

**MÁSTER UNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE
LA INFORMACIÓN Y LAS COMUNICACIONES**

TRABAJO FIN DE MÁSTER

**ANÁLISIS DEL MODELO DE
DATOS DE LA RED SOCIAL
WHATSAPP Y SUS APLICACIONES
AL PERITAJE**

Autor
D. Carlos Pintos Teigeiro

Director del Trabajo Fin de Máster
D. Santiago Hernández Ramos

CURSO 2019-2020



RESUMEN

La red social de mensajería instantánea WhatsApp ha tomado el relevo de muchas otras formas de comunicación llegando incluso a sustituirlas. Actualmente es la aplicación de mensajería instantánea más utilizada con más de 2000 millones de usuarios. Esto hace que conversaciones a través de esta aplicación sean evidencias que son aportadas diariamente a infinidad de procesos judiciales. El presente trabajo realiza un análisis del modelo de datos de la aplicación WhatsApp y de algunos de los artefactos con los que se relaciona para ver sus aplicaciones a la obtención de evidencias para un procedimiento judicial.

El trabajo realiza un análisis del estado del arte en procedimientos y herramientas para la recuperación de información de dispositivos móviles. A partir de esto se desarrolla un análisis de la estructura de carpetas, su contenido y del modelo de datos en la plataforma IOS y Android analizando todas las bases de datos, la estructura de sus campos y el contenido de los mismos. Se ha podido documentar las diferencias entre ambos modelos, mostrando que IOS ofrece un modelo de datos más estructurado y normalizado pero que al mismo tiempo aporta menos información desde el punto de vista forense ya que en Android al haber información repetida en varias tablas, permite la realización de comprobaciones cruzadas que dificultan la falsificación de datos. Adicionalmente se realiza un análisis de los datos que la base de datos contiene de cara a definir el comportamiento de la aplicación en aquellas funcionalidades que pueden tener interés desde el punto de vista forense. Se responden a preguntas como ¿Cómo se realiza una comunicación? ¿Qué usuarios participaron en la misma? ¿Se puede demostrar que un usuario recibió/envió un mensaje? ¿formaba un usuario parte de un grupo? ¿Se pueden recuperar mensajes borrados?

Para el desarrollo del trabajo se ha creado una infraestructura con dos terminales Apple con sistemas operativos IOS 12 e IOS 13 y con dos máquinas virtuales con sistema Android sobre la que se han realizado pruebas de concepto de cara a analizar el comportamiento de la aplicación. Se han cubierto las funcionalidades de gestión de contactos, envío de mensajes, llamadas, gestión de grupos de usuarios, bloqueos, borrado de mensajes y uso de WhatsApp Web.

El desarrollo del trabajo permite tener una visión clara de cómo se realiza una comunicación, identificando el tipo de mensaje, verificando el tipo de contenido enviado (y accediendo y recuperando el mismo), desarrolla la forma de identificar el estado del mensaje (enviado, entregado, leído, etc.). Tanto a nivel mensaje individual, grupos, como listas de distribución. Se ha identificado la forma de detectar la fuente del envío del mensaje (WhatsApp Web o terminal). Incluso se analizan las distintas formas de recuperar información borrada de la base de datos. Además, el trabajo analiza la realización de llamadas permitiendo identificar información ellas (destinatarios, duración, tipo, etc.).

El trabajo ha permitido mostrar las diferencias entre ambas plataformas e identificar en el modelo de datos la implementación de funcionalidades que todavía no están desarrolladas y/o puestas a disposición del público, lo que aporta una base para la realización de trabajos futuros en funcionalidades como el pago, el uso de distintos terminales o el borrado diferido.



ABSTRACT

WhatsApp instant messaging platform has taken over many other ways of communication even replacing them. Is the most used instant messaging application with over 2000 million users worldwide. This makes that conversations thought this mobile app become evidences that are provided daily to countless judicial processes. The present job develops an analysis of WhatsApp app data model and of some of the artifacts with which it is involved to investigate its applications to acquire evidences that can be used in a court.

The study carries out an analysis of the state of the art in procedures and tools for the retrieval of information from mobile devices. From this, an analysis of the folder structure, its content, and the data model in the IOS and Android platforms is developed, analyzing all the databases, the structure of their fields and their content. It has been possible to document the differences between the two models, showing that IOS offers a more structured and normalized data model but at the same time provides less information from the forensic point of view since in Android, as there is repeated information in several tables, allows performing cross-checks that make data falsification difficult. Additionally, an analysis of the data that the database contains is carried out to define the behavior of the application in those functionalities that may be of interest from a forensic point of view. Questions such as How is communication carried out? What users participated in it? Can it be proven that a user received /sent a message? Was a user part of a group? Can deleted messages be recovered?

For the development of the study, an infrastructure has been created with two Apple terminals with operating systems IOS 12 and IOS 13 and with two virtual machines with Android system on which concept tests have been carried out in order to analyze the behavior of the application. The functionalities of managing contacts, sending messages, calls, managing user groups, blocking, deleting messages, and using WhatsApp Web have been covered.

The development of the study allows having a clear vision of how a communication is carried out, identifying the type of message, verifying the type of content sent (and accessing and retrieving it), developing the way to identify the status of the message (sent, delivered , read, etc). Both at the individual message level, groups, and distribution lists. The way to detect the source of sending the message (WhatsApp Web or a physical terminal) has been identified. The different ways of recovering information deleted from the database are even analyzed. In addition, the work analyzes the making of calls, allowing them to identify information (recipients, duration, type, etc.).

The study has allowed to show the differences between both platforms and to identify in the data model the implementation of functionalities that are still being developed and/or not made available to the public, which provides a basis for carrying out future work on functionalities such as payment , the use of different terminals or delayed deletion.



AGRADECIMIENTOS

Quiero agradecer a las empresas [Compelson Labs](#) y a [Oxygen Forensics](#) por la cesión para la realización de este trabajo de una licencia del software [Mobileedit Forensics Express](#) y [Oxygen Forensics Detective](#) que han resultado de extraordinaria utilidad para la obtención de artefactos y el análisis de los mismos. Debo hacer una especial mención a los técnicos de soporte de ambas empresas que han tenido la cortesía de atender mis preguntas y resolver las dudas que pudieran surgir.

Adicionalmente quiero agradecer a las personas más especiales que cada día están a mi lado y que con su apoyo me han acompañado con el esfuerzo de la realización del máster y de este trabajo, Ana, Javier y especialmente Marian (por lo que le toca aguantar) sois mi motivación para ser mejor cada día.

Pero sobre todo este trabajo está dedicado a la mejor persona que he conocido nunca. Muchas gracias, papá por haber sido ser un ejemplo para mí cada día de tu vida. Gracias por haber estado ahí siempre con tu cariño y tu buen humor. Me has mostrado el camino que las buenas personas siguen y me has enseñado con el ejemplo los valores que hacen de mí la persona que soy hoy.

ÍNDICE DE CAPÍTULOS Y ANEXOS

1	INTRODUCCIÓN	21
2	ESTADO DE LA CUESTIÓN	23
2.1	EXTRACCIÓN DE LA BASE DE DATOS DE WHATSAPP	23
2.2	ESTADO DEL ARTE EN EXTRACCIÓN Y ANÁLISIS DE WHATSAPP	26
3	DESCRIPCIÓN DEL PROBLEMA	29
4	SOLUCIÓN PROPUESTA	30
4.1	OBJETIVOS	30
4.2	METODOLOGÍA	30
5	PRUEBAS Y VALIDACIÓN	32
5.1	ANÁLISIS DEL MODELO DE DATOS DE WHATSAPP EN LA PLATAFORMA IOS.	32
5.1.1	ESTRUCTURA DE CARPETAS Y UBICACIÓN DE ARCHIVOS	32
5.1.2	ESTRUCTURA DE LA BASE DE DATOS BIZ.SQLITE	35
5.1.3	ESTRUCTURA DE LA BASE DE DATOS BACKEDUPVALUEKEY.SQLITE	39
5.1.4	ESTRUCTURA DE LA BASE DE DATOS CALLHISTORY.SQLITE.....	40
5.1.5	ESTRUCTURA DE LA BASE DE DATOS CONTACTSV2.SQLITE.....	42
5.1.6	ESTRUCTURA DE LA BASE DE DATOS CHATSTORAGE.SQLITE	46
5.1.7	BASES DE DATOS RANKING.SQLITE, EMOJI.SQLITE Y STICKER.SQLITE.....	63
5.2	ANÁLISIS DEL MODELO DE DATOS DE WHATSAPP PARA ANDROID	63
5.2.1	ESTRUCTURA DE CARPETAS Y UBICACIÓN DE ARCHIVOS	63
5.2.2	ESTRUCTURA DE LA BASE DE DATOS AXOLOTL.DB	67
5.2.3	ESTRUCTURA DE LA BASE DE DATOS CHATSETTINGS.DB	68
5.2.4	ESTRUCTURA DE LA BASE DE DATOS COMPANION_DEVICES.DB	68
5.2.5	ESTRUCTURA DE LA BASE DE DATOS HSMPACKS.DB.....	69
5.2.6	ESTRUCTURA DE LA BASE DE DATOS LOCATION.DB	70

5.2.7	ESTRUCTURA DE LA BASE DE DATOS MEDIA.DB	72
5.2.8	ESTRUCTURA DE LA BASE DE DATOS MSGSTORE.DB.....	73
5.2.9	ESTRUCTURA DE LA BASE DE DATOS PAYMENTS.DB	145
5.2.10	ESTRUCTURA DE LA BASE DE DATOS STICKERS.DB	146
5.2.11	ESTRUCTURA DE LA BASE DE DATOS WA.DB	147
5.2.12	ESTRUCTURA DE LA BASE DE DATOS WEB_SESSIONS.DB	158
5.3	TIPOS DE COMUNICACIÓN Y SUS IDENTIFICADORES	159
6	EXPERIMENTACIÓN Y RESULTADOS	161
6.1	ANÁLISIS FORENSE DEL COMPORTAMIENTO DE LA APLICACIÓN	161
6.1.1	CU.01 CONTACTOS EN WHATSAPP	161
6.1.2	CU.02 ENVÍO DE MENSAJES.	161
6.1.3	CU.03 LLAMADAS	162
6.1.4	CU.04 GRUPOS	162
6.1.5	CU.05 BLOQUEO.....	162
6.1.6	CU.06 BORRADO DE MENSAJES	162
6.1.7	CU.07 WHATSAPP WEB	162
6.1.8	CU.08 UBICACIÓN EN TIEMPO REAL	163
6.2	CONTACTOS EN WHATSAPP	163
6.2.1	ALMACENAMIENTO DE INFORMACIÓN DE CONTACTOS	163
6.2.2	CREACIÓN Y BORRADO DE USUARIOS.....	165
6.3	ENVÍO DE MENSAJES.	166
6.3.1	ENVÍO Y RECEPCIÓN DE MENSAJES EN DISPOSITIVOS ANDROID	167
6.3.2	ENVÍO Y RECEPCIÓN DE MENSAJES EN DISPOSITIVOS IOS.....	169
6.3.3	LLAMADAS EN WHATSAPP	172
6.4	GRUPOS	174
6.4.1	ENVÍO DE MENSAJES EN GRUPOS.....	174
6.4.2	CREACIÓN DE UN GRUPO.....	175
6.4.3	AÑADIR Y ELIMINAR USUARIOS A UN GRUPO	175

6.5	LISTAS DE DISTRIBUCIÓN	176
6.6	BLOQUEOS DE USUARIOS	177
6.7	BORRADO DE DATOS.....	178
6.8	ENVÍO DESDE DISTINTOS TERMINALES.....	180
6.9	UBICACIÓN EN TIEMPO REAL.....	180
7	CONCLUSIONES	183
8	TRABAJOS FUTUROS.....	185
9	BIBLIOGRAFÍA.....	187

ÍNDICE TABLAS

Tabla 1 Comparativa del estado del Arte en extracción y análisis de WhatsApp	28
Tabla 2 Contenido de la estructura de carpetas de backup iOS	35
Tabla 3 Esquema de la tabla ZWAAGREATECALLEVENT	41
Tabla 4 Esquema de la tabla ZWACDCALLEVENT	42
Tabla 5 Esquema de la tabla ZWACDCALLEVENTPARTICIPANT	42
Tabla 6 Esquema de la tabla ZWAADDRESSBOOKCONTACT	45
Tabla 7 Esquema de la tabla ZWABLACKLISTITEM	47
Tabla 8 Esquema de la tabla ZWACHATPROPERTIES	48
Tabla 9 Esquema de la tabla ZWACHATPUSHCONFIG	48
Tabla 10 Esquema de la tabla ZWACHATSESSION	50
Tabla 11 Esquema de la tabla ZWAGROUPINFO	51
Tabla 12 Esquema de la tabla ZWAGROUPMEMBER	52
Tabla 13 Esquema de la tabla ZWAGROUPMEMBERSCHANGE	52
Tabla 14 Esquema de la tabla ZWAMEDIAITEM	54
Tabla 15 Esquema de la tabla ZWAMESSAGE	58
Tabla 16 Esquema de la tabla ZWAMESSAGEDATAITEM	59
Tabla 17 Esquema de la tabla ZWAMESSAGEINFO	60
Tabla 18 Esquema de la tabla ZWAPROFILEPICTUREITEM	61
Tabla 19 Esquema de la tabla ZWAPROFILEPUSHNAME	61
Tabla 20 Contenido de la estructura de directorios en terminal Android	67
Tabla 21 Esquema de la tabla location_cache	71
Tabla 22 Esquema de la tabla location_key_distribution	71
Tabla 23 Esquema de la tabla location_sharer	72
Tabla 24 Esquema de la tabla call_log	75
Tabla 25 Esquema de la tabla call_log_participant_v2	76
Tabla 26 Esquema de la tabla chat	80
Tabla 27 Esquema de la tabla chat_list	83
Tabla 28 Esquema de la tabla frequents	85
Tabla 29 Contenido de la tabla group_participants	88

Tabla 30 Contenido de la tabla jid.....	90
Tabla 31 Contenido de la tabla message_forwarded.....	96
Tabla 32 Contenido de la tabla message_ftwv2	97
Tabla 33 Contenido de la tabla message_ftsv2_content.....	98
Tabla 34 Contenido de la tabla message_ftsv2_docsizes.....	99
Tabla 35 Contenido de la tabla message_media	106
Tabla 36 Contenido de la tabla message_streaming_sidecar.....	115
Tabla 37 Contenido de la tabla message_thumbnails	121
Tabla 38 Contenido de la tabla message_vcard_jid.....	122
Tabla 39 Contenido de la tabla messages	130
Tabla 40 Contenido de la tabla messages_fts_content	132
Tabla 41 Contenido de la tabla messages_vcard	135
Tabla 42 Contenido de la tabla messages_vcards_jid.....	136
Tabla 43 Contenido de la tabla missed_call_participants.....	137
Tabla 44 Contenido de la tabla missed_call_logs	138
Tabla 45 Contenido de la tabla props	140
Tabla 46 Contenido de la tabla sqlite_sequence	143

ÍNDICE FIGURAS

Ilustración 1 Estructura de carpetas en backup iOS	33
Ilustración 2.- Esquema de la base de datos Biz.sqlite.....	36
Ilustración 3 Esquema de la tabla ZWABIZPROFILEDATA	37
Ilustración 4 Esquema de la tabla AWABIZVERIFIEDNAME	38
Ilustración 5 Esquema de la base de datos Backedupvaluekey.sqlite	39
Ilustración 6 Esquma de la base de datos CallHistory.sqlite.....	40
Ilustración 7 Esquema de la base de datos ContactsV2.sqlite.....	43
Ilustración 8 Esquema de la base de datos ChatStorage.sqlite	46
Ilustración 9 Estructura de directorios en terminal Android	64
Ilustración 10 Esquema de la base de datos axolotl.db	67
Ilustración 11 Estructura de la base de datos chatsettings.db	68
Ilustración 12 Esquema de la base de datos companion_devices.db.....	69
Ilustración 13 Esquema de la base de datos hsmpacks.db	69
Ilustración 14 Esquema de la base de datos Location.db	70
Ilustración 15 Esquema de la base de datos media.db.....	72
Ilustración 16 Esquema de la tabla awaymessages	73
Ilustración 17 Esquema de la tabla call_log	74
Ilustración 18 Esquema de la tabla call_log_participant_v2.....	75
Ilustración 19 Esquema de la tabla chat	77
Ilustración 20 Esquema de la tabla chat_list.....	80
Ilustración 21 Esquema de la tabla conversion_tuples.....	84
Ilustración 22 Esquema de la tabla deletec_chat_box	84
Ilustración 23 Esquema de la tabla frequent	85
Ilustración 24 Esquema de la tabla frequents.....	85
Ilustración 25 Esquema de la tabla group_notification_version	86
Ilustración 26 Esquema de la tabla group_participant_device.....	86
Ilustración 27 Esquema de la tabla group_participant_user	87
Ilustración 28 Esquema de la tabla group_participants.....	87
Ilustración 29 Esquema de la tabla group_participant_history	88
Ilustración 30 Esquema de la tabla jid	89

Ilustración 31 Esquema de la tabla keywords	90
Ilustración 32 Esquema de la tabla labelled_jid.....	90
Ilustración 33 Esquema de la tabla labelled_jids	91
Ilustración 34 Esquema de la tabla labelled_messages	91
Ilustración 35 Esquema de la tabla labelled_messages_fts	91
Ilustración 36 Esquema de la tabla labelled_fts_content	92
Ilustración 37 Esquema de la tabla labelled_fts_segdir.....	92
Ilustración 38 Esquema de la tabla messages_fts_segments	92
Ilustración 39 Esquema de la tabla labels	93
Ilustración 40 Esquema de la tabla hash_thumbnail	93
Ilustración 41 Esquema de la tabla media_refs	93
Ilustración 42Esquema de la tabla message	94
Ilustración 43 Esquema de la tabla message_ephemeral.....	95
Ilustración 44 Esquema de la tabla message_ephemeral_setting.....	95
Ilustración 45 Esquema de la tabla message_external_ad_content.....	96
Ilustración 46.....	96
Ilustración 47 Esquema de la tabla message_ftsv2.....	97
Ilustración 48 Esquema de la tabla message_ftsv2_content.....	98
Ilustración 49 Esquema de la tabla message_ftsv2_docszie.....	98
Ilustración 50 Esquema de la tabla message_ftv2_segdir	99
Ilustración 51 Esquema de la tabla message_ftv2_segments.....	99
Ilustración 52 Esquema de la tabla message_ftv2_stats	100
Ilustración 53 Esquema de la tabla message_future	100
Ilustración 54 Esquema de la tabla message_group_invite	100
Ilustración 55 Esquema de la tabla message_link.....	101
Ilustración 56 Esquema de la tabla message_location.....	101
Ilustración 57 Esquema de la tabla message_media	102
Ilustración 58 Esquema de la tabla message_media_interactive_annotation	106
Ilustración 59 Esquema de la tabla message_media_annotation_vertex	106
Ilustración 60 Esquema de la tabla message_media_vcard_count	107
Ilustración 61 Esquema de la tabla message_mentions	107
Ilustración 62 Esquema de la tabla message_orphaned_edit.....	107
Ilustración 63 Esquema de la tabla message_payments.....	108
Ilustración 64 Esquema de la tabla message_payment_status_update	108

Ilustración 65 Esquema de la tabla message_payment_transaction_reminder.....	109
Ilustración 66 Esquema de la tabla message_product.....	109
Ilustración 67 Esquema de la tabla message_quoted.....	110
Ilustración 68 Esquema de la tabla message_quoted_group_invite	110
Ilustración 69 Esquema de la tabla message_quoted_group_invite_legacy	111
Ilustración 70 Esquema de la tabla message_location	111
Ilustración 71 Esquema de la tabla message_media	112
Ilustración 72 Esquema de la tabla message_mentions	112
Ilustración 73 Esquema de la tabla message_quoted_product.....	113
Ilustración 74 Esquema de la tabla message_quoted_text	113
Ilustración 75 Esquema de la tabla message_quoted_vcard.....	114
Ilustración 76 Esquema de la tabla message_revoked	114
Ilustración 77 Esquema de la tabla message_send_count	114
Ilustración 78 Esquema de la tabla message_streaming_sidecar	115
Ilustración 79 Esquema de la tabla message_system.....	115
Ilustración 80 Esquema de la tabla message_system_block_contact	116
Ilustración 81 Esquema de la tabla message_system_chat_participant	116
Ilustración 82 Esquema de la tabla message_system_device_change.....	116
Ilustración 83 Esquema de la tabla message_system_ephemeral_setting_not_applied....	117
Ilustración 84 Esquema de la tabla message_system_group	117
Ilustración 85 Esquema de la tabla message_system_number_change	117
Ilustración 86 Esquema de la tabla message_system_photo_change	118
Ilustración 87 Esquema de la tabla message_system_value_change.....	118
Ilustración 88 Esquema de la tabla message_template.....	118
Ilustración 89 Esquema de la tabla message_template_button	119
Ilustración 90 Esquema de la tabla message_template_quoted.....	119
Ilustración 91 Esquema de la tabla message_text	120
Ilustración 92 Esquema de la tabla message_thumbnail.....	120
Ilustración 93 Esquema de la tabla message_thumbnails	120
Ilustración 94 Esquema de la tabla message_vcard	121
Ilustración 95 Esquema de la tabla message_vcard_jid	122
Ilustración 96 Esquema de la tabla messages.....	124

