o incluso menos. Por ello, es fundamental analizar las posibles copias de seguridad y obtener todos los dispositivos de los participantes en el chat de interés, aumentando las probabilidades de que algún usuario no haya eliminado los mensajes y/o archivos buscados.

De hecho, se puede consultar en la tabla "**backup_changes**" de la base de datos "**msgstore.db**" los mensajes que han sido eliminados (por cualquier motivo) en la aplicación y están pendientes de borrarse en la copia de seguridad local que se está creando incrementalmente. Esta consulta se centra en el valor "DELETE" para el campo "**operation**", el valor "message" para el campo "**table_name**" y el valor del campo "**table_row_id**", que se corresponde con el número de registro que tenía el mensaje eliminado en la tabla "**message**". Los cambios registrados en la tabla "**backup_changes**" se refieren a la última copia de seguridad local generada y habría que consultar también las copias de seguridad anteriores ante la posibilidad de que contengan alguno de los mensajes eliminados. Si se elimina un mensaje después de que ya se haya generado una copia de seguridad, ésta no se verá afectada por ese borrado. Lógicamente si no se han llevado a cabo esos cambios en las copias de seguridad, se podrá recuperar toda la información de esa copia de la base de datos "**msgstore.db**", pero la posibilidad de que los archivos transmitidos se encuentren en el dispositivo dependerá de circunstancias variadas ya explicadas en esta investigación.

Cada sistema operativo tiene sus ventajas y desventajas a la hora de realizar análisis forenses. Sin embargo, ambos ofrecen una gran cantidad de información que el usuario final generalmente desconoce que se encuentra almacenada en el dispositivo y que no es visible a través de las interfaces gráficas de la aplicación. Este tipo de información oculta puede ser clave para reconstruir eventos y aportar pruebas en investigaciones forenses, siempre y cuando el analista tenga la experiencia y las herramientas necesarias para extraerla e interpretarla de manera adecuada.

Referencias

Cellebrite – <https://cellebrite.com>

DB Browser for SQLite – <https://sqlitebrowser.org/>

Download WhatsApp Messenger APKs for Android - APKMirror – <https://www.apkmirror.com/apk/whatsapp-inc/whatsapp/>

GitHub - ElDavoo/wa-crypt-tools: Manage WhatsApp .crypt12, .crypt14 and .crypt15 files. – <https://github.com/ElDavoo/wa-crypt-tools>

HashMyFiles: Calculate MD5/SHA1/CRC32 hash of files – HashMyFiles: Calculate MD5/SHA1/CRC32 hash of files

<https://www.whatsapp.com/>

Notepad++ – <https://notepad-plus-plus.org/downloads/>

Oxygen Forensics Detective - <https://www.oxygenforensics.com/en/>

Protobuf Decoder – <https://github.com/pawitp/protobuf-decoder>

WABetaInfo – <https://wabetainfo.com/>

ANÁLISIS FORENSE DE LA APLICACIÓN WHATSAPP EN SISTEMAS ANDROID E IOS

Este estudio explora la funcionalidad de la aplicación WhatsApp en sus versiones para las plataformas Android e iOS, centrándose en sus características, arquitectura y gestión de datos desde una perspectiva forense digital. WhatsApp, como una de las aplicaciones de mensajería más utilizadas a nivel mundial, se presenta como una fuente crucial de evidencia en investigaciones forenses. En la investigación se analizan las similitudes y diferencias en la funcionalidad entre los dos sistemas operativos. Además, se examinan los artefactos generados por WhatsApp, como registros, bases de datos y archivos multimedia, y se evalúa su relevancia forense. El estudio tiene como objetivo proporcionar una visión más profunda de los mecanismos que subyacen al funcionamiento de WhatsApp, ayudando a los expertos forenses a identificar y analizar rastros digitales relevantes. Al comprender los comportamientos específicos de la plataforma, esta investigación contribuye a mejorar las metodologías forenses y a garantizar una recopilación exhaustiva de evidencias en contextos legales y de investigación. De la misma forma, permite verificar y complementar manualmente información presentada por herramientas forenses especializadas.



VNiVERSiDAD
D SALAMANCA