Ilustración 97 Esquema de la tabla messages_dehydrated_hsm	131
Ilustración 98 Esquema de la tabla messages_fts.....	131
Ilustración 99 Esquema de la tabla messages_fts_content	131
Ilustración 100 Esquema de la tabla messages_fts_segdir	132
Ilustración 101 Esquema de la tabla messages_fts_segments	132
Ilustración 102 Esquema de la tabla messages_hydrated_four_row_template	133
Ilustración 103 Esquema de la tabla messages_link	133
Ilustración 104 Esquema de la tabla messages_quotes.....	134
Ilustración 105 Esquema de la tabla messages_vcard	135
Ilustración 106 Esquema de la tabla messages_vcards_jid.....	136
Ilustración 107 Esquema de la tabla missed_call_log_participant	136
Ilustración 108 Esquema de la tabla missed_call_logs	137
Ilustración 109 Esquema de la tabla pay_transaction	138
Ilustración 110 Esquema de la tabla pay_transactions.....	139
Ilustración 111 Esquema de la tabla props	139
Ilustración 112 Esquema de la tabla quick_replies	140
Ilustración 113 Esquema de la tabla quick_reply_attachments	140
Ilustración 114 Esquema de la tabla quick_reply_keywords	141
Ilustración 115 Esquema de la tabla quick_reply_usage	141
Ilustración 116 Esquema de la tabla quoted_message_product	141
Ilustración 117 Esquema de la tabla receipt_device.....	142
Ilustración 118 Esquema de la tabla receipt_orphaned	142
Ilustración 119 Esquema de la tabla receipt_user	142
Ilustración 120 Esquema de la tabla receipts	143
Ilustración 121 Esquema de la tabla status.....	144
Ilustración 122 Esquema de la tabla status_list.....	144
Ilustración 123 Esquema de la tabla user_device.....	145
Ilustración 124 Esquema de la tabla user_device_info.....	145
Ilustración 125 Esquema de la tabla contacts.....	145
Ilustración 126 Esquema de la tabla methods	146
Ilustración 127 Esquema de la tabla tmp_transactions.....	146
Ilustración 128 Esquema de la base de datos stickers.db.....	147
Ilustración 129 Esquema de la base de datos wa_contacts.db	148
Ilustración 130 Esquema de la tabla system_contacts_version_table	148

Ilustración 131 Esquema de la tabla wa_biz_profiles.....	149
Ilustración 132 Esquema de la tabla wa_biz_profiles_categories	149
Ilustración 133 Esquema de la tabla wa_biz_profiles_hours.....	150
Ilustración 134 Esquema de la tabla wa_biz_profiles_websites.....	150
Ilustración 135 Esquema de la tabla wa_block_list	150
Ilustración 136 Esquema de la tabla wa_contact_capabilities	151
Ilustración 137 Esquema de la tabla wa_contact_storage_usage	151
Ilustración 138 Esquema de la tabla wa_contacts.....	152
Ilustración 139 Contenido de la tabla wa_contacts.....	155
Ilustración 140 Esquema de la tabla wa_group_add_black_list.....	155
Ilustración 141 Esquema de la tabla wa_group_admin_settings	156
Ilustración 142 Esquema de la tabla wa_group_descriptions	156
Ilustración 143 Esquema de la tabla wa_last_entry_point.....	156
Ilustración 144 Esquema de la tabla wa_vnames	157
Ilustración 145 Esquema de la tabla wa_vnames_localized	158
Ilustración 146 Esquema de la base de datos web_sessions.sqlite	158
Ilustración 147 Esquema de la tabla android_metadata	158
Ilustración 148 Esquema de la tabla sessions	159
Ilustración 149 Contenido de las tablas ZWAPROFILEPUSHNAME Y ZWAPROFILEPICTUREITEM	164
Ilustración 150 Contenido de la tabla wa_contacts.....	165
Ilustración 151 Información de llamadas en whatsapp.log en android.....	173
Ilustración 152 Captura de registro de la tabla chatlist con mensaje de una lista de distribución	176
Ilustración 153 Captura de registro de la tabla ZWACHATSESSION con mensaje de una lista de distribución	176
Ilustración 154 Solicitud en el log de la lista de bloqueados	177
Ilustración 155 Contenido de la tabla message_ftsv2_content.....	179
Ilustración 156 Contenido de la tabla ZWAMESSAGE con mensajes enviados vía whatsappweb	180

1 INTRODUCCIÓN

WhatsApp es una red social con más de 2.000 millones de usuarios (Dos mil millones de usuarios - Conectando al mundo de manera privada, 12) , que actualmente forma parte del día a día tanto en lo que se refiere a actividades particulares como empresariales. Por lo tanto, las conversaciones que se mantienen a través de la misma se han convertido en importantes evidencias en una gran cantidad de procedimientos judiciales.

Actualmente, gran cantidad de delitos (Europol, 2019) son realizados a través o con el soporte de la red social WhatsApp: sus capacidades de cifrado la convierten en un medio de comunicación para grupos criminales tanto entre ellos como con sus víctimas. Del mismo modo como red social es usada como medio en casos de acoso, bulling, stalking o simplemente como un medio de comunicación que aporta evidencias en relaciones comerciales que pueden ser analizadas y aportadas como evidencias.

En un procedimiento judicial es fundamental el correcto y meticuloso tratamiento de los artefactos a analizar, preservando su integridad para poder obtener las evidencias que se encuentran en ellos. Del mismo modo, es fundamental conocer el comportamiento del programa y la forma en la que se almacenan los datos. De esta forma se podrá realizar un análisis adecuado y así llegar a conclusiones debidamente documentadas que puedan ser aportadas como evidencias en un proceso judicial.

Con la red social WhatsApp, existe una dificultad relacionada con todo este procedimiento de análisis y es que, por un lado, se trata de un producto de una empresa privada que no facilita información sobre el mismo y que, por otro lado, está en constante evolución lo que hace que sea necesario una revisión continua cuando una nueva funcionalidad es publicada para poder sacar partido a las conclusiones que se puedan extraer de la misma.

Es por ello necesario el análisis de la información que contiene, puede aportar muchísimos datos que van mucho más allá del propio contenido del mensaje: información como la autoría del mensaje, fechas de envío y recepción, geolocalización, receptores, dispositivos desde los que se ha enviado, etc.



2 ESTADO DE LA CUESTIÓN

De cara a entender el estado del arte en el análisis forense de WhatsApp, en primer lugar, es importante entender cuál es el entorno tecnológico en el cual se encuentra la red social WhatsApp.

WhatsApp es una red social que utiliza una aplicación de mensajería basada en el protocolo XMPP (XMPP, Fecha no reseñada). No obstante, no se trata del protocolo original inventado por D. Jeremie Miller en 1998 sino una versión modificada denominada FunXMPP, (Internet Engineering Task Force (IETF) , 2017) que basándose en el anterior protocolo descrito en las RFCs 6120 (Internet Engineering Task Force (IETF) , 2012), 6121 (Extensible Messaging and Presence Protocol (XMPP):Instant Messaging and Presence, 2011)y 7622 (Internet Engineering Task Force (IETF) , 2015), utiliza XML como sintaxis.

Actualmente WhatsApp se ofrece principalmente en dos plataformas terminales con sistema operativo IOS (fabricados por Apple) y terminales con sistema operativo Android (de distintos fabricantes), dando soporte a distintos tipos de formatos (teléfonos móviles, phablets, tabletas). Adicionalmente WhatsApp ha creado un nuevo modelo de entorno compatible con ambas plataformas que es el WhatsApp Web, consiste en un cliente a ejecutar en un ordenador con sistema operativo Windows, IOS o Linux que está enlazado con un terminal concreto a través de un token y que permite el uso de la aplicación sobre estas plataformas. Y como nueva funcionalidad, WhatsApp está anunciando la posibilidad de contar con una cuenta de WhatsApp instalada sobre distintos terminales (Fernández, Samuel, 2020) (aunque todavía no está disponible en el momento de la redacción del presente trabajo)

2.1 EXTRACCIÓN DE LA BASE DE DATOS DE WHATSAPP

Cuando hablamos de realizar un análisis forense sobre un terminal en cualquiera de los mencionados entornos, podemos encontrar dos situaciones distintas. Por un lado, tendríamos un análisis que podríamos denominar consensuado, en el cual el profesional que debe desarrollar el análisis cuenta con el permiso del titular de la cuenta para poder realizar el mismo, por lo tanto, se dispone con todas las claves de acceso al terminal y datos de la cuenta de WhatsApp para poder recuperar información. El otro modelo sería el no consensuado donde, a partir de una orden judicial, por ejemplo, se nos solicita el análisis de un terminal para el cual no se dispone de acceso al mismo (teléfono desbloqueado, etc.). La forma de ejecutar el análisis difiere enormemente de un modelo a otro.

De una forma o de otra podríamos diferenciar tres entornos distintos que condicionan el análisis.

1.- Análisis pericial de WhatsApp en un entorno Android

2.- Análisis pericial de WhatsApp en un entorno IOS

3.- Análisis pericial de WhatsApp en un entorno WhatsApp Web

Un dispositivo móvil no deja de ser una caja fuerte que protege la información que contiene, de esta forma en un dispositivo existe información pública, visible para todos los usuarios e información protegida, almacenada en la memoria interna del dispositivo pero que sólo es visible a través de aplicaciones o incluso directamente no es accesible.

Para garantizar la privacidad y confidencialidad de los usuarios, y para dar cumplimiento a la normativa de protección de datos, la información de la aplicación WhatsApp (mensajes, imágenes, configuración, etc.), se encuentra protegida en la memoria interna del dispositivo.

Para poder peritar una conversación de WhatsApp es necesario acceder a las conversaciones o directamente a los ficheros que las contienen almacenadas dentro del dispositivo. Para ello se pueden utilizar las técnicas que se indican a continuación.

1.- Peritación de las conversaciones directamente obteniendo capturas de las mismas.

En España, la validez de una evidencia depende exclusivamente del criterio del Juez que presida la sala en la que se desarrolla el procedimiento judicial, por lo que, aunque este método es el que menor fiabilidad aporta a la evidencia podría ser válido. Sería al menos necesario verificar que el dispositivo no ha sufrido una rotura de seguridad y que la memoria interna del dispositivo sigue siendo privada. Como evidencia se presentarían capturas de pantalla para su consideración en el procedimiento.

2.- Extracción de base de datos a partir de Token.

Actualmente WhatsApp permite la instalación para una cuenta de un cliente en un ordenador personal, el anteriormente mencionado WhatsApp Web. Este programa tiene como característica que no guarda en local una copia de la base de datos de WhatsApp, sino que enlaza con el terminal que está asociado a la cuenta y extrae los mensajes que muestra por pantalla. El enlace se realiza a través de un token que es validado por los servidores de WhatsApp y permite la operación. Actualmente numerosas herramientas forenses permiten utilizar este método para, a partir del token de autenticación, simular ser una aplicación WhatsApp Web y extraer los mensajes del dispositivo para su análisis y peritación. Este método que actualmente es el más sencillo y más seguro, tiene como inconveniente que no se accede al artefacto original, sino que se genera una copia parcial del mismo. De esta forma no todos los mensajes de la base de datos tienen por qué estar en la copia y además otros elementos valiosos que pueden ser objeto de análisis como el espacio dónde encontrar mensajes borrados no estaría accesible.

3.- Extracción de la base de datos del terminal.

Este método es el que ofrece una mayor oportunidad para el análisis pericial ya que a través del mismo, se accede a toda la información original que puede ser objeto de análisis. El inconveniente está en que esta información está protegida, por lo que para acceder al contenido de la misma es necesario evadir las medidas de seguridad del terminal móvil. Hacer lo que se denomina “root” o “jailbreak” al terminal. Esto puede entrañar bastante dificultad y riesgo debido a que puede afectar al funcionamiento e integridad del dispositivo.

No obstante, podemos hablar de forma distinta de las dos arquitecturas existentes.

1.- Arquitectura iOS. En este caso, cuando estamos realizando lo que antes denominamos un análisis consensuado, existe un método sencillo de acceder al artefacto para su análisis. En dispositivos iOS por su mayor seguridad no contienen en su interior una base de datos cifrada por lo cual es posible, si se dispone de las claves del terminal, utilizar el programa iTunes de Apple para realizar una copia de seguridad del dispositivo y a partir del mismo poder extraer la base de datos de WhatsApp para su análisis. En caso de análisis no consensuados puede ser complicado y a veces incluso imposible acceder a la base de datos ya que el dispositivo está cifrado. También podría extraerse una copia de un terminal al que previamente se le ha roto la seguridad ejecutando un “jailbreak” pero es más arriesgado ya que en este proceso podrían destruirse las evidencias.

2.- Respecto a una arquitectura Android, el sistema permite obtener una copia de seguridad de la base de datos, bien sea directamente del terminal o de la copia de seguridad que se almacena en la nube asociada a la cuenta Google asociada a WhatsApp. El problema está en que en dispositivos Android, la base de datos está cifrada habiendo incrementado la robustez del cifrado a lo largo de los años. Aquí existen varios métodos para extraer la base de datos. Para el caso de un análisis consensuado, se puede acceder a la copia de seguridad de la base de datos y utilizando programas comerciales utilizar el token para acceder a la base de datos y extraer los mensajes. También es posible realizar un downgrade de la versión de WhatsApp instalada hasta una versión que permita la extracción de la base de datos sin necesidad de contar la contraseña. Para el caso de un análisis no consensuado es necesario evadir las medidas de seguridad del dispositivo móvil para acceder a la base de datos. Posteriormente en la ruta `/data/data/files/com.whatsapp/key` o `/data/data/com.whatsapp` dependiendo del dispositivo se encuentra un fichero denominado key, que contiene la clave que nos permite descifrar la base de datos.

Para acceder al terminal se debe acceder utilizar ADB (Android Debug Bridge) (Calvo, 2019). Esta herramienta permite extraer cualquier contenido del terminal, sin embargo, es necesario que el terminal se encuentre en modo root, lo que implica evadir las medidas de seguridad. El poner el terminal en modo root es una operación arriesgada ya que, puede alterar o destruir información del terminal o incluso bloquearlo y en segundo lugar tal en determinados casos este proceso puede no ser viable.

No obstante, desde el punto de vista pericial, el acceder a estos contenidos es lo más adecuado ya que de esta forma tenemos acceso a toda la información del aplicativo pudiendo realizar cualquier análisis que sea requerido.

Existe un último método de extracción, que consiste en un análisis no consensuado para el que no se dispone de acceso a la memoria interna del terminal. Este método tiene más aplicaciones forenses que de investigación. Extrayendo la tarjeta SIM e instalándola en otro dispositivo desbloqueado existen herramientas que pueden, para esa tarjeta SIM obtener un token de WhatsApp que permita configurar la cuenta en un nuevo terminal de forma que no se obtiene información de lo existente en el teléfono, pero sí de cualquier nuevo mensaje que se reciba, los contactos, grupos y sus miembros o las llamadas no contestadas.

2.2 ESTADO DEL ARTE EN EXTRACCIÓN Y ANÁLISIS DE WHATSAPP

Tal y como comentamos anteriormente existen diversos métodos para acceder al contenido de un dispositivo móvil, estos métodos son implementados por diversos fabricantes en sus desarrollos ofreciendo una diversa gama de productos que nos permiten extraer la información para realizar el análisis. De esta forma, en el proceso de realización de este trabajo se han analizado estas herramientas como líderes de su sector para el Análisis de WhatsApp entre las cuales debemos destacar y agradecer la atención de Oxygen y MobilEdit que han tenido la cortesía de facilitar una licencia de Demo al redactor del presente trabajo para poder evaluarlas y contar con material para la realización de este trabajo.

Para alguna de ellas no ha sido posible obtener suficiente información para completar la tabla.

Empresa	Producto	Extracción Física (root)	Descifrado de BBDD	Extracción por Token Cloud	Extracción por Token PC	Extracción de backup local (iTunes/Android)	Extracción por WhatsApp Cloud
Celebrate	Celebrate touch	X	X	X	X	X	
	Celebrate Udef Ultimate (Celebrate, Fecha no reseñada)	X	X	X	X	X	
Guidance Software	Encase Forensics (Guidance Software, Fecha no reseñada)						
Oxygen	Oxygen Detective (Oxygen Forensics, Fecha no reseñada)	X	X	X	X	X	X
MobilEdit	MobilEdit Forensics (MobilEdit, Fecha no reseñada)	X	X	X	X	X	
Elcomsoft	Elcomsoft Mobile Forensic Bundle (Elcomsoft, Fecha no reseñada)	X	X	X	X	X	
	Elcomsoft Explorer for WhatsApp (Elcomsoft, Fecha no reseñada)			X	X	X	

Empresa	Producto	Extracción Física (root)	Descifrado de BBDD	Extracción por Token Cloud	Extracción por Token PC	Extracción de backup local (iTunes/Android)	Extracción por WhatsApp Cloud
Magnet forensics	Magnet Axiom (Magnet forensics, Fecha no reseñada)	X	X	X	X	X	

Tabla 1 Comparativa del estado del Arte en extracción y análisis de WhatsApp

Es importante destacar que la anterior tabla muestra únicamente funcionalidades asociadas a la captura y análisis de artefactos relacionados con la red social WhatsApp sin entrar en la calidad o eficiencia de las mismas. Es decir, cada empresa y su software utilizarán métodos y algoritmos distintos por ejemplo para romper la seguridad de teléfonos móviles y de esta forma acceder a su contenido, no se entra en la anterior tabla a evaluar la calidad o eficiencia de estos métodos y algoritmos, sino que muestra la existencia de los mismos.

3 DESCRIPCIÓN DEL PROBLEMA

El problema identificado tras el análisis del estado de la cuestión es que, pese a que existen numerosas herramientas comerciales que permiten la extracción de información de dispositivos móviles y la obtención y descifrado de las bases de datos de WhatsApp, no se ha localizado un estudio académico que analice el comportamiento de la información dentro de este modelo de datos.

Por un lado, la constante evolución del producto que, al ser un producto propietario, no documenta sus cambios a nivel de diseño del modelo de datos. Además de la creación de nuevas funcionalidades y la liberación de nuevas versiones casi cada mes hace que la información publicada sea en su mayor parte obsoleta e incompleta. Por otro lado, los productos comerciales existentes extraen la información, pero dejan en manos del investigador el estudio del comportamiento de la misma quedando muchas preguntas que sólo pueden ser respondidas a través de la realización de un trabajo de campo que nos proporcione la información necesaria para poder documentar este comportamiento y aplicarlo a la práctica forense. Este trabajo pretender responder preguntas como ¿Es posible conocer analizando el modelo de datos si un mensaje se envió desde un terminal o a través de la aplicación web? ¿Cuándo un usuario está bloqueado queda rastro en la base de datos de los intentos de envío y recepción? ¿y en el dispositivo destinatario de la comunicación? No tienen respuesta a través de la actual oferta de herramientas forenses. La respuesta a estas y otras cuestiones pueden esclarecer diferentes sucesos en la práctica forense, entre los que destacan si alguien desde un ordenador desatendido pudo suplantar al usuario sin tener acceso a su dispositivo móvil, o si alguien pudo fingir el envío de un mensaje a un usuario que no podía recibirla, requieren del análisis del modelo de datos y del comportamiento de la aplicación para la obtención de conclusiones documentadas y que puedan ser aportadas como evidencias a un procedimiento judicial. Realmente las posibilidades son muy numerosas y merece la pena la realización del trabajo.

4 SOLUCIÓN PROPUESTA

4.1 OBJETIVOS

El objetivo del presente trabajo de fin de master es realizar un análisis completo del proceso de peritación de una base de datos de WhatsApp de una cuenta de usuario particular. Analizar y describir el proceso de captura y preservación de las evidencias, detallando incluso el estado del arte en productos comerciales que facilitan esta tarea. De cara a completar el trabajo se tendrán en cuenta otros artefactos que directamente completan la información necesaria para la peritación.

A lo largo del desarrollo del presente trabajo, se realizará un análisis del modelo de datos de WhatsApp describiendo la estructura y contenido del mismo, y adicionalmente se realizará un análisis del comportamiento de la aplicación de WhatsApp y su reflejo en el modelo de datos, todo ello teniendo en cuenta su aplicación a un proceso pericial. Se estudiará las dos plataformas existentes más populares: IOS y Android, mostrando las diferencias entre ambas tanto en lo que se refiere al modelo de datos, así como la forma en la que se registra la información. El trabajo analiza los tipos de comunicación existentes en una cuenta de WhatsApp, documentando los distintos estados por los que pasa un mensaje cuando se envía o la forma en la que se gestionan los distintos contenidos enviados.

4.2 METODOLOGÍA

En el apartado anterior se han mostrado distintos métodos para la obtención de evidencias de cara a la peritación de artefactos de la red social WhatsApp. Aunque estos métodos son apropiados (y en algunos casos no hay otra opción para acceder a la información) para un análisis pericial real, en el caso que nos ocupa se persigue realizar un trabajo de investigación. Por lo tanto, es importante garantizar que los artefactos se mantienen íntegros y no son alterados ni modificados de ninguna forma a través de un proceso de root o similar. De esta forma se garantiza que cualquier otro investigador puede seguir el mismo procedimiento para verificar los resultados o incluso para ampliar la investigación con nuevas funcionalidades que se publique.

En el análisis se ha podido observar que el entorno WhatsApp Web no es adecuado para realizar el análisis ya que este entorno no guarda copia de la base de datos objeto del mismo. Por ese motivo se descarta, aunque dicho entorno será utilizado en alguno de los casos de estudio.

Respecto a los dos entornos restantes contamos con dos tipos de plataformas, la plataforma Android y la plataforma iOS. Es importante acceder a la base de datos original y completa por lo que el acceso al dispositivo es necesario. En esta línea en el caso de iOS se cuenta con acceso a dos terminales independientes que pueden ser utilizados para el estudio y cuyo contenido se puede extraer de forma íntegra a través del análisis de la copia de seguridad generada con el programa iTunes.

Un caso más complejo es el de la plataforma Android, la base de datos se encuentra cifrada en el terminal, tal y como se comentaba en el apartado anterior. Es necesario romper la seguridad del terminal, esto implica que el contenido del terminal puede ser alterado y por lo tanto el estudio podría ser cuestionado. Por ello se ha optado por crear un terminal adhoc. A partir de una máquina virtual en entorno VirtualBox, se proceda a realizar una instalación de un sistema operativo Android en dos máquinas independientes. En estas máquinas se dan de alta dos aplicaciones de WhatsApp asociadas a dos líneas de teléfono ubicadas en dos teléfonos móviles (que sólo son necesarios para la creación de la cuenta). A partir de este momento y accediendo a través de la Wifi del ordenador en el que se encuentran las máquinas se puede operar con WhatsApp como con cualquier terminal estándar. Finalmente, el disco duro virtual es convertido de formato .vdi a formato .img utilizando la utilidad vboxmanage.exe para posteriormente ser cargada a través del programa forense Autopsy y de esta forma extraer la base de datos de forma íntegra y sin modificaciones ni alteraciones de ningún tipo.

Con ello, tal y como se mencionaba, se puede realizar un estudio y un análisis contando con unas evidencias de partida íntegras y sin alteraciones que puedan modificar o tergiversar los resultados.

En la realización del análisis se ha podido observar que en el modelo de datos de ambas plataformas existen muchas tablas vacías, a través del nombre de la tabla se puede inferir que algunas de ellas están relacionadas con funcionalidades futuras que actualmente están anunciadas, pero no implantadas a nivel mundial (como el pago a través de WhatsApp que únicamente está disponible en modo Beta en India). Por otro lado, se han encontrado un gran número de tablas de bases de datos vacías. El investigador es de la opinión que esto es debido a mantener la compatibilidad entre versiones y/o terminales (no tiene mucho sentido que en Android exista una tabla message y otra tabla messages estando la primera vacía y conteniendo una estructura similar de contenidos). Esto ha podido constatarse en el entorno iPhone en el cual la aplicación montada en un terminal iPhone 5 con versión iOS 10.3.4 frente a un segundo

terminal iPhone 11 con versión iOS 13.6.1. En el primero se ha podido constatar que los contactos se encuentran recogidos en una tabla concreta tal y como se verá más adelante mientras que en iPhone 11 se encuentran en una tabla distinta siendo la misma versión de la aplicación.

La aplicación analizada para dispositivos Apple es la versión IOS 2.20.92, la versión analizada para Android es la 2.20.192.17

5 PRUEBAS Y VALIDACIÓN

5.1 ANÁLISIS DEL MODELO DE DATOS DE WHATSAPP EN LA PLATAFORMA IOS.

A partir de uno de los terminales de los que se dispone se procede a generar un backup con iTunes que es extraído utilizando las aplicaciones Oxygen Forensics y MobilEdit. Tras la extracción se puede constatar la ubicación de los ficheros. En el dispositivo se encuentra instalada la versión de WhatsApp 2.20.90 publicada el 20 de agosto de 2020.

5.1.1 ESTRUCTURA DE CARPETAS Y UBICACIÓN DE ARCHIVOS

La ruta de acceso a los ficheros objeto de análisis es /pr00ivate/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared. En dicha carpeta se encuentran los siguientes ficheros y carpetas.

Nombre	Fecha de modificación	Tipo
Biz	10/01/2020 19:45	Carpeta de archivos
FieldStats	24/03/2019 11:29	Carpeta de archivos
FieldStats2	30/09/2019 6:18	Carpeta de archivos
Library	24/03/2019 11:29	Carpeta de archivos
Media	01/04/2019 11:23	Carpeta de archivos
Message	28/07/2020 17:59	Carpeta de archivos
stickers	24/03/2019 11:30	Carpeta de archivos
BackedUpKeyValue.sqlite	03/08/2020 20:25	Archivo SQLITE
CallHistory.sqlite	03/08/2020 20:13	Archivo SQLITE
calls.backup.log	03/08/2020 20:11	Documento de te...
calls.log	03/08/2020 20:11	Documento de te...
ChatStorage.sqlite	03/08/2020 20:25	Archivo SQLITE
consumer_version	24/03/2019 11:29	Archivo
ContactsV2.sqlite	03/08/2020 20:25	Archivo SQLITE
current_wallpaper.jpg	24/03/2019 11:29	Archivo JPG
emoji.sqlite	28/07/2020 17:08	Archivo SQLITE
Ranking.sqlite	03/08/2020 20:25	Archivo SQLITE
status.blacklist	03/08/2020 20:11	Archivo BLACKLIST
status.whitelist	03/08/2020 20:11	Archivo WHITELIST
Sticker.sqlite	03/08/2020 20:25	Archivo SQLITE

Ilustración 1 Estructura de carpetas en backup iOS

El contenido de la estructura es el siguiente.

Nombre	Tipo	Descripción
Biz	Carpeta	Contiene el fichero biz.sqlite. Esta base de datos contiene información relacionada con cuentas Bussiness. WhatsApp Bussiness es una aplicación independiente que fue liberada para entornos Android el 18 de enero de 2018 (WhatsApp, 2018), para entornos iOS fue publicada el 4 de abril de 2019 (WhatsApp, 2019)
FieldStats	Carpeta	Carpeta que contiene una segunda carpeta de nombre WhatsApp y en su interior un fichero de nombre wam.wam cuyo uso es desconocido. A través de un editor hexadecimal se puede observar que contiene

		información como el modelo del terminal utilizado o el número de versión de la aplicación.
FieldStats2	Carpeta	Carpeta con la misma estructura que la anterior, tiene el mismo contenido y se ha podido constatar que el fichero que contiene, al menos en la captura analizada, tiene el mismo contenido.
Library	Carpeta	Carpeta que contiene a su vez una carpeta denominada Preferences en la que se encuentra el fichero group.net.whatsapp.WhatsApp.shared.plist, se ha podido observar que en este fichero se encuentra información de configuración de la cuenta como el estado definido por el usuario para WhatsApp, versión de la aplicación. Es el fichero con las preferencias de usuario.
Media	Carpeta	Carpeta que contiene a su vez la carpeta Profile y que a su vez contiene thumbnails y ficheros que son o han sido usados por el titular de la cuenta como imagen de estado de su cuenta.
Messages	Carpeta	Carpeta que contiene un conjunto de carpetas con los ficheros de audio, vídeo y fotografías de los distintos chats, incluyendo las imágenes de estado de los distintos contactos.
Stickers	Carpeta	Carpeta que contiene una carpeta con ficheros de stickers que pueden ser enviados en los mensajes.
BackedUpKeyValue.sqlite	Fichero	Esta base de datos contiene metainformación sobre la base de datos
BackedUpKeyValue.sqlite-shm	Fichero	Fichero temporal de la base de datos SQLite
BackedUpKeyValue.sqlite-wal	Fichero	Fichero caché de la base de datos SQLite
Calls.backup.log	Fichero	Fichero plist que contiene el backup del log de llamadas
Calls.log	Fichero	Fichero plist que contiene el log de llamadas de WhatsApp
ChatStorage.sqlite	Fichero	Base de datos con los mensajes enviados y recibidos por WhatsApp
Consumer_version	Fichero	Fichero que contiene el número de versión de la aplicación

ContactsV2.sqlite	Fichero	Base de datos que contiene la información de los contactos de la aplicación
Current_wallpaper.jpg	Fichero	Imagen que representa el fondo que se mostrará en la aplicación para el usuario
Emoji.sqlite	Fichero	Base de datos de emojis que se pueden usar en la aplicación
Ranking.sqlite	Fichero	Se desconoce el uso de esta base de datos por parte de WhatsApp
Ranking.sqlite-shm	Fichero	Fichero temporal de la base de datos anterior
Ranking.sqlite-wal	Fichero	Fichero caché de la base de datos anterior
Status.blacklist	Fichero	Fichero plist que contiene la blacklist de la aplicación
Status.whitelist	Fichero	Fichero plist que contiene la whitelist de la aplicación
Sticker.sqlite	Fichero	Base de datos de stickers de WhatsApp

Tabla 2 Contenido de la estructura de carpetas de backup iOS

5.1.2 ESTRUCTURA DE LA BASE DE DATOS BIZ.SQLITE

De esta base de datos se muestra el esquema. Se ha podido verificar que Biz.sqlite contiene información sobre los contactos que tiene el usuario que están dados de alta como empresa (y que por lo tanto usan la aplicación WhatsApp Business). Adicionalmente hay que indicar que esta base de datos sólo existe para terminales con las últimas versiones de sistema operativo (se ha verificado para versión 13, y se ha comprobado su ausencia en versión 12). A continuación, se muestra el esquema de esta base de datos.

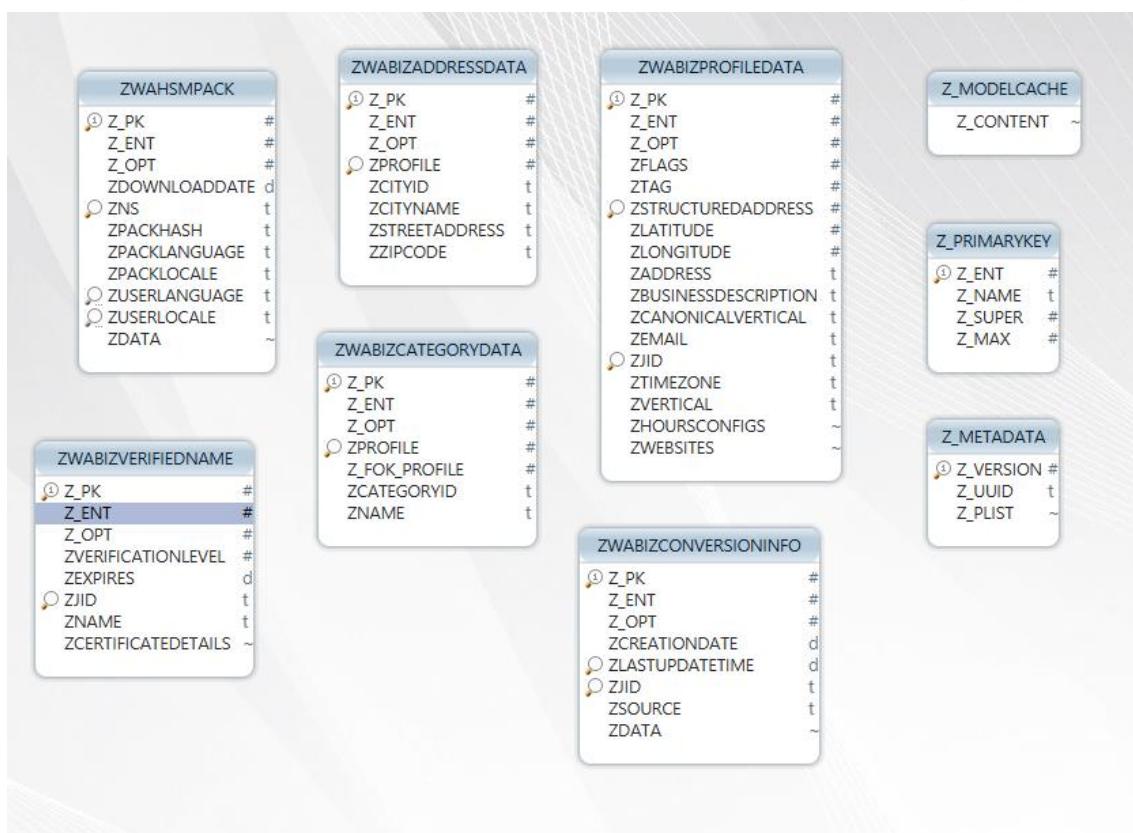


Ilustración 2.- Esquema de las base de datos *Biz.sqlite*

Las tablas ZWABIZADDRESSDATA, ZWABIZCATEGORYDATA, ZWABIZADDRESSINFO, ZWABIZCONVERSIONINFO contiene distinta información sobre el negocio, no obstante, en las bases de datos analizadas se ha podido constatar que dichas tablas están vacías. La información existente se encuentra en ZWABIZPROFILEDATA y AWABIZVERIFIEDNAME. Estas dos tablas guardan información sobre el contacto y el negocio que regenta. Se muestra a continuación el detalle del contenido de las tablas.

Edit Table in Schema Default

Table ... ? ZWABIZPROFILEDDATA #3986c1

Descri... ?

Columns Primary Key / Unique / Indexes Foreign Keys Check Constraints Options

Visible	Name	Details	Description
<input checked="" type="checkbox"/>	Z_PK	integer	
<input checked="" type="checkbox"/>	-- Z_ENT	integer	
<input checked="" type="checkbox"/>	-- Z_OPT	integer	
<input checked="" type="checkbox"/>	-- ZFLAGS	integer	
<input checked="" type="checkbox"/>	-- ZTAG	integer	
<input checked="" type="checkbox"/>	ZSTRUCTUREDADDRESS	integer	
<input checked="" type="checkbox"/>	-- ZLATITUDE	float	
<input checked="" type="checkbox"/>	-- ZLONGITUDE	float	
<input checked="" type="checkbox"/>	-- ZADDRESS	varchar	
<input checked="" type="checkbox"/>	-- ZBUSINESSDESCRIPTION	varchar	
<input checked="" type="checkbox"/>	-- ZCANONICALVERTICAL	varchar	
<input checked="" type="checkbox"/>	-- ZEMAIL	varchar	
<input checked="" type="checkbox"/>	ZJID	varchar	
<input checked="" type="checkbox"/>	-- ZTIMEZONE	varchar	
<input checked="" type="checkbox"/>	-- ZVERTICAL	varchar	
<input checked="" type="checkbox"/>	-- ZHOURSCONFIGS	blob	
<input checked="" type="checkbox"/>	-- ZWEBSITES	blob	

Edit Add Drop Up Down Visible Columns

Help Aceptar Cancelar

Ilustración 3 Esquema de la tabla ZWABIZPROFILEDDATA

Esta tabla tiene distintos grados de completitud dependiendo del nivel de detalle con el que contacto haya completado su perfil, entre otras cabe destacar ZTAG que corresponde al

identificador, ZLATITUDE y ZLONGITUDE que son las coordenadas GPS de la ubicación de la empresa, BUSSINESSDESCRIPTION muestra la descripción que el usuario ha incluido de la empresa. ZCANONICALVERTICAL y ZVERTICAL representan la categoría de la empresa (entretenimiento, viajes, etc.) en inglés y español respectivamente. TIMEZONE contiene la zona horaria. ZHOURSCONFIGS y ZWEBSITES son campos binarios que contienen la configuración del horario de apertura de la empresa y la/s página/s web

The screenshot shows the 'Edit Table in Schema Default' dialog box. At the top, there is a search bar with 'ZWABIZVERIFIEDNAME' and a color preview box showing '#3986c1'. Below the search bar are two empty text input fields and a toolbar with icons for copy, paste, and other operations.

Below the toolbar is a navigation bar with tabs: 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and a help icon. The 'Columns X' tab is selected.

The main area is a table titled 'Visi...' with columns for 'Name', 'Details', and 'Description'. The table contains the following data:

Visi...	Name	Details	Description
<input checked="" type="checkbox"/>	Z_PK	integer	
<input checked="" type="checkbox"/>	-- Z_ENT	integer	
<input checked="" type="checkbox"/>	-- Z_OPT	integer	
<input checked="" type="checkbox"/>	-- ZVERIFICATIONLEVEL	integer	
<input checked="" type="checkbox"/>	-- ZEXPIRES	timestamp	
<input checked="" type="checkbox"/>	ZJID	varchar	
<input checked="" type="checkbox"/>	-- ZNAME	varchar	
<input checked="" type="checkbox"/>	-- ZCERTIFICATEDETAILS	blob	

At the bottom of the dialog box are buttons for 'Edit', 'Add', 'Drop', 'Up', 'Down', 'Visible Columns', 'Help', 'Aceptar' (Accept), and 'Cancelar' (Cancel).

Ilustración 4 Esquema de la tabla AWABIZVERIFIEDNAME

En esta tabla caben destacar los siguientes campos: ZVERIFICATIONLEVEL contiene un identificador que representa el nivel de verificación de la cuenta (teléfono, correo electrónico, etc.). ZJID es un campo importante ya que contiene el identificador con la estructura númerodetelefono@s.whatsapp.net por ejemplo 3466666666@whatsapp.net y por último ZNAME contiene el nombre del contacto.

5.1.3 ESTRUCTURA DE LA BASE DE DATOS BACKEDUPVALUEKEY.SQLITE

De esta base de datos no se cuenta con información que pueda resultar de interés para el objeto de este documento por lo que únicamente se muestra el esquema de la misma.



Ilustración 5 Esquema de la base de datos Backedupvaluekey.sqlite

5.1.4 ESTRUCTURA DE LA BASE DE DATOS CALLHISTORY.SQLITE

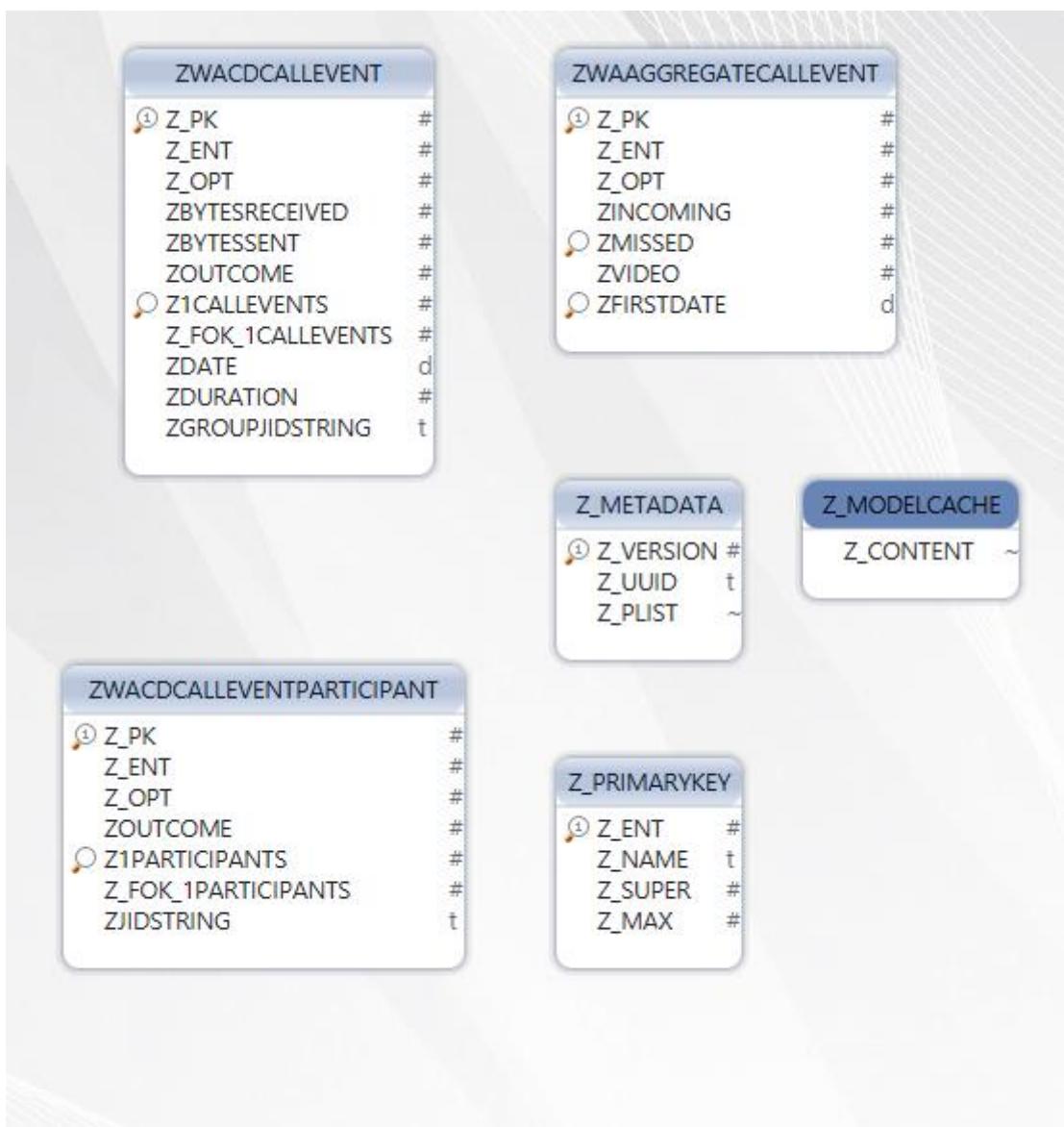


Ilustración 6 Esquema de la base de datos CallHistory.sqlite

No se puede determinar exactamente el objeto de la siguiente base de datos dado que las tablas que contiene están vacías.

Tabla ZWAAGGREGATECALLEVENT

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos
Z_OPT	Entero	Desconocido
ZINCOMING	Entero	
ZMISSED	Entero	
ZVIDEO	Entero	
ZFIRSTDATE	Timestamp	

Tabla 3 Esquema de la tabla ZWAAGREATECALLEVENT

Tabla ZWACDCALLEVENT

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos
Z_OPT	Entero	Desconocido
ZBYTESRECEIVED	Entero	
ZBYTESSENT	Entero	
ZOUTCOME	Entero	
Z1CALLEVENTS	Entero	
Z_FOK_1CALLEVENTS	Entero	
ZDATE	Timestamp	
ZDURATION	Real	
ZGROUPIDSTRING	Texto	

Tabla 4 Esquema de la tabla ZWACDCALLEVENT

Tabla ZWACDCALLEVENTPARTICIPANT

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos
Z_OPT	Entero	Desconocido
ZOUTCOME	Entero	
Z1PARTICIPANTS	Entero	
Z_FOK_1PARTICIPANTS	Entero	
ZGROUPIDSTRING	Texto	

Tabla 5 Esquema de la tabla ZWACDCALLEVENTPARTICIPANT

Las tablas **Z_METADATA**, **Z_MODELCACHE** y **Z_PRIMARYKEY**, contienen información interna de la base de datos sin demasiada relevancia para el análisis forense por ejemplo **Z_PRIMARYKEY** contiene información general sobre la base de datos, el campo que es clave primaria de las principales tablas y el número de registros que contiene (que nos puede aportar cierta información como el número de llamadas, llamadas grupales, etc.

5.1.5 ESTRUCTURA DE LA BASE DE DATOS CONTACTSV2.SQLITE



Ilustración 7 Esquema de la base de datos ContactsV2.sqlite

Esta base de datos presenta distinta información según se trate de un terminal con sistema operativo IOS 12 que sí contiene información y IOS 13 que está vacía. En IOS 12 guarda una lista de todos los contactos del teléfono tengan o no cuenta de WhatsApp, en la misma únicamente cabe destacar la tabla ZWAADDRESSBOOKCONTACT que contiene información sobre los contactos del terminal, los campos de la tabla son los siguientes

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos (valor 1)
Z_OPT	Entero	Desconocido
ZPHONESTATUS	Entero	Estado de la cuenta, presenta valores de 1 a 3 siendo 1 cuando la cuenta es una cuenta activa, se desconoce lo que representan los otros dos valores

ZSECTIONSORT	Entero	Desconocido, en la muestra investigada este campo tiene valor 0
ZSORT	Entero	Desconocido
ZSPOTLIGHSTATUS	Entero	Desconocido, aunque se observa en la muestra analizada que toma valores -5 y 1 siendo 1 los contactos activos en WhatsApp.
ZABOUTTIMESTAMP	Timestamp	Fecha y hora en formato Apple Absolute Time (UTC). Sólo está completado en registros de cuentas activas en WhatsApp se interpreta como la fecha/hora de cambio del texto de usuario (siguiente campo) en la red WhatsApp
ZABOUTTEXT	Varchar	Texto que el usuario configura en su cuenta de WhatsApp para que se muestre en su perfil
ZFULLNAME	Varchar	Nombre completo del contacto (en el teléfono en el que reside la base de datos)
ZGIVENNAME	Varchar	Nombre (en el teléfono en el que reside la base de datos)
ZHIGHLIGHTEDNAME	Varchar	Apellidos (en el teléfono en el que reside la base de datos)
ZIDENTIFIER	Varchar	Identificador
ZLOCALIZEDPHONENUMBER	Varchar	No usado
ZPHONE NUMBER	Varchar	Número de teléfono del contacto, en caso de cuentas dadas de alta en WhatsApp refleja el número de teléfono asociado a la cuenta
ZPHONE NUMBER LABEL	Varchar	Etiqueta del contacto asociada al número de teléfono asociado a la cuenta. Teléfono de casa, del trabajo, móvil... En caso de contacto no asociado a WhatsApp se muestra vacío
ZSEARCHTOKENLIST	Varchar	Cadena de texto que agrupa los datos del contacto para la búsqueda (nombre, apellidos, empresa, etc.)
ZSECTIONTITLE	Varchar	Sección en la que se encuentra el contacto (inicial a la que está asociada, p.e. para Carlos sería una C)

ZWHATSAPPID	Varchar	Corresponde al número completo del teléfono móvil asociado a la cuenta, en caso de que el contacto no tenga cuenta asociada está vacío.
ZDEVICELIST	Blob	Campo vacío

Tabla 6 Esquema de la tabla ZWAADDRESSBOOKCONTACT

5.1.6 ESTRUCTURA DE LA BASE DE DATOS CHATSTORAGE.SQLITE

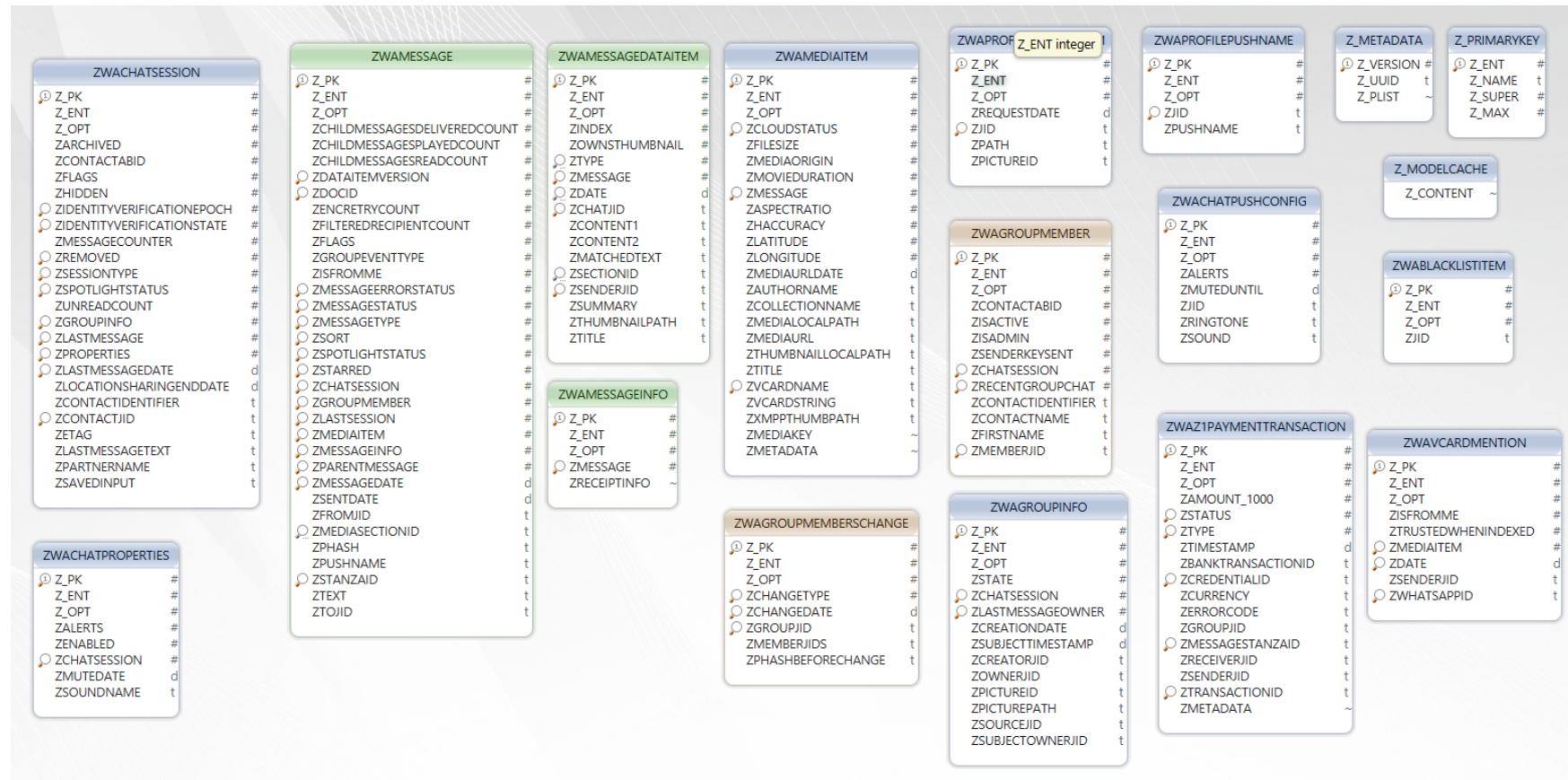


Ilustración 8 Esquema de la base de datos ChatStorage.sqlite

Esta base de datos en la que cuenta con información más interesante desde el punto de vista del análisis forense. No se profundizará en todas las tablas sino en aquellas que guardan información que puede ser relevante.

Existen dos tablas que son interesantes pero que actualmente no contienen información, pertenecen a una funcionalidad que no está activa actualmente excepto en la India y que no ha podido ser verificada, el pago a través de WhatsApp. Se trata de las tablas.

- ZWAVCARMENTION
- ZWA1PAYMENTTRANSACTION

Aunque muchos de los campos se pudo intuir su significado y contenido no se realizará esta tarea dado que no es posible aportar evidencias que justifiquen los razonamientos.

Tabla ZWABLACKLISTITEM

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos
Z_OPT	Entero	Desconocido
ZJID	Varchar	Contiene el identificador del usuario de WhatsApp

Tabla 7 Esquema de la tabla ZWABLACKLISTITEM

Tabla ZWACHATPROPERTIES

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos
Z_OPT	Entero	Desconocido
ZALERTS	Entero	En la muestra analizada este campo está vacío

ZENABLED	Entero	En la muestra analizada este campo está vacío
ZCHATSESSION	Entero	En la muestra analizada este campo está vacío
ZMUTEDATE	Entero	En la muestra analizada este campo está vacío
ZSOUNDNAME	Varchar	En la muestra analizada este campo está vacío

Tabla 8 Esquema de la tabla ZWACHATPROPERTIES

Tabla ZWACHATPUSHCONFIG

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos (valor 3)
Z_OPT	Entero	Desconocido
ZALERTS	Entero	Desconocido, en la muestra analizada el valor es 0
ZMUTEDUNTIL	Timestamp	Fecha hora hasta que el chat está silenciado
ZJID	Varchar	Identificador del chat
ZRINGTONE	Varchar	Nombre del fichero del tono asociado al chat
ZSOUND	Varchar	Nombre del sonido asociado al chat

Tabla 9 Esquema de la tabla ZWACHATPUSHCONFIG

Tabla ZWACHATSESSION

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos (en este caso valor 4)
Z_OPT	Entero	Desconocido

ZARCHIVED	Entero	Contiene un valor 1 en caso de que la conversación haya sido archivada y 0 en caso contrario
ZCONTACTBID	Entero	Desconocido, valor 0
ZFLAGS	Entero	Desconocido, en la muestra analizada toma valor 272, 256, 280, 1280 ,1296 y 1304
ZHIDDEN	Entero	Toma valor 0 si es una conversación oculta y 1 en caso contrario
TYVERIFICATIONEPOCH	Entero	Desconocido, distintos valores
TYVERIFICATIONSTATE	Entero	Desconocido, en la muestra analizada toma distintos valores
ZMESSAGECOUNTER	Entero	Número de mensajes de la conversación
ZREMOVED	Entero	Desconocido, en la muestra analizada toma valor 0
ZSESSIONTYPE	Entero	Desconocido en la muestra analizada toma valores 0 y 3
ZSPOTLIGHTSTATUS	Entero	Desconocido toma valor -5 y 1
ZUNREADCOUNT	Entero	Número de mensajes sin leer
ZGROUPINFO	Entero	Número de grupo al que pertenece la conversación (nulo si no es un grupo)
ZLASTMESSAGE	Entero	Identificador del último mensaje de la conversación
ZPROPERTIES	Entero	En la muestra analizada tiene valor nulo
LASTMESSAGEDATE	Timestamp	Fecha y hora en formato Apple Absolute Time del último mensaje de la conversación
ZLOCATIONSHARINGENDDATE	Timestamp	Desconocido, en la muestra analizada el campo está vacío

CONTACTIDENTIFIER	Varchar	Identificador del mensaje que coincide con el identificador del contacto de la tabla ZWAADDRESSBOOKCONTACT
ZCONTACTJID	Varchar	Identificador del contacto en la red social WhatsApp.
ZETAG	Varchar	Desconocido
ZLASTMESSAGETEXT	Varchar	Vacio en la muestra analizada
ZPARTNERNAME	Varchar	Nombre del contacto
ZSAVEDINPUT	Varchar	Vacio en la muestra analizada

Tabla 10 Esquema de la tabla ZWACHATSESSION

Tabla ZWAGROUPINFO

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos
Z_OPT	Entero	Desconocido
ZSTATE	Entero	Estado de la comunicación con distintos valores 0 – Mensaje entregado 3 – No ha sido posible entregarlo en el servidor 4 – Entregado en el servidor 5 – Entregado en el terminal 8 – Mensaje leído
ZCHATSESSION	Entero	Identificador de la sesión de chat
ZLASTMESSAGEOWNER	Entero	Identificador del último usuario que escribió un mensaje en el grupo
ZCREATIONDATE	Timestamp	Timestamp que recoge la fecha de creación del grupo
ZSUBJECTTIMESTAMP	Timestamp	Timestamp que recoge la fecha en la que se creó el asunto del grupo
ZCREATORJID	Varchar	Identificador del creador del grupo

ZOWNERID	Varchar	Identificador del creador del grupo
ZPICTUREPATH	Varchar	Path a la foto del grupo
ZSOURCEJID	Varchar	En la muestra analizada este campo bien estaba vacío o mostraba el mismo valor que ZOWNERID
ZSUBJECTOWNERID	Varchar	En la muestra analizada este campo bien estaba vacío o mostraba el mismo valor que ZOWNERID

Tabla 11 Esquema de la tabla ZWAGROUPINFO

Tabla ZWAGROUPEMEMBER

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos
Z_OPT	Entero	Desconocido
ZCONTACTABID	Entero	Desconocido, valor 0
ZISACTIVE	Entero	Campo que define si un contacto está activo en WhatsApp, valor 1 activo valor 0 inactivo
ZISADMIN	Entero	Campo que indica si el usuario es administrador en algún grupo 1 es administrador 0 no es administrador
ZSENDERKEYSENT	Entero	Desconocido, en la muestra se muestra valor vacío, 0 o 1
ZCHATSESSION	Entero	Identificador del grupo en el que se encuentra el usuario del registro
ZRECENTGROUPCHAT	Varchar	Desconocido
ZCONTACTIDENTIFIER	Varchar	Identificador del contacto de WhatsApp

ZCONTACTNAME	Varchar	Nombre completo del contacto en la agenda del terminal
ZFIRSTNAME	Varchar	Nombre del contacto en la agenda del terminal
ZMEMBERJID	Varchar	Identificador de WhatsApp para el contacto

Tabla 12 Esquema de la tabla ZWAGROUPMEMBER

Tabla ZWAGROUPMEMBERSCHANGE

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos (valor 7)
Z_OPT	Entero	Desconocido
ZCHANGETYPE	Entero	Desconocido, valor 3
ZCHANGEDATE	Timestamp	Desconocido, fecha en formato Apple Absolute time, todas las filas muestran el mismo valor en la muestra analizada
ZGROUPJID	Varchar	Identificador del grupo
ZMEMBERJIDS	Varchar	Identificador del miembro del grupo
ZPHASHBEFORECHANGE	Varchar	Desconocido, contiene un hash

Tabla 13 Esquema de la tabla ZWAGROUPMEMBERSCHANGE

Tabla ZWAMEDIAITEM

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos, en este caso es el valor 8
Z_OPT	Entero	Desconocido
ZCLOUDSTATUS	Entero	Campo que toma valor 4 cuando el archivo ha sido descargado

ZFILESIZE	Entero	Tamaño del archivo descargado, la unidad de la cifra almacenada corresponde a bytes
ZMEDIAORIGIN	Entero	Desconocido en la muestra analizada toma valores de 0 y 1
ZMOVIEDURATION	Entero	Duración de los ficheros multimedia, en caso de los ficheros PDF puede contener el número de páginas del documento
ZMESSAGE	Entero	Número de secuencia del mensaje (diferente del número de secuencia de registro de la tabla que se recoge en el campo Z_PK)
ZASPECTRATIO	Real	Ratio de aspecto, en la muestra analizada el valor era 0.0
ZHACCURACY	Real	Desconocido, el valor en la muestra analizado es 0.0
ZLATITUDE	Real	Anchura definida en pixels
ZLONGITUDE	Real	Altura definida en pixels
ZMEDIAURLDATE	Timestamp	Timestamp del fichero
ZAUTHORNAME	Varchar	Nombre del autor para el caso de documentos que contengan este metadato
ZCOLLECTIONNAME	Varchar	Desconocido, en la muestra analizada está vacío
ZMEDIALOCALPATH	Varchar	Ruta del fichero y ubicación en el dispositivo local
ZMEDIAURL	Varchar	URL donde se descargó el fichero. Alguna de las direcciones tienen la extensión .enc, esto se muestra para el caso de ficheros que fueron enviados

		entre usuarios, indica que estos ficheros están encriptados.
ZTHUMBNAILLOCALPATH	Varchar	En la muestra analizada el valor es nulo
ZTITLE	Varchar	<p>Este campo muestra distintos valores. En la muestra analizada se han detectado:</p> <ul style="list-style-type: none"> • Nulo • Título • Cabecera del fichero
ZVCARDNAME	Varchar	<p>Este campo contiene el hash del fichero, en caso de que el fichero haya sido enviado a un grupo contiene el identificador del grupo</p> <p>En caso del envío de una Vcard, aquí se guarda el nombre del contacto de la Vcard</p>
ZVCARDSTRING	Varchar	<p>Este campo contiene información sobre el fichero que ha sido transferido.</p> <ul style="list-style-type: none"> • Image/jpeg • Image/webp • Audio/ogg • Etc <p>En caso de envío de una Vcard aquí se incluyen los datos de la misma</p>
ZXMPPTHUMBPATH	Varchar	Ruta hasta el thumbnail del fichero en el dispositivo local
ZMEDIAKEY	Blob	Desconocido
ZMETADATA	Blob	Metadatos del fichero transmitido

Tabla 14 Esquema de la tabla ZWAMEDIAITEM

Tabla ZWAMESSAGE

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite

Z_ENT	Entero	Identificador de la tabla en la base de datos, en este caso es el valor 9
Z_OPT	Entero	Desconocido
ZCHILDMESSAGESDELIVERDCOUNT	Entero	Desconocido en la muestra analizada el valor es 0
ZCHILDMESSAGESPLAYEDCOUNT	Entero	Desconocido en la muestra analizada el valor es 0
ZCHILDMESSAGESREADCOUNT	Entero	Desconocido en la muestra analizada el valor es 0
ZDATAITEMVERSION	Entero	Desconocido en la muestra analizada el valor es 3
ZDOCID	Entero	Desconocido en la muestra analizada muestra valores numéricos entre 38 y 49
ZENCRETRYCOUNT	Entero	Desconocido en la muestra analizada el valor es 0
ZFILTEREDRECIPIENTCOUNT	Entero	Desconocido en la muestra analizada el valor es 0
ZFLAGS	Entero	Desconocido en la muestra analizada presenta distintos valores
ZGROUPEVENTTYPE	Entero	Desconocido, en la muestra analizada presenta valores 0, 1 y 2
ZSORT	Entero	Desconocido
ZISFROMME	Entero	Indica la dirección del mensaje. 0 de entrada 1 de salida
ZMESSAGEERRORSTATUS	Entero	Estado del mensaje 0 si ha sido enviado o recibido.

ZMESSAGESTATUS	Entero	<p>Estado del mensaje en la muestra analizada contiene los siguientes valores</p> <ul style="list-style-type: none"> • 0 – Mensaje entregado • 3 – No ha sido posible entregarlo en el servidor • 4 – Entregado en el servidor • 5 – Entregado en el terminal • 8 – Mensaje leído
ZMESSAGETYPE	Entero	<p>Tipo de mensaje, en la muestra analizada contiene los siguientes valores</p> <ul style="list-style-type: none"> • 0 – Mensaje de texto • 1 – Imagen • 2 – Audio • 3 y 13 – Vídeo • 4 – VCARD • 5 - Ubicación • 6 – Mensaje de control (por ejemplo, creación de grupo) • 7 - Enlace • 8 – Documento • 9 – Fichero pdf • 10 – Control. P.e. Cambio de número de teléfono de cuenta de WhatsApp • 11 – GIF animado • 12 – Mensaje de sistema • 14 – Mensaje grupal eliminado para todos

		<ul style="list-style-type: none"> • 15 – Sticker • 16 – Ubicación en tiempo real
ZSORT	Entero	Desconocido
ZSPOTLIGHTSTATUS	Entero	Desconocido en la muestra analizada los valores existentes eran 2 y -32768
ZSTARRED	Entero	Desconocido, en la muestra analizada los valores eran vacío o 0
ZCHATSESSION	Entero	Desconocido en la muestra analizada los valores eran 2, 3 o 4
ZGROUPMEMBER	Entero	Desconocido en la muestra analizada es un campo sin usar
ZLASTSESSION	Entero	Desconocido, en la muestra analizada el valor es vacío, 2, 3 o 4 (mayoritariamente vacío)
ZMEDIAITEM	Entero	Valor numérico que apunta al registro de la tabla ZWAMESSAGEITEM
ZMESSAGEINFO	Entero	Valor numérico que apunta al registro de la tabla ZWAMESSAGEINFO
ZPARENTMESSAGE	Entero	En comunicaciones tipo lista de distribución, para los mensajes dirigidos a cada uno de los miembros de la lista guarda el identificador del registro del mensaje original
ZMESSAGEDATE	Timestamp	Fecha y hora del mensaje en formato OS X Epoch Time

ZSENTDATE	Timestamp	Fecha y hora en que el mensaje fue enviado en formato OS X Epoch Time (vacío en caso de ser un mensaje recibido)
ZFROMJID	Varchar	Identificador de WhatsApp del remitente
ZMEDIASECTIONID	Varchar	Contiene el año y el mes en los que el fichero fue enviado
ZPHASH	Varchar	Desconocido, en la muestra analizada no toma valor
ZPUSHNAME	Varchar	Desconocido en la muestra analizada no toma valor
ZSTANDAID	Varchar	Identificador único del mensaje
ZTEXT	Varchar	Contenido del mensaje
ZTOJID	Varchar	Identificador de WhatsApp del destinatario del mensaje

Tabla 15 Esquema de la tabla ZWAMESSAGE

Tabla ZWMESSAGEDATAITEM

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos, en este caso es el valor 10
Z_OPT	Entero	Desconocido
ZINDEX	Entero	Desconocido
ZOWNSTHUMBNAIL	Entero	Desconocido
ZTYPE	Entero	Desconocido, en la muestra analizada el valor mostrado es 0

ZMESSAGE	Entero	Identificador del mensaje de la tabla ZWAMESSAGE
ZDATE	Timestamp	Fecha de creación del elemento, en la muestra analizada coincide con el valor del campo ZMESSAGEDATE de la tabla ZWAMESSAGE
ZCHATJID	VARCHAR	Identificador del chat
ZCONTENT1	VARCHAR	URL del elemento
ZCONTENT2	VARCHAR	Este campo bien está vacío o bien contiene una segunda URL del elemento, por ejemplo, si ZCONTENT1 fuera http://youtu.be En este campo podría contener http://www.youtube.com
ZMATCHEDTEXT	VARCHAR	Texto asociado al enlace, en la muestra coincide con el valor del campo ZCONTENT1
ZSECTIONID	VARCHAR	Año y mes de creación del elemento
ZSENDERID	VARCHAR	Desconocido, en la muestra utilizada está sin usar.
ZSUMMARY	VARCHAR	Sumario del contenido si existe
ZTHUMBNAILPATH	VARCHAR	Path a la ubicación local del thumbnail
ZTITLE	VARCHAR	Título del elemento enviado

Tabla 16 Esquema de la tabla ZWAMESSAGEDATAITEM

Tabla ZWAMESSAGEINFO

Campo	Tipo	Descripción
-------	------	-------------

Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos, en este caso es el valor 11
Z_OPT	Entero	Desconocido
ZMESSAGE	Entero	Identificador del mensaje de la tabla ZWAMESSAGE
ZRECEIPTINFO	Blob	Información de la entrega, en algún caso muestra el número de teléfono origen del mensaje, en otros el contenido es desconocido

Tabla 17 Esquema de la tabla ZWAMESSAGEINFO

Tabla ZWAPROFILEPICTURITEM

Esta tabla asocia un identificador de WhatsApp con su avatar del contacto.

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos, en este caso es el valor 12
Z_OPT	Entero	Desconocido
ZREQUESTDATE	Timestamp	Timestamp en el que se solicitó al servidor el envío del avatar del contacto
ZJID	Varchar	Identificador del contacto en WhatsApp
ZPATH	Varchar	Path en el dispositivo local a la ubicación de la imagen del avatar del contacto

ZPICTUREID	Varchar	Identificador de la imagen
------------	---------	----------------------------

Tabla 18 Esquema de la tabla ZWAPROFILEPICTUREITEM

Tabla ZWAPROFILEPUSHNAME

Esta tabla asocia un identificador de WhatsApp con el contacto en la agenda.

Campo	Tipo	Descripción
Z_PK	Entero	Número de registro de la tabla, definido por el propio SQLite
Z_ENT	Entero	Identificador de la tabla en la base de datos, en este caso es el valor 13
Z_OPT	Entero	Desconocido
ZJID	Varchar	Identificador del contacto en WhatsApp
ZPUSHNAME	Varchar	Nombre del contacto en la agenda del dispositivo

Tabla 19 Esquema de la tabla ZWAPROFILEPUSHNAME

Las tablas **Z_METADATA**, **Z_MODELCACHE** y **Z_PRIMARYKEY**, contienen información interna de la base de datos sin demasiada relevancia para el análisis forense por ejemplo **Z_PRIMARYKEY** contiene información general sobre la base de datos, el campo que es clave primaria de las principales tablas y el número de registros que contiene (que nos puede aportar cierta información como el número de mensajes, chats, ficheros, contactos, etc.)

5.1.7 BASES DE DATOS RANKING.SQLITE, EMOJI.SQLITE Y STICKER.SQLITE

Estas bases de datos no forman parte de este estudio por ser bases de datos de uso interno de WhatsApp sin interés para el objeto del informe.

5.2 ANÁLISIS DEL MODELO DE DATOS DE WHATSAPP PARA ANDROID

Para el entorno Android, tal y como se ha comentado en secciones anteriores, se han generado dos máquinas virtuales que se han asociado a unas tarjetas SIM adquiridas para la realización del proyecto. Se han realizado diversas pruebas y finalmente se ha procedido a convertir el disco de la máquina Virtual Box a formato VDI que es legible por la aplicación forense Autopsy, mediante el uso del siguiente comando.

```
"c:\Program Files\Oracle\VirtualBox\VBoxManage.exe" clonehd "..\Android 9.1 x86 Primera.vdi" autopsy_android1.img --format raw
```

Finalmente, se utiliza la aplicación Autopsy versión 14.15.0 para acceder al contenido del disco y extraer la información de los ficheros y base de datos de WhatsApp.

En el dispositivo se encuentra instalada la versión de WhatsApp 2.20.197.17 publicada el 17 de agosto de 2020.

5.2.1 ESTRUCTURA DE CARPETAS Y UBICACIÓN DE ARCHIVOS

La ruta de acceso a los ficheros objeto de análisis es /data/data/com.whatsapp/

En dicha carpeta se encuentran los siguientes ficheros y carpetas.

Nombre	Fecha de modificación	Tipo
app_minidumps	24/08/2020 11:13	Carpeta de archivos
cache	24/08/2020 11:13	Carpeta de archivos
code_cache	24/08/2020 11:13	Carpeta de archivos
databases	24/08/2020 11:29	Carpeta de archivos
files	24/08/2020 11:13	Carpeta de archivos
media	24/08/2020 11:13	Carpeta de archivos
lib-main	24/08/2020 11:13	Carpeta de archivos
no_backup	24/08/2020 11:13	Carpeta de archivos
shared_prefs	24/08/2020 11:13	Carpeta de archivos

Ilustración 9 Estructura de directorios en terminal Android

El contenido de la estructura es el siguiente.

Nombre	Tipo	Descripción
app_minidumps	Carpeta	En la muestra analizada esta carpeta se encuentra vacía.
cache	Carpeta	Carpeta que, tal y como su nombre indica, contiene información en diversas carpetas y ficheros que se describen a continuación.
cache\export_chats	Carpeta	Carpeta que contiene la caché de los chats que son exportados a petición del usuario
cache\export_gdpr	Carpeta	El usuario tiene la opción de solicitar a WhatsApp la descarga de sus datos, en esta carpeta se guarda la caché para la generación del fichero
cache\minidumps	Carpeta	En la muestra analizada esta carpeta está vacía
cache\Profile Pictures	Carpeta	Carpeta que guarda en ficheros y carpetas la caché de las fotos de perfil de los contactos del usuario del teléfono. Los datos se guardan con formato numero_de_telefono.jpg p.e. 346666666666.jpg
cache\ProfilePicture Temp	Carpeta	Carpeta que guarda archivos temporales correspondientes a las imágenes de perfil de los usuarios, en la muestra analizada se observan varios ficheros .jpg pero que se muestran con tamaño 0, una revisión del contenido en hexadecimal confirma que el fichero no tiene contenido en el momento de la extracción
cache\stickers_cache	Carpeta	Carpeta que en la muestra analizada está vacía
cache\breakpad.health	Fichero	Fichero de configuración en formato XML que contiene información sobre diversos parámetros internos de la aplicación pref_sync_protocol_version o snet_safe_browsing_last_update_time_ms_12
cache\breakpad.health-slack	Fichero	Fichero vacío

code_cache	Carpeta	Carpetas vacías
databases	Carpeta	Carpetas que contienen las distintas bases de datos de la aplicación. En la misma asociada a cada fichero de base de datos se encuentran los siguientes ficheros. Base_de_datos-shm, Base_de_datos-wal, Base_de_datos-wal-slack que son ficheros temporales por lo que no se detallará su contenido en la presente tabla
databases\jobqueue-WhatsAppJobManager	Fichero	Fichero temporal que guarda información sobre la cola de trabajos de la aplicación
databases\axolotl.db	Fichero	Base de datos que contiene información sobre claves criptográficas que se usan para identificar al usuario
databases\chatsettings.db	Fichero	Base de datos que contienen información de configuración de la aplicación en el terminal en el que se encuentra.
databases\companion_devices.db	Fichero	Base de datos que en la muestra analizada se encuentra vacía. Podría estar relacionada con una nueva funcionalidad anunciada a través de la cual se permitiría el uso de la misma cuenta de WhatsApp en varios terminales telefónicos distintos (Mehta, 2020)
databases\hsmpacks.db	Fichero	Base de datos que en las muestras analizadas se encuentra vacía. Se trata de una base de datos que guarda información sobre mensajes promocionales o de venta. HSM responde al acrónimo Highly Structured Message (ClickaTell, Fecha no reseñada), consisten en plantillas de mensajes para uso publicitario o comercial que son usadas por negocios para gestionar las comunicaciones con los clientes.
databases\location.db	Fichero	Base de datos que se usa para gestionar las localizaciones compartidas entre usuarios.
databases\media.db	Fichero	Base de datos que en la muestra analizada está vacía. Tras el análisis del nombre de los campos se puede inferir que la base de datos contiene información sobre campañas publicitarias presumiblemente para cuentas business.
databases\msgstore.db	Fichero	Base de datos con los mensajes enviados y recibidos por WhatsApp
databases\payments.db	Fichero	Base de datos que en la muestra actualizada está vacía. Podría contener información sobre una funcionalidad que no está activa

		actualmente excepto en la India y que no ha podido ser verificada, el pago a través de WhatsApp
databases\wa.db	Fichero	Base de datos que contiene la información sobre los contactos de la cuenta analizada.
databases\web_sessions.db	Fichero	Base de datos que contiene la información sobre las conexiones activas con WhatsApp Web
files	Carpeta	Carpeta que contiene distintas carpetas: avatars, gifs, papelera, logs.... Adicionalmente cuenta con un conjunto de ficheros de uso interno de WhatsApp y por este motivo no aportan información interesante para este trabajo por lo que no serán analizados: DATA_disk_creation_time_its, _m_t, DATA_ServerControlledParametersManager.data.com.whatsapp, invalids_numbers...
files\Shared	Carpeta	Esta carpeta contiene ficheros que han sido compartidos por el usuario
files\trash	Carpeta	Carpeta papelera, en ella se han encontrado ficheros diversos... .xml, mp3, etc.
files\Avatars	Carpeta	Carpeta que contiene avatars de distintos grupos y usuarios
files\decompressed	Carpeta	Carpeta que contiene ficheros de la aplicación WhatsApp (librerías, etc.)
files\Gifs	Carpeta	Carpeta vacía
files\Logs	Carpeta	Carpeta que contiene el fichero whatsapp.log que contiene el log de la aplicación del día en curso. Adicionalmente guarda un fichero .tar.gz con los logs de forma individual de cada uno de los últimos 7 días.
files\Stickers	Carpeta	Carpeta vacía en la muestra analizada
files\key	Carpeta	En teléfonos estándar la base de datos se encuentra protegida por un cifrado crypt12, de hecho, todas las copias de seguridad de la base de datos de WhatsApp que se encuentran en la tarjeta SD del terminal se encuentran cifradas. La clave para su descifrado se puede localizar en la parte oculta del terminal, concretamente en este fichero denominado key.
files\backup_token	Carpeta	Token que permite acceder a la copia de seguridad de la base de datos alojado en la cuenta Google Cloud
media\WhatsApp Audio	Carpeta	Carpeta que contiene los audios enviados y recibidos
media\WhatsApp Documents	Carpeta	Carpeta que contiene los documentos enviados y recibidos
media\WhatsApp Images	Carpeta	Carpeta que contiene las imágenes enviadas y recibidas

media\WhatsApp Stickers	Carpeta	Carpetas que contiene los stickers enviados y recibidos
media\WhatsApp Video	Carpeta	Carpetas que contiene los videos enviados y recibidos
media\WhatsApp Voice Notes	Carpeta	Carpetas que contiene las notas de voz enviadas y recibidas.
lib_main	Carpeta	Carpetas que contiene las librerías que utiliza el programa WhatsApp
shared_prefs	Carpeta	Carpetas que contiene diversos archivos .xml con las preferencias del programa

Tabla 20 Contenido de la estructura de directorios en terminal Android

5.2.2 ESTRUCTURA DE LA BASE DE DATOS AXOLOTL.DB

Se ha podido verificar que la misma contiene información sobre las claves criptográficas que se utilizan para autenticar al usuario en la aplicación. No se profundizará en el análisis de la misma ya que su contenido afecta más a la seguridad de las comunicaciones que al análisis forense de la aplicación. A continuación, se muestra el esquema de la base de datos

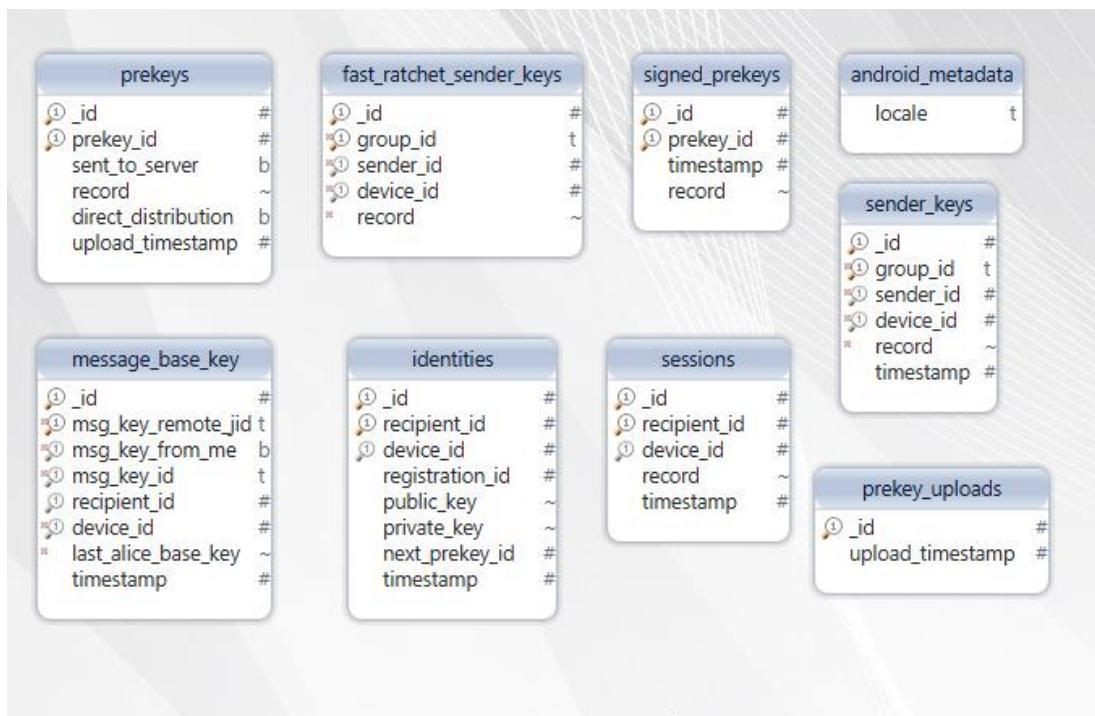


Ilustración 10 Esquema de la base de datos axolotl.db

5.2.3 ESTRUCTURA DE LA BASE DE DATOS CHATSETTINGS.DB

Se ha podido verificar que la misma contiene información sobre la configuración de los chats, de esta forma es donde para un chat concreto (identificado a través de su jid), se registran las configuraciones específicas del mismo, si han sido silenciadas las notificaciones (campo muted), el tono para la notificación de recepción de un mensaje (campo message_tone), información diversa que no es de especial interés para el análisis forense.

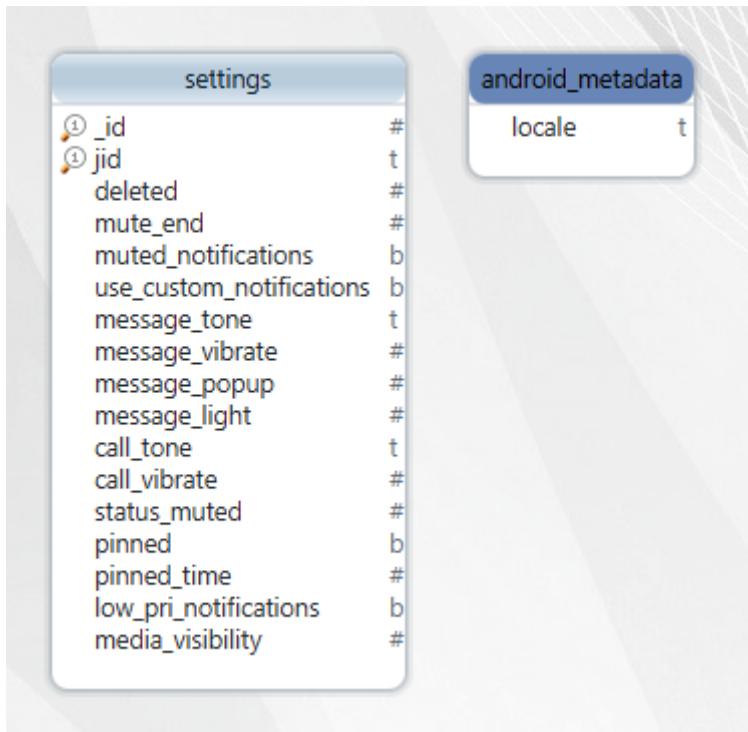


Ilustración 11 Estructura de la base de datos chatsettings.db

5.2.4 ESTRUCTURA DE LA BASE DE DATOS COMPANION_DEVICES.DB

Tal y como se comentaba anteriormente en la muestra analizada la base de datos está vacía. Se ha verificado en distintos terminales, por lo que es probable que esta tabla todavía no esté en uso, se infiere que pertenece a una funcionalidad futura pero que ya ha sido anunciada (Mehta, 2020)

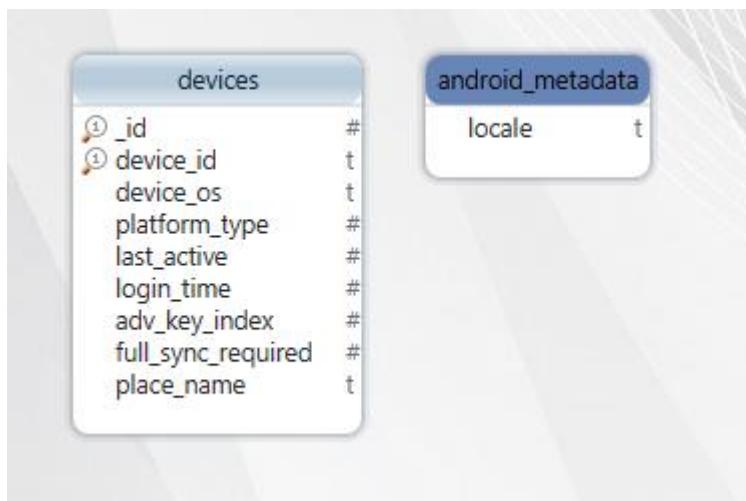


Ilustración 12 Esquema de la base de datos `companion_devices.db`

5.2.5 ESTRUCTURA DE LA BASE DE DATOS HSMPACKS.DB

Tal y como se comentaba anteriormente se trata de una base de datos que en las muestras analizadas se encuentra vacía. De acuerdo con el nombre de la base de datos se infiere que contiene información sobre mensajes promocionales o de venta. HSM responde al acrónimo Highly Structured Message, consisten en plantillas de mensajes para uso publicitario o comercial que son usadas por negocios para gestionar las comunicaciones con los clientes. No obstante, no ha podido ser verificado ya que esta funcionalidad parece más asociada a cuentas business y en el presente estudio se centra en cuentas de uso personal.

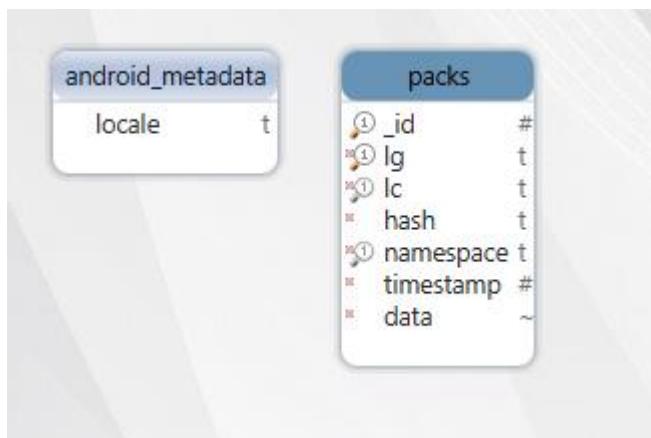


Ilustración 13 Esquema de la base de datos `hsmpacks.db`

5.2.6 ESTRUCTURA DE LA BASE DE DATOS LOCATION.DB

Esta base de datos podría resultar de interés para el análisis forense, aunque es poco probable que su análisis aporte mucha información. En la misma se guarda información sobre las geolocalizaciones compartidas con el usuario y por el usuario en distintas tablas. Algunas de las localizaciones son compartidas en tiempo real y durante un periodo limitado de tiempo tras el cual son borradas de la base de datos por lo que se convierte en información volátil.

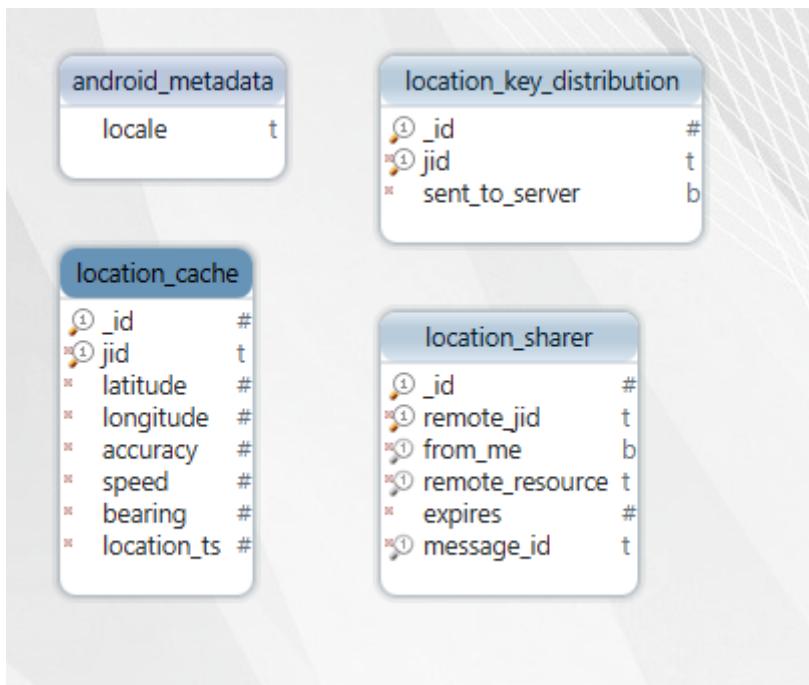


Ilustración 14 Esquema de la base de datos Location.db

Tabla location_cache

Tabla que contiene las localizaciones almacenadas. Se trata de una caché por lo que la información es volátil.

Campo	Tipo	Descripción
<code>_id</code>	Entero	Número de registro de la tabla, definido por el propio SQLite
<code>_jid</code>	Texto	Identificador del contacto, compuesto por el número de teléfono del mismo seguido de la cadena @s.whatsapp.net
<code>latitude</code>	Real	Latitud de la localización
<code>longitude</code>	Real	Longitud de la localización

accuracy	Entero	Precisión de la localización
speed	Real	Velocidad de desplazamiento registrada por el GPS
bearing	Entero	Dirección en la que se realiza el desplazamiento
location_ts	Timestamp	Fecha y hora en la que se ha registrado la localización.

Tabla 21 Esquema de la tabla location_cache

Tabla location_key_distribution

Tabla que contiene información sobre el envío de localizaciones al servidor de WhatsApp

Campo	Tipo	Descripción
_id	Entero	Número de registro de la tabla, definido por el propio SQLite
_jid	Texto	Identificador del contacto, compuesto por el número de teléfono del mismo seguido de la cadena @s.whatsapp.net
sent_to_server	Booleano	Indica si la localización ha sido enviada al servidor de WhatsApp (1) o no (0)

Tabla 22 Esquema de la tabla location_key_distribution

Tabla location_sharer

Tabla que contiene información sobre con quién o de quién se comparte la localización desde el terminal analizado.

Campo	Tipo	Descripción
_id	Entero	Número de registro de la tabla, definido por el propio SQLite
remote_jid	Texto	Identificador del contacto con el que se comparte localización, compuesto por el número de teléfono del mismo

		seguido de la cadena @s.whatsapp.net
from_me	Booleano	Indica si el propietario del terminal es el que comparte la localización (1) o bien si es el contacto remoto quien comparte su localización (0)
remote_resource	Texto	Información sobre el recurso remoto
Expires	Entero	Campo que indica durante cuánto tiempo la localización será compartida, WhatsApp en su aplicación predefine varios valores.
message_id	Texto	Identificador del mensaje en el cual se ha compartido la ubicación.

Tabla 23 Esquema de la tabla location_sharer

5.2.7 ESTRUCTURA DE LA BASE DE DATOS MEDIA.DB

En las muestras analizadas el contenido de la base de datos estaba vacía, parece contener información sobre campañas publicitarias para cuentas business que no entran dentro del alcance del presente trabajo.

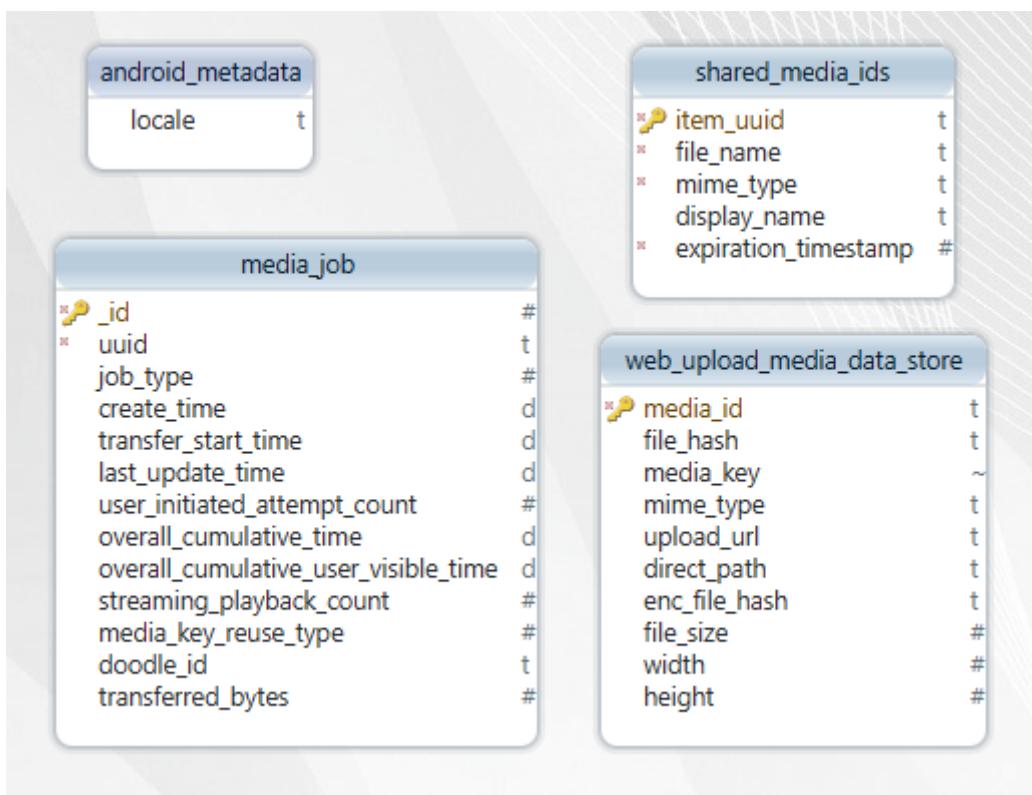


Ilustración 15 Esquema de la base de datos media.db

5.2.8 ESTRUCTURA DE LA BASE DE DATOS MSGSTORE.DB

Esta base de datos es la más importante desde el punto de vista forense, contiene la información sobre los mensajes enviados y recibidos. Se trata de una base de datos extensa con 110 tablas por lo que, por su tamaño no se muestra el esquema general de la misma.

Tabla awaymessages

En las muestras analizadas esta tabla se encuentra vacía. Por ello únicamente se muestra la estructura de la misma.

The screenshot shows a database management interface for editing a table named 'away_messages'. The table structure is defined as follows:

Vis...	Name	Details	Description
<input checked="" type="checkbox"/>	① _id	integer	
<input checked="" type="checkbox"/>	① jid	text not null	

Below the table, there are several buttons: Edit, Add, Drop, Up, Down, Visible Columns, Help, Aceptar, and Cancelar.

Ilustración 16 Esquema de la tabla awaymessages

Tabla call_log

Esta tabla guarda el registro de las llamadas realizadas desde y hacia el terminal, la estructura de la tabla es la siguiente

Vis...	Name	Details	Description
✓	⌚ _id	integer	
✓	⌚ jid_row_id	integer	
✓	⌚ from_me	integer	
✓	⌚ call_id	text	
✓	⌚ transaction_id	integer	
✓	-- timestamp	integer	
✓	-- video_call	integer	
✓	-- duration	integer	
✓	-- call_result	integer	
✓	-- bytes_transferred	integer	
✓	-- group_jid_row_id	integer not null def...	

Ilustración 17 Esquema de la tabla call_log

El contenido de los campos es el siguiente

Campo	Tipo	Descripción
_id	Entero	Número de registro de la tabla, definido por el propio SQLite
jid_row_id	Entero	Identificador del contacto con el que se realiza la llamada
from_me	Entero	Indica si el propietario del terminal es el que realiza la llamada (1) o bien si es el destinatario de la misma (0)
call_id	Texto	Identificador de la llamada compuesto por el literal “call:” seguido de una cadena de 32 caracteres
transaction_id	Entero	Identificador de la transacción
timestamp	Entero	Fecha y hora en la cual se ha producido la llamada

video_call	Entero	Campo con valor 1 si se trata de una vídeo llamada y 0 si es una llamada de audio
duration	Entero	Duración en segundos de la llamada
call_result	Entero	Resultado de la llamada en la muestra analizada se han encontrado los siguientes valores <ul style="list-style-type: none"> • 2 llamada sin respuesta siendo destinatario de la llamada • 3 error en la llamada • 4 llamada rechazada o perdida siendo remitente de la llamada • 5 llamada finalizada
bytes_transferred	Entero	Número de bytes transferidos
group_jid_row_id	Entero	Identificador del grupo en caso de tratarse de una llamada grupal, 0 en caso contrario

Tabla 24 Esquema de la tabla call_log

Tabla call_log_participant_v2

Esta tabla guarda el registro de los participantes en las llamadas realizadas desde y hacia el terminal, la estructura de la tabla es la siguiente

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	② call_log_row_id	integer
<input checked="" type="checkbox"/>	③ jid_row_id	integer
<input checked="" type="checkbox"/>	④ call_result	integer

Ilustración 18 Esquema de la tabla call_log_participant_v2

El contenido de los campos es el siguiente

Campo	Tipo	Descripción
<code>_id</code>	Entero	Número de registro de la tabla, definido por el propio SQLite
<code>call_log_row_id</code>	Entero	Número de llamada registrada en la tabla <code>call_log</code>
<code>Jid_row_id</code>	Entero	Identificador del registro en la tabla de contactos con el que se mantiene la conversación
<code>call_result</code>	Entero	Resultado de la llamada, las pruebas analizadas nos muestran los siguientes valores <ul style="list-style-type: none"> • 2 llamada sin respuesta siendo destinatario de la llamada • 3 error en la llamada • 4 llamada rechazada o perdida siendo remitente de la llamada • 5 llamada finalizada

Tabla 25 Esquema de la tabla `call_log_participant_v2`

Tabla chat

Esta tabla guarda el registro de los chats que se guardan en el terminal, la estructura de la tabla es la siguiente

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	jid_row_id	integer
<input checked="" type="checkbox"/>	hidden	integer
<input checked="" type="checkbox"/>	subject	text
<input checked="" type="checkbox"/>	created_timestamp	integer
<input checked="" type="checkbox"/>	display_message_row_id	integer
<input checked="" type="checkbox"/>	last_message_row_id	integer
<input checked="" type="checkbox"/>	last_read_message_row_id	integer
<input checked="" type="checkbox"/>	last_read_receipt_sent_message_row_id	integer
<input checked="" type="checkbox"/>	last_important_message_row_id	integer
<input checked="" type="checkbox"/>	archived	integer
<input checked="" type="checkbox"/>	sort_timestamp	integer
<input checked="" type="checkbox"/>	mod_tag	integer
<input checked="" type="checkbox"/>	gen	real
<input checked="" type="checkbox"/>	spam_detection	integer
<input checked="" type="checkbox"/>	unseen_earliest_message_received_time	integer
<input checked="" type="checkbox"/>	unseen_message_count	integer
<input checked="" type="checkbox"/>	unseen_missed_calls_count	integer
<input checked="" type="checkbox"/>	unseen_row_count	integer
<input checked="" type="checkbox"/>	plaintext_disabled	integer
<input checked="" type="checkbox"/>	vcard_ui_dismissed	integer
<input checked="" type="checkbox"/>	change_number_notified_message_row_id	integer
<input checked="" type="checkbox"/>	show_group_description	integer
<input checked="" type="checkbox"/>	ephemeral_expiration	integer
<input checked="" type="checkbox"/>	ephemeral_setting_timestamp	integer
<input checked="" type="checkbox"/>	last_read_ephemeral_message_row_id	integer

Ilustración 19 Esquema de la tabla chat

El contenido de los campos es el siguiente

Campo	Tipo	Descripción
_id	Entero	Número de registro de la tabla, definido por el propio SQLite

Jid_row_id	Entero	Identificador del contacto con el que se mantiene el chat
hidden	Entero	Indica si el chat está oculto (1) o no (0)
subject	Texto	Asunto del chat, en caso de que se trate de un grupo y que esté definido null en caso contrario.
created_timestamp	Entero	Fecha y hora en la cual se ha creado el chat en formato Unix Epoch Time
display_message_row_id	Entero	Número de fila del mensaje la tabla mensajes que se muestra
last_message_row_id	Entero	Número de fila del último mensaje del chat en la tabla mensajes
last_message_read_row_id	Entero	Número de fila del último mensaje leído del chat en la tabla mensajes
last_read_receipt_sent_message_row_id	Entero	Número de fila del último mensaje recibido en el chat en la tabla mensajes
last_important_message_row_id	Entero	Número de fila del último mensaje considerado por la aplicación como importante del chat en la tabla mensajes. En la muestra analizada el valor es 1 que corresponde con un mensaje de la aplicación
archived	Entero	Indica que el chat está archivado (1) o no (0)

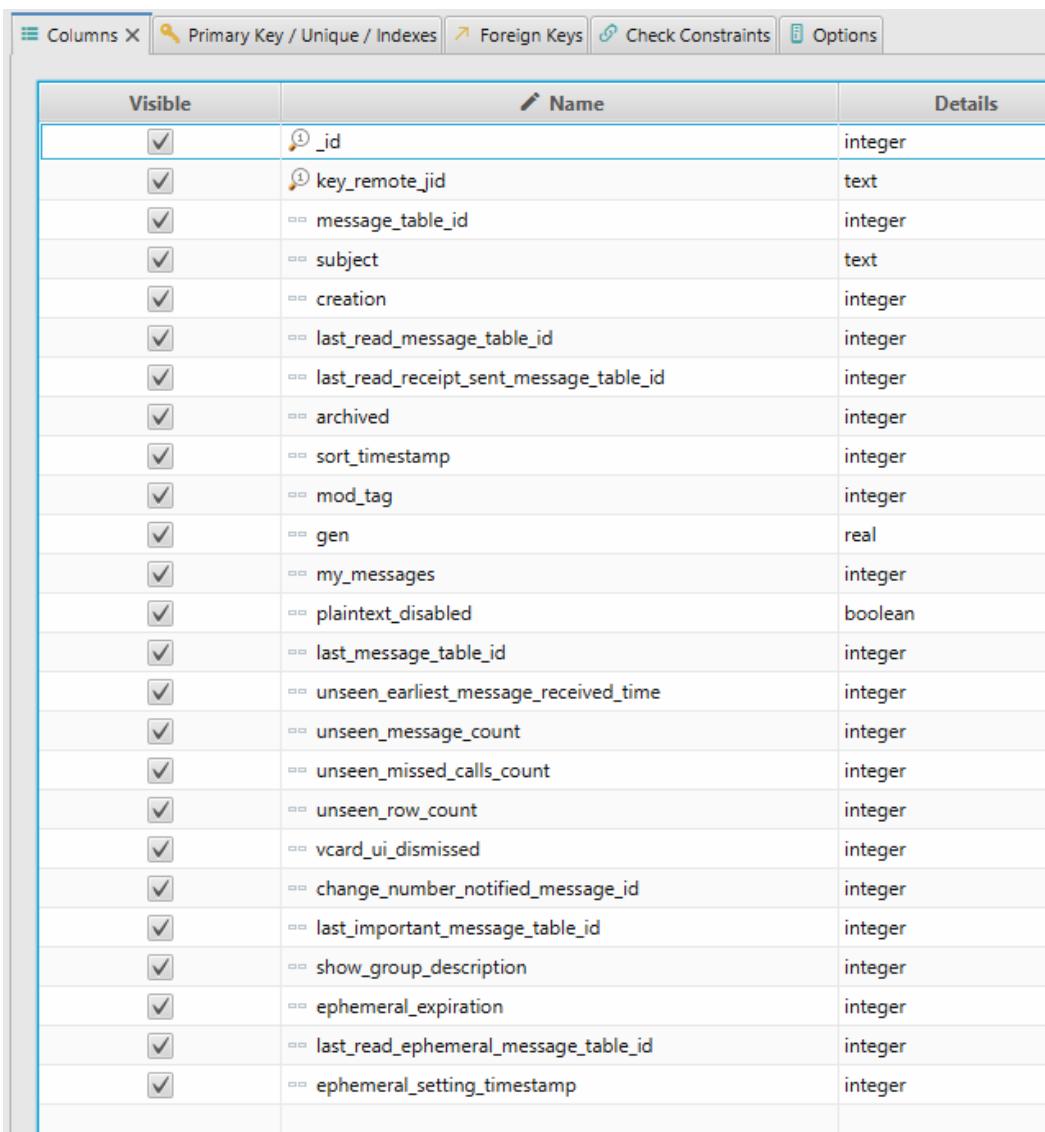
sort_timestamp	Entero	Timestamp en formato UNIX epoch time en el que el chat fue ordenado
mod_tag	Entero	Desconocido
gen	Real	Desconocido en la muestra analizada el valor es 0.0
spam_detection	Entero	Desconocido, en las muestras analizadas en una de las bases de datos el campo tomaba valor 1 o nulo y en la otra -1 o nulo.
unseen_earliest_message_received_time	Entero	Timestamp en formato UNIX Epoch Time que refleja la fecha y hora en la que se recibió el último mensaje sin leer
unseen_message_count	Entero	Número de mensajes sin leer
unseen_missed_calls_count	Entero	Número de llamadas perdidas
unseen_row_count	Entero	Número de líneas sin leer en los mensajes
plaintext_disabled	Entero	Campo que toma valor 1 o nulo pero cuya función se desconoce
vcard_ui_dismissed	Entero	Desconocido
change_number_notified_message_row_id	Entero	Campo que indica el número de fila en la tabla messages en el que se notifica un cambio en el número de teléfono

show_group_description	Entero	Campo que toma valor 1 para grupos en los que se quiera mostrar la descripción del grupo y 0 en el resto.
ephemeral_expiration	Entero	Desconocido.
ephemeral_setting_timestamp	Entero	Desconocido.
last_read_ephemeral_message_row_id	Entero	Desconocido.

Tabla 26 Esquema de la tabla chat

Tabla chat_list

Esta tabla es muy similar a la anterior mostrando información sobre los chats que se guardan en el terminal, la estructura de la tabla es la siguiente



The screenshot shows a database schema viewer with the following interface elements:

- Top navigation bar with tabs: Columns, Primary Key / Unique / Indexes (selected), Foreign Keys, Check Constraints, Options.
- Table header: Visible, Name, Details.
- Table body containing 33 rows, each representing a column definition:

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	key_remote_jid	text
<input checked="" type="checkbox"/>	message_table_id	integer
<input checked="" type="checkbox"/>	subject	text
<input checked="" type="checkbox"/>	creation	integer
<input checked="" type="checkbox"/>	last_read_message_table_id	integer
<input checked="" type="checkbox"/>	last_read_receipt_sent_message_table_id	integer
<input checked="" type="checkbox"/>	archived	integer
<input checked="" type="checkbox"/>	sort_timestamp	integer
<input checked="" type="checkbox"/>	mod_tag	integer
<input checked="" type="checkbox"/>	gen	real
<input checked="" type="checkbox"/>	my_messages	integer
<input checked="" type="checkbox"/>	plaintext_disabled	boolean
<input checked="" type="checkbox"/>	last_message_table_id	integer
<input checked="" type="checkbox"/>	unseen_earliest_message_received_time	integer
<input checked="" type="checkbox"/>	unseen_message_count	integer
<input checked="" type="checkbox"/>	unseen_missed_calls_count	integer
<input checked="" type="checkbox"/>	unseen_row_count	integer
<input checked="" type="checkbox"/>	vcard_ui_dismissed	integer
<input checked="" type="checkbox"/>	change_number_notified_message_id	integer
<input checked="" type="checkbox"/>	last_important_message_table_id	integer
<input checked="" type="checkbox"/>	show_group_description	integer
<input checked="" type="checkbox"/>	ephemeral_expiration	integer
<input checked="" type="checkbox"/>	last_read_ephemeral_message_table_id	integer
<input checked="" type="checkbox"/>	ephemeral_setting_timestamp	integer

Ilustración 20 Esquema de la tabla chat_list

El contenido de los campos es el siguiente

Campo	Tipo	Descripción
<code>_id</code>	Entero	Número de registro de la tabla, definido por el propio SQLite
<code>key_remote_jid</code>	Texto	Identificador del contacto con el que se mantiene el chat. En caso de chats individuales el valor es el número de teléfono seguido por la cadena "@s.whatsapp.net", en caso de grupos está compuesto por el número de teléfono del creador del grupo seguido de un guión "-" y el timestamp en el que se creó el chat (campo <code>created_timestamp</code> de la tabla <code>chat</code>), por último, incorpora la cadena "@g.us"
<code>message_table_id</code>	Entero	Desconocido
<code>subject</code>	Texto	Asunto del chat, en caso de que se trate de un grupo y que esté definido null en caso contrario.
<code>creation</code>	Entero	Fecha y hora en la cual se ha creado el chat en formato Unix Epoch Time

last_read_message_table_id	Entero	Identificador de la fila en la tabla messages que indica el último mensaje leído del chat.
last_read_receipt_sent_message_table_id	Entero	Identificador de la fila en la tabla messages que indica el último mensaje cuyo acuse de lectura fue enviado.
archived	Entero	Indica que el chat está archivado (1) o no (0)
sort_timestamp	Entero	Timestamp en formato UNIX epoch time en el que el chat fue ordenado
mod_tag	Entero	Desconocido
gen	Real	Desconocido en la muestra analizada el valor es 0.0
my_messages	Entero	En la muestra analizada se ha podido observar que se trata de un campo que toma valor -1 si el chat no contiene mensajes del usuario y 1 en caso contrario.
plaintext_disabled	Booleano	Campo que toma valor 1 o nulo pero cuya función se desconoce
last_message_table_id		Identificador del registro en la tabla messages que indica el último mensaje del chat.
unseen_earliest_message_received_time	Entero	Timestamp en formato UNIX Epoch Time que refleja la fecha y hora en la

		que se recibió el primer mensaje del chat
unseen_message_count	Entero	Número de mensajes sin leer
unseen_missed_calls_count	Entero	Número de llamadas perdidas
unseen_row_count	Entero	Número de líneas sin leer en los mensajes
vcard_ui_dismissed	Entero	Desconocido
change_number_notified_message_id	Entero	Campo que indica el número de fila en la tabla messages en el que se notifica un cambio en el número de teléfono
last_important_message_table_id		Identificador del último mensaje que la aplicación considera importante, en la muestra analizada apuntaba a un mensaje de sistema.
show_group_description	Entero	Campo que toma valor 1 para grupos en los que se quiera mostrar la descripción del grupo y 0 en el resto.
ephemeral_expiration	Entero	Desconocido.
last_read_ephemeral_message_row_id	Entero	Desconocido.
ephemeral_setting_timestamp	Entero	Desconocido.

Tabla 27 Esquema de la tabla chat_list

Tabla conversion_tuples

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	① jid_row_id	integer
<input checked="" type="checkbox"/>	--- data	text
<input checked="" type="checkbox"/>	--- source	text
<input checked="" type="checkbox"/>	--- biz_count	integer
<input checked="" type="checkbox"/>	--- has_user_sent_last_message	boolean
<input checked="" type="checkbox"/>	--- last_interaction	integer

Ilustración 21 Esquema de la tabla conversion_tuples

Tabla deleted_chat_box

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	② chat_row_id	integer not null
<input checked="" type="checkbox"/>	--- block_size	integer
<input checked="" type="checkbox"/>	--- deleted_message_row_id	integer
<input checked="" type="checkbox"/>	--- deleted_starred_message_row_id	integer
<input checked="" type="checkbox"/>	--- deleted_messages_remove_files	boolean
<input checked="" type="checkbox"/>	--- deleted_categories_message_row_id	integer
<input checked="" type="checkbox"/>	--- deleted_categories_starred_message_row_id	integer
<input checked="" type="checkbox"/>	--- deleted_categories_remove_files	boolean
<input checked="" type="checkbox"/>	--- deleted_message_categories	text

Ilustración 22 Esquema de la tabla deletec_chat_box

Tabla frequent

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Columns X		Primary Key / Unique / Indexes	Foreign Key
Visible	Name	Details	
<input checked="" type="checkbox"/>	① _id	integer	
<input checked="" type="checkbox"/>	① jid_row_id	integer not null	
<input checked="" type="checkbox"/>	① type	integer not null	
<input checked="" type="checkbox"/>	message_count	integer not null	

Ilustración 23 Esquema de la tabla frequent

Tabla frequentes

Tabla que muestra contactos con los que se intercambia información, así como el número de mensajes enviados, aunque no está claro el uso que se hace de esta información en la aplicación.

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	jid	text not null
<input checked="" type="checkbox"/>	type	integer not null
<input checked="" type="checkbox"/>	message_count	integer not null

Ilustración 24 Esquema de la tabla frequent

La descripción de los campos es la siguiente

Campo	Tipo	Descripción
_id	Entero	Número de registro de la tabla, definido por el propio SQLite
Jid	Entero	Número de identificador del contacto con el formato descrito en tablas anteriores
type	Entero	Desconocido
message_count	Entero	Número de mensajes intercambiados

Tabla 28 Esquema de la tabla frequent

Tabla group_notification_version

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows a table structure with three tabs at the top: 'Columns X', 'Primary Key / Unique / Indexes', and 'Foreign Keys'. The 'Columns X' tab is selected. The table has three columns: 'Visible', 'Name', and 'Details'. There are four rows:

Visible	Name	Details
<input checked="" type="checkbox"/>	group_jid_row_id	integer
<input checked="" type="checkbox"/>	subject_timestamp	integer not null
<input checked="" type="checkbox"/>	announcement_version	integer not null
<input checked="" type="checkbox"/>	participant_version	integer not null

Ilustración 25 Esquema de la tabla group_notification_version

Tabla group_participant_device

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows a table structure with three tabs at the top: 'Columns X', 'Primary Key / Unique / Indexes', and 'Foreign Keys'. The 'Columns X' tab is selected. The table has three columns: 'Visible', 'Name', and 'Details'. There are four rows:

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	group_participant_row_id	integer not null
<input checked="" type="checkbox"/>	device_jid_row_id	integer not null
<input checked="" type="checkbox"/>	sent_sender_key	integer

Ilustración 26 Esquema de la tabla group_participant_device

Tabla group_participant_user

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① group_jid_row_id	integer not null
<input checked="" type="checkbox"/>	① user_jid_row_id	integer not null
<input checked="" type="checkbox"/>	== rank	integer
<input checked="" type="checkbox"/>	== pending	integer

Ilustración 27 Esquema de la tabla group_participant_user

Tabla group_participants

Tabla que recoge información de los usuarios de WhatsApp que participan en los grupos, la estructura de la tabla es la siguiente.

The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① gjid	text not null
<input checked="" type="checkbox"/>	① jid	text not null
<input checked="" type="checkbox"/>	== admin	integer
<input checked="" type="checkbox"/>	== pending	integer
<input checked="" type="checkbox"/>	== sent_sender_key	integer

Ilustración 28 Esquema de la tabla group_participants

El contenido de la tabla se describe a continuación

Campo	Tipo	Descripción
_id	Entero	Número de registro de la tabla, definido por el propio SQLite
gjid	Texto	Número de identificador del grupo con el formato descrito en tablas anteriores

jid	Texto	Número de identificador del contacto que pertenece al grupo con el formato indicado en tablas anteriores
Admin	Entero	Indica si el contacto es administrador del grupo. En las muestras analizadas los valores eran 2 para administrador y 0 para no administrador
Pending	Entero	Desconocido en la muestra analizada toma valor 0
Sent_sender_key	Entero	Desconocido en la muestra analizada el campo toma valor 1 o 0

Tabla 29 Contenido de la tabla group_participants

Tabla group_participant_history

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	timestamp	datetime not null
<input checked="" type="checkbox"/>	gjid	text not null
<input checked="" type="checkbox"/>	jid	text not null
<input checked="" type="checkbox"/>	action	integer not null
<input checked="" type="checkbox"/>	old_phash	text not null
<input checked="" type="checkbox"/>	new_phash	text not null

Ilustración 29 Esquema de la tabla group_participant_history

Tabla jid

Tabla que recoge información de los usuarios de WhatsApp que participan en los grupos, la estructura de la tabla es la siguiente.

Visible	Name	Details
✓	_id	integer
✓	user	text not null
✓	server	text not null
✓	agent	integer
✓	device	integer
✓	type	integer
✓	raw_string	text

Ilustración 30 Esquema de la tabla jid

El contenido de la tabla se describe a continuación

campo	Tipo	Descripción
_id	Entero	Número de registro de la tabla, definido por el propio SQLite
user	Texto	Número de teléfono del usuario y en caso de grupos, número de teléfono del administrador “-“ timestamp de creación del grupo.
server	Texto	El valor de este campo es s.whatsapp.net para usuarios particulares y g.us para grupos
agent	Entero	Desconocido, en las muestras analizadas toma valor 0
device	Entero	Desconocido, en las muestras analizadas toma valor 0
type	Entero	Tipo del contacto, se han identificado los siguientes valores 0 Usuario particular 1 Grupo 5 Usuario de sistema

		17 Desconocido.
raw_string	Texto	Cadena que construye el jid, para los tipos 0 y 1 corresponde a lo descrito anteriormente. Adicionalmente 5 corresponde a status@broadcast y 17 el jid se construye igual que el usuario particular pero añadiendo ".0:0" antes del símbolo arroba y tras el número de teléfono. P.e. 34666666666.0:0@s.whatsapp.net

Tabla 30 Contenido de la tabla jid

Tabla keywords

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Columns X			Primary Key / Unique / Indexes
Visible	Name	Details	
<input checked="" type="checkbox"/>	① _id	integer	
<input checked="" type="checkbox"/>	① keyword	text not null	

Ilustración 31 Esquema de la tabla keywords

Tabla labeled_jid

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① label_id	integer not null
<input checked="" type="checkbox"/>	① jid_row_id	integer not null

Ilustración 32 Esquema de la tabla labelled_jid

Tabla labeled_jids

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① label_id	integer not null
<input checked="" type="checkbox"/>	① jid	text

Ilustración 33 Esquema de la tabla labelled_jids

Tabla labeled_messages

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① label_id	integer not null
<input checked="" type="checkbox"/>	① message_row_id	integer not null

Ilustración 34 Esquema de la tabla labelled_messages

Tabla labeled_messages_fts

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Visible	Name	Details
<input checked="" type="checkbox"/>	== content	enum

Ilustración 35 Esquema de la tabla labelled_messages_fts

Tabla labeled_messages_fts_content

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows the 'Columns' tab of the MySQL Workbench interface. The table structure is as follows:

Visible	Name	Details
<input checked="" type="checkbox"/>	docid	integer
<input checked="" type="checkbox"/>	c0content	enum

Ilustración 36 Esquema de la tabla labelled_fts_content

Tabla labeled_messages_fts_segdir

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows the 'Columns' tab of the MySQL Workbench interface. The table structure is as follows:

Visible	Name	Details
<input checked="" type="checkbox"/>	level	integer
<input checked="" type="checkbox"/>	idx	integer
<input checked="" type="checkbox"/>	start_block	integer
<input checked="" type="checkbox"/>	leaves_end_block	integer
<input checked="" type="checkbox"/>	end_block	integer
<input checked="" type="checkbox"/>	root	blob

Ilustración 37 Esquema de la tabla labelled_fts_segdir

Tabla labeled_messages_fts_segments

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows the 'Columns' tab of the MySQL Workbench interface. The table structure is as follows:

Visible	Name	Details
<input checked="" type="checkbox"/>	blockid	integer
<input checked="" type="checkbox"/>	block	blob

Ilustración 38 Esquema de la tabla messages_fts_segments

Tabla labels

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Illustración 39 Esquema de la tabla labels

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① label_name	text
<input checked="" type="checkbox"/>	== predefined_id	integer
<input checked="" type="checkbox"/>	== color_id	integer

Ilustración 39 Esquema de la tabla labels

Tabla media_hash_thumbnail

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Illustración 40 Esquema de la tabla hash_thumbnail

Visible	Name	Details
<input checked="" type="checkbox"/>	① media_hash	text
<input checked="" type="checkbox"/>	== thumbnail	blob

Ilustración 40 Esquema de la tabla hash_thumbnail

Tabla media_refs

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

Illustración 41 Esquema de la tabla media_refs

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① path	text
<input checked="" type="checkbox"/>	== ref_count	integer

Ilustración 41 Esquema de la tabla media_refs

Tabla message

Tabla que no se describirá ya que únicamente muestra una única fila y todos los valores coinciden en todas las muestras analizadas. Sin embargo, en la tabla messages sí se muestra toda la información de los mensajes. Los campos que toman valor son los siguientes

- `_id` con valor 1
- `chat_row_id` con valor -1
- `from_me` con valor 0
- `key_id` con valor -1
- `sort_id` con valor 0

El resto de los campos tienen valor nulo

La estructura de la tabla se muestra a continuación.

Visible	Name	Details
<input checked="" type="checkbox"/>	<code>_id</code>	integer
<input checked="" type="checkbox"/>	<code>chat_row_id</code>	integer not null
<input checked="" type="checkbox"/>	<code>from_me</code>	integer not null
<input checked="" type="checkbox"/>	<code>key_id</code>	text not null
<input checked="" type="checkbox"/>	<code>sender_jid_row_id</code>	integer
<input checked="" type="checkbox"/>	<code>status</code>	integer
<input checked="" type="checkbox"/>	<code>broadcast</code>	integer
<input checked="" type="checkbox"/>	<code>recipient_count</code>	integer
<input checked="" type="checkbox"/>	<code>participant_hash</code>	text
<input checked="" type="checkbox"/>	<code>origination_flags</code>	integer
<input checked="" type="checkbox"/>	<code>origin</code>	integer
<input checked="" type="checkbox"/>	<code>timestamp</code>	integer
<input checked="" type="checkbox"/>	<code>received_timestamp</code>	integer
<input checked="" type="checkbox"/>	<code>receipt_server_timestamp</code>	integer
<input checked="" type="checkbox"/>	<code>message_type</code>	integer
<input checked="" type="checkbox"/>	<code>text_data</code>	text
<input checked="" type="checkbox"/>	<code>starred</code>	integer
<input checked="" type="checkbox"/>	<code>lookup_tables</code>	integer
<input checked="" type="checkbox"/>	<code>sort_id</code>	integer not null default 0

Ilustración 42 Esquema de la tabla message

Tabla message_ephemeral

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma. Por el nombre de la tabla podría estar destinada a guardar mensajes “efímeros” es decir que se borran pasado un tiempo (funcionalidad anunciada en varios medios)

The screenshot shows a database schema editor interface with a toolbar at the top featuring tabs for 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. The 'Columns X' tab is active. Below the toolbar is a table with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains three checked checkboxes. The 'Name' column lists three columns: 'message_row_id', 'duration', and 'expire_timestamp'. The 'Details' column specifies their types as 'integer', 'integer not null', and 'integer not null' respectively.

Visible	Name	Details
<input checked="" type="checkbox"/>	① message_row_id	integer
<input checked="" type="checkbox"/>	duration	integer not null
<input checked="" type="checkbox"/>	expire_timestamp	integer not null

Ilustración 43 Esquema de la tabla message_ephemeral

Tabla message_ephemeral_setting

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows a database schema editor interface with a toolbar at the top featuring tabs for 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. The 'Columns X' tab is active. Below the toolbar is a table with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains two checked checkboxes. The 'Name' column lists two columns: 'message_row_id' and 'setting_duration'. The 'Details' column specifies their types as 'integer' and 'integer' respectively.

Visible	Name	Details
<input checked="" type="checkbox"/>	① message_row_id	integer
<input checked="" type="checkbox"/>	setting_duration	integer

Ilustración 44 Esquema de la tabla message_ephemeral_setting

Tabla message_external_ad_content

Tabla que en la muestra analizada no es utilizada por lo únicamente se muestra la estructura de la misma.

The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	title	text
<input checked="" type="checkbox"/>	body	text
<input checked="" type="checkbox"/>	media_type	integer
<input checked="" type="checkbox"/>	thumbnail_url	text
<input checked="" type="checkbox"/>	full_thumbnail	blob
<input checked="" type="checkbox"/>	micro_thumbnail	blob
<input checked="" type="checkbox"/>	media_url	text
<input checked="" type="checkbox"/>	source_type	text
<input checked="" type="checkbox"/>	source_id	text
<input checked="" type="checkbox"/>	source_url	text

Ilustración 45 Esquema de la tabla message_external_ad_content

Tabla message forwarded

Tabla que en la muestra analizada que contiene información sobre los mensajes que han sido reenviados.

The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	forward_score	integer

Ilustración 46

campo	Tipo	Descripción
message_row_id	Entero	Número de registro de la tabla messages que ha sido reenviado
forward_score	Entero	Número de veces que ha sido reenviado

Tabla 31 Contenido de la tabla message_forwarded

Tabla message_ftsv2

Tabla que en la muestra información sobre los mensajes que han sido enviados desde el teléfono analizado. La estructura de la tabla es la siguiente

Visible	Name	Details
<input checked="" type="checkbox"/>	content	enum
<input checked="" type="checkbox"/>	fts_jid	enum
<input checked="" type="checkbox"/>	fts_namespace	enum

Ilustración 47 Esquema de la tabla message_ftsv2

El contenido de la tabla es el siguiente

campo	Tipo	Descripción
content	Enum	Campo que contiene el campo enviado en un mensaje
fts_jid	Enum	Desconocido, los valores que muestra son "0 f", "f e", "h j", "h e", "f e".
fts_namespace	Enum	Presenta distintos valores Blanco para mensajes de texto "fv" para mensaje de vídeo "fa" para mensajes de audio "fi" para ubicación "fd" para documento

Tabla 32 Contenido de la tabla message_ftwv2

Tabla message_ftsv2_content

Tabla que en la muestra información sobre los mensajes que han sido enviados desde el teléfono analizado. La estructura de la tabla es la siguiente

Visible	Name	Details
<input checked="" type="checkbox"/>	docid	integer
<input checked="" type="checkbox"/>	c0content	enum
<input checked="" type="checkbox"/>	c1fts_jid	enum
<input checked="" type="checkbox"/>	c2fts_namespace	enum

Ilustración 48 Esquema de la tabla message_ftsv2_content

El contenido de la tabla es el siguiente

campo	Tipo	Descripción
docid	Integer	Número del mensaje, corresponde con el campo _id de la tabla messages
c0content	Enum	Campo que contiene el campo enviado en un mensaje
c1fts_jid	Enum	Desconocido, los valores que muestra son "0 f", "f e", "h j", "h e", "f e".
c2fts_namespace	Enum	Presenta distintos valores Blanco para mensajes de texto "fv" para mensaje de vídeo "fa" para mensajes de audio "fi" para ubicación "fd" para documento

Tabla 33 Contenido de la tabla message_ftsv2_content

Tabla message_ftsv2_docsizes

Tabla que en la muestra información sobre los mensajes que han sido enviados desde el teléfono analizado. La estructura de la tabla es la siguiente, aunque se desconoce su función

Visible	Name	Details
<input checked="" type="checkbox"/>	docid	integer
<input checked="" type="checkbox"/>	size	blob

Ilustración 49 Esquema de la tabla message_ftsv2_docsizes

El contenido de la tabla es el siguiente

campo	Tipo	Descripción
docid	Integer	Número del mensaje, corresponde con el campo _id de la tabla messages
Size	Blob	Campo binario que contiene en hexadecimal el tamaño de los mensajes de la tabla anterior.

Tabla 34 Contenido de la tabla message_ftsv2_docsizes

Tabla message_ftsv2_segdir

Tabla que en la muestra analizada se encuentra informada manteniendo información con las anteriores, pero de la que no se puede aportar información por lo que únicamente se muestra la estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	level	integer
<input checked="" type="checkbox"/>	idx	integer
<input checked="" type="checkbox"/>	start_block	integer
<input checked="" type="checkbox"/>	leaves_end_block	integer
<input checked="" type="checkbox"/>	end_block	integer
<input checked="" type="checkbox"/>	root	blob

Ilustración 50 Esquema de la tabla message_ftv2_segdir

Tabla message_ftsv2_segments

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	blockid	integer
<input checked="" type="checkbox"/>	block	blob

Ilustración 51 Esquema de la tabla message_ftv2_segments

Tabla message_ftv2_stats

Tabla que en la muestra analizada se encuentra informada manteniendo información con las anteriores, pero de la que no se puede aportar información por lo que únicamente se muestra la estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	id	integer
<input checked="" type="checkbox"/>	value	blob

Ilustración 52 Esquema de la tabla message_ftv2_stats

Tabla message_future

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	version	integer
<input checked="" type="checkbox"/>	data	blob

Ilustración 53 Esquema de la tabla message_future

Tabla message_group_invite

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	group_jid_row_id	integer not null
<input checked="" type="checkbox"/>	admin_jid_row_id	integer not null
<input checked="" type="checkbox"/>	group_name	text
<input checked="" type="checkbox"/>	invite_code	text
<input checked="" type="checkbox"/>	expiration	integer
<input checked="" type="checkbox"/>	invite_time	integer
<input checked="" type="checkbox"/>	expired	integer

Ilustración 54 Esquema de la tabla message_group_invite

Tabla message_link

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible		Name	Details
<input checked="" type="checkbox"/>	_id		integer
<input checked="" type="checkbox"/>	== chat_row_id		integer
<input checked="" type="checkbox"/>	== message_row_id		integer
<input checked="" type="checkbox"/>	== link_index		integer

Ilustración 55 Esquema de la tabla message_link

Tabla message_location

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible		Name	Details
<input checked="" type="checkbox"/>	message_row_id		integer
<input checked="" type="checkbox"/>	== chat_row_id		integer
<input checked="" type="checkbox"/>	== latitude		real
<input checked="" type="checkbox"/>	== longitude		real
<input checked="" type="checkbox"/>	== place_name		text
<input checked="" type="checkbox"/>	== place_address		text
<input checked="" type="checkbox"/>	== url		text
<input checked="" type="checkbox"/>	== live_location_share_duration		integer
<input checked="" type="checkbox"/>	== live_location_sequence_number		integer
<input checked="" type="checkbox"/>	== live_location_final_latitude		real
<input checked="" type="checkbox"/>	== live_location_final_longitude		real
<input checked="" type="checkbox"/>	== live_location_final_timestamp		integer
<input checked="" type="checkbox"/>	== map_download_status		integer

Ilustración 56 Esquema de la tabla message_location

Tabla message_media

Tabla que en las muestras analizadas contiene información sobre los contenidos enviados en los mensajes. La estructura es la siguiente

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	chat_row_id	integer
<input checked="" type="checkbox"/>	autotransfer_retry_enabled	integer
<input checked="" type="checkbox"/>	multicast_id	text
<input checked="" type="checkbox"/>	media_job_uuid	text
<input checked="" type="checkbox"/>	transferred	integer
<input checked="" type="checkbox"/>	transcoded	integer
<input checked="" type="checkbox"/>	file_path	text
<input checked="" type="checkbox"/>	file_size	integer
<input checked="" type="checkbox"/>	suspicious_content	integer
<input checked="" type="checkbox"/>	trim_from	integer
<input checked="" type="checkbox"/>	trim_to	integer
<input checked="" type="checkbox"/>	face_x	integer
<input checked="" type="checkbox"/>	face_y	integer
<input checked="" type="checkbox"/>	media_key	blob
<input checked="" type="checkbox"/>	media_key_timestamp	integer
<input checked="" type="checkbox"/>	width	integer
<input checked="" type="checkbox"/>	height	integer
<input checked="" type="checkbox"/>	has_streaming_sidecar	integer
<input checked="" type="checkbox"/>	gif_attribution	integer
<input checked="" type="checkbox"/>	thumbnail_height_width_ratio	real
<input checked="" type="checkbox"/>	direct_path	text
<input checked="" type="checkbox"/>	first_scan_sidecar	blob
<input checked="" type="checkbox"/>	first_scan_length	integer
<input checked="" type="checkbox"/>	message_url	text
<input checked="" type="checkbox"/>	mime_type	text
<input checked="" type="checkbox"/>	file_length	integer
<input checked="" type="checkbox"/>	media_name	text
<input checked="" type="checkbox"/>	file_hash	text
<input checked="" type="checkbox"/>	media_duration	integer
<input checked="" type="checkbox"/>	page_count	integer
<input checked="" type="checkbox"/>	enc_file_hash	text
<input checked="" type="checkbox"/>	partial_media_hash	text
<input checked="" type="checkbox"/>	partial_media_enc_hash	text
<input checked="" type="checkbox"/>	is_animated_sticker	integer
<input checked="" type="checkbox"/>	original_file_hash	text

Ilustración 57 Esquema de la tabla message_media

Campo	Tipo	Descripción
message_row_id	Entero	Número identificador de mensaje definido en la tabla messages
chat_row_id	Texto	Número identificador del chat definido en la tabla chats
autotransfer_retry_enabled	Texto	Campo que toma valor 1 si está activado el reenvío automático de mensaje en el momento del envío del mensaje
multicast_id	Entero	Desconocido, en las muestras analizadas toma valor nulo
media_job_uuid	Entero	Identificador del medio enviado
Transferred	Entero	Valor 1 si el objeto ha sido enviado
transcoded	Texto	Valor 0 si no ha sido convertido o 1 si ha sido convertido
file_path	Texto	Ruta a la ubicación en local donde se almacena el fichero tras su descarga por parte del usuario
file_size	Entero	Tamaño del fichero en bytes
suspicious_content	Entero	Valor 1 si los servidores de WhatsApp detectan contenido sospechoso, 0 en caso contrario
trim_from	Entero	Desconocido, en la muestra analizada el valor es 0
trim_to	Entero	Desconocido en la muestra analizada el valor es 0
face_x	Entero	Desconocido

face_y	Entero	Desconocido
media_key	Blob	Clave asociada al fichero, se usa para descifrar la url incluida en el campo message_url
media_key_timestamp	Entero	Timestamp en formato Unix Epoch Time asociado al campo anterior
Width	Entero	Anchura en pixels
height	Entero	Altura en pixels
has_streaming_sidecar	Entero	Valor 1 si dispone de versión en streaming y 0 en caso contrario
gif_attribution	Entero	En la muestra analizada el valor es 0
thumbnail_height_width_ratio	Real	Ratio de tamaño del thumbnail
direct_path	Texto	Este campo contiene una ruta de la ubicación del objeto, pero no en el terminal del usuario
first_scan_sidecar	Blob	Desconocido
first_scan_length	Entero	Valor 0 excepto para aquellas filas que tengan informado el campo anterior
message_url	Texto	Url que pueda estar cifrada (extension .enc), en este caso la aplicación la descifraría con la clave definida en el campo media_key
mime_type	Texto	Tipo mime (application/pdf, audio/ogg, video/mp4, etc)

file_length	Entero	Longitud del objeto en bytes
media_name	Texto	Nombre del objeto en el terminal que envía el mensaje, se trata del nombre del fichero local no se completa en la base de datos del destino.
file_hash	Texto	Hash del fichero
media_duration	Entero	Duración del objeto en segundos (0 en caso de documentos u otros objetos sin duración)
page_count	Entero	Número de páginas (0 para objetos que no tienen páginas)
enc_file_hash	Texto	Hash del fichero cifrado
partial_media_hash	Texto	Hash del objeto (en la muestra analizada está con valor nulo excepto para un fichero de imagen) sin un mime type asociado
partial_media_enc_hash	Texto	Hash del objeto cifrado (en la muestra analizada está con valor nulo excepto para un fichero de imagen) sin un mime type asociado
is_animated_sticker	Entero	Valor 1 si es un sticker animado, 0 para el resto.

original_file_hash	Texto	En la muestra analizada este campo tiene valor nulo
---------------------------	-------	---

Tabla 35 Contenido de la tabla message_media

Tabla message_media_interactive_annotation

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ message_row_id	integer
<input checked="" type="checkbox"/>	⇒ location_latitude	real
<input checked="" type="checkbox"/>	⇒ location_longitude	real
<input checked="" type="checkbox"/>	⇒ location_name	text
<input checked="" type="checkbox"/>	⌚ sort_order	integer

Ilustración 58 Esquema de la tabla message_media_interactive_annotation

Tabla message_media_annotation_vertex

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ message_media_interactive_annotation_row_id	integer
<input checked="" type="checkbox"/>	⇒ x	real
<input checked="" type="checkbox"/>	⇒ y	real
<input checked="" type="checkbox"/>	⌚ sort_order	integer

Ilustración 59 Esquema de la tabla message_media_annotation_vertex

Tabla message_media_vcard_count

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows the 'Columns' tab of the MySQL Workbench interface. The table structure is as follows:

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① message_row_id	integer
<input checked="" type="checkbox"/>	== count	integer

Ilustración 60 Esquema de la tabla message_media_vcard_count

Tabla message_mentions

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows the 'Columns' tab of the MySQL Workbench interface. The table structure is as follows:

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① message_row_id	integer
<input checked="" type="checkbox"/>	① jid_row_id	integer

Ilustración 61 Esquema de la tabla message_mentions

Tabla message_orphaned_edit

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows the 'Columns' tab of the MySQL Workbench interface. The table structure is as follows:

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① key_id	text not null
<input checked="" type="checkbox"/>	① from_me	integer not null
<input checked="" type="checkbox"/>	① chat_row_id	integer not null
<input checked="" type="checkbox"/>	① sender_jid_row_id	integer not null default 0
<input checked="" type="checkbox"/>	== timestamp	integer
<input checked="" type="checkbox"/>	== message_type	integer not null
<input checked="" type="checkbox"/>	== revoked_key_id	text
<input checked="" type="checkbox"/>	== retry_count	integer

Ilustración 62 Esquema de la tabla message_orphaned_edit

Tabla message_payment

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	sender_jid_row_id	integer
<input checked="" type="checkbox"/>	receiver_jid_row_id	integer
<input checked="" type="checkbox"/>	amount_with_symbol	text
<input checked="" type="checkbox"/>	remote_resource	text
<input checked="" type="checkbox"/>	remote_message_sender_jid_row_id	integer
<input checked="" type="checkbox"/>	remote_message_from_me	integer
<input checked="" type="checkbox"/>	remote_message_key	text

Ilustración 63 Esquema de la tabla message_payments

Tabla message_payment_status_update

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	transaction_info	text
<input checked="" type="checkbox"/>	transaction_data	text
<input checked="" type="checkbox"/>	init_timestamp	text
<input checked="" type="checkbox"/>	update_timestamp	text
<input checked="" type="checkbox"/>	amount_data	text

Ilustración 64 Esquema de la tabla message_payment_status_update

Tabla message_payment_transaction_reminder

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	web_stub	text
<input checked="" type="checkbox"/>	amount	text
<input checked="" type="checkbox"/>	transfer_date	text
<input checked="" type="checkbox"/>	payment_sender_name	text
<input checked="" type="checkbox"/>	expiration	integer
<input checked="" type="checkbox"/>	remote_message_key	text

Ilustración 65 Esquema de la tabla message_payment_transaction_reminder

Tabla message_product

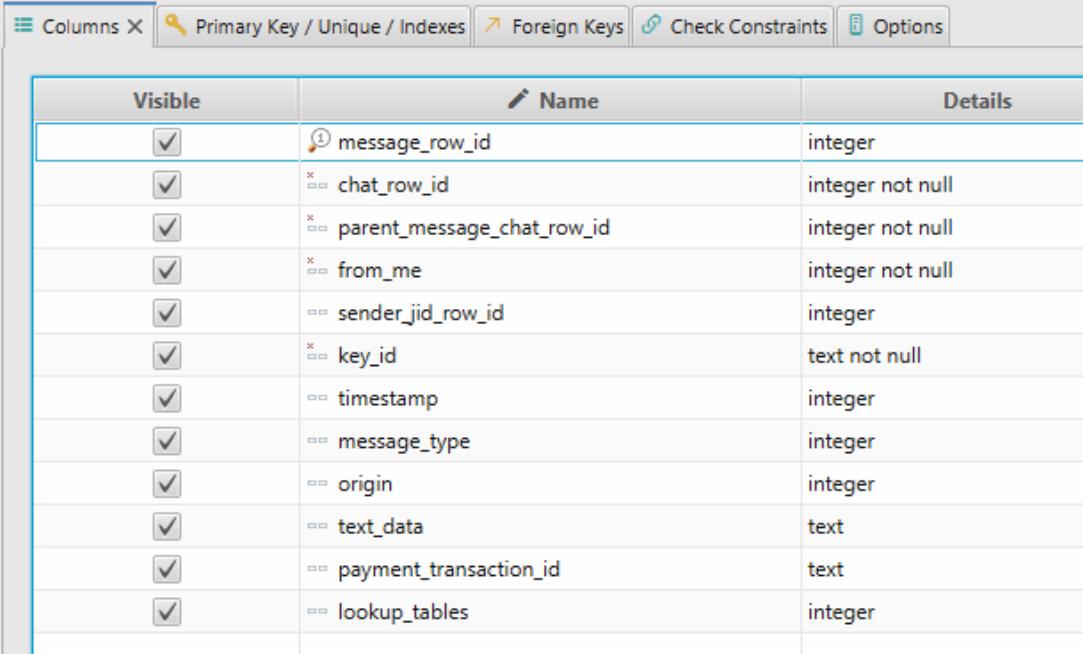
Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	business_owner_jid	integer
<input checked="" type="checkbox"/>	product_id	text
<input checked="" type="checkbox"/>	title	text
<input checked="" type="checkbox"/>	description	text
<input checked="" type="checkbox"/>	currency_code	text
<input checked="" type="checkbox"/>	amount_1000	integer
<input checked="" type="checkbox"/>	retailer_id	text
<input checked="" type="checkbox"/>	url	text
<input checked="" type="checkbox"/>	product_image_count	integer

Ilustración 66 Esquema de la tabla message_product

Tabla message_quoted

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.



The screenshot shows a database schema viewer with the following interface elements:

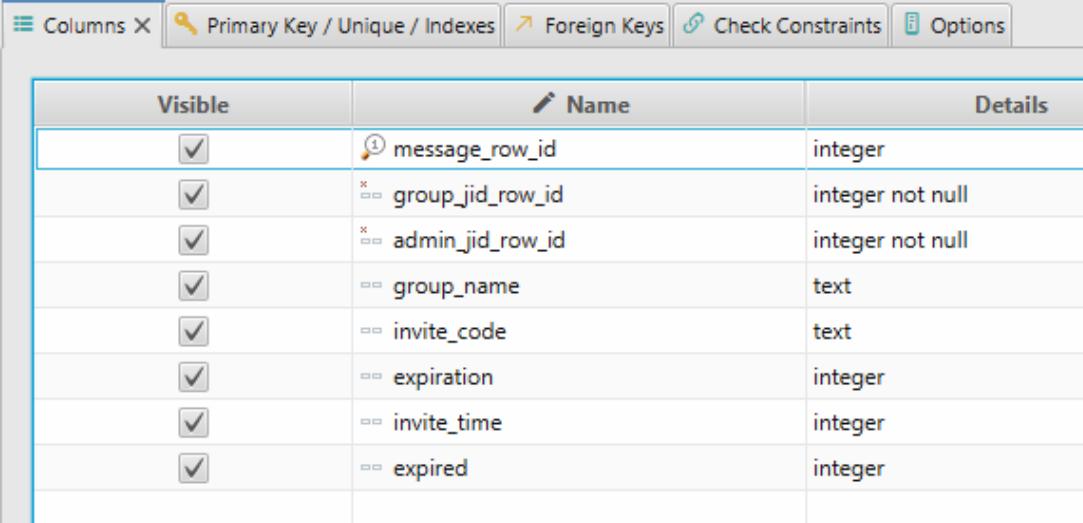
- Top navigation bar: Columns X, Primary Key / Unique / Indexes, Foreign Keys, Check Constraints, Options.
- Table header: Visible, Name, Details.
- Table body: 12 rows of columns, all checked as visible.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	chat_row_id	integer not null
<input checked="" type="checkbox"/>	parent_message_chat_row_id	integer not null
<input checked="" type="checkbox"/>	from_me	integer not null
<input checked="" type="checkbox"/>	sender_jid_row_id	integer
<input checked="" type="checkbox"/>	key_id	text not null
<input checked="" type="checkbox"/>	timestamp	integer
<input checked="" type="checkbox"/>	message_type	integer
<input checked="" type="checkbox"/>	origin	integer
<input checked="" type="checkbox"/>	text_data	text
<input checked="" type="checkbox"/>	payment_transaction_id	text
<input checked="" type="checkbox"/>	lookup_tables	integer

Ilustración 67 Esquema de la tabla message_quoted

Tabla message_quoted_group_invite

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.



The screenshot shows a database schema viewer with the following interface elements:

- Top navigation bar: Columns X, Primary Key / Unique / Indexes, Foreign Keys, Check Constraints, Options.
- Table header: Visible, Name, Details.
- Table body: 8 rows of columns, all checked as visible.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	group_jid_row_id	integer not null
<input checked="" type="checkbox"/>	admin_jid_row_id	integer not null
<input checked="" type="checkbox"/>	group_name	text
<input checked="" type="checkbox"/>	invite_code	text
<input checked="" type="checkbox"/>	expiration	integer
<input checked="" type="checkbox"/>	invite_time	integer
<input checked="" type="checkbox"/>	expired	integer

Ilustración 68 Esquema de la tabla message_quoted_group_invite

Tabla message_quoted_group_invite_legacy

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	group_jid_row_id	integer not null
<input checked="" type="checkbox"/>	admin_jid_row_id	integer not null
<input checked="" type="checkbox"/>	group_name	text
<input checked="" type="checkbox"/>	invite_code	text
<input checked="" type="checkbox"/>	expiration	integer
<input checked="" type="checkbox"/>	invite_time	integer
<input checked="" type="checkbox"/>	expired	integer

Ilustración 69 Esquema de la tabla message_quoted_group_invite_legacy

Tabla message_location

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	latitude	real
<input checked="" type="checkbox"/>	longitude	real
<input checked="" type="checkbox"/>	place_name	text
<input checked="" type="checkbox"/>	place_address	text
<input checked="" type="checkbox"/>	url	text
<input checked="" type="checkbox"/>	thumbnail	blob

Ilustración 70 Esquema de la tabla message_location

Tabla message_media

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a database schema viewer with the following interface elements at the top:

- Columns X
- Primary Key / Unique / Indexes
- Foreign Keys
- Check Constraints
- Options

The main area displays a table with three columns: Visible, Name, and Details. The table contains 18 rows, each representing a column in the message_media table. All columns are marked as visible (checked). The details for each column are as follows:

Visible	Name	Details
✓	① message_row_id	integer
✓	media_job_uuid	text
✓	transferred	integer
✓	file_path	text
✓	file_size	integer
✓	media_key	blob
✓	media_key_timestamp	integer
✓	width	integer
✓	height	integer
✓	direct_path	text
✓	message_url	text
✓	mime_type	text
✓	file_length	integer
✓	media_name	text
✓	file_hash	text
✓	media_duration	integer
✓	page_count	integer
✓	enc_file_hash	text
✓	thumbnail	blob

Ilustración 71 Esquema de la tabla message_media

Tabla message_mentions

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a database schema viewer with the following interface elements at the top:

- Columns X
- Primary Key / Unique / Indexes
- Foreign Keys
- Check Constraints
- Options

The main area displays a table with three columns: Visible, Name, and Detail. The table contains 3 rows, each representing a column in the message_mentions table. All columns are marked as visible (checked). The details for each column are as follows:

Visible	Name	Detail
✓	① _id	integer
✓	① message_row_id	integer
✓	① jid_row_id	integer

Ilustración 72 Esquema de la tabla message_mentions

Tabla message_quoted_product

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a database schema editor interface with a toolbar at the top containing buttons for 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. Below the toolbar is a table structure with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains checkboxes, all of which are checked for every row. The 'Name' column lists the column names, and the 'Details' column lists their data types. The columns are:

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	business_owner_jid	integer
<input checked="" type="checkbox"/>	url	text
<input checked="" type="checkbox"/>	product_id	text
<input checked="" type="checkbox"/>	title	text
<input checked="" type="checkbox"/>	description	text
<input checked="" type="checkbox"/>	currency_code	text
<input checked="" type="checkbox"/>	amount_1000	integer
<input checked="" type="checkbox"/>	retailer_id	text
<input checked="" type="checkbox"/>	product_image_count	integer

Ilustración 73 Esquema de la tabla message_quoted_product

Tabla message_quoted_text

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a database schema editor interface with a toolbar at the top containing buttons for 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. Below the toolbar is a table structure with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains checkboxes, both of which are checked for every row. The 'Name' column lists the column names, and the 'Details' column lists their data types. The columns are:

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	thumbnail	blob

Ilustración 74 Esquema de la tabla message_quoted_text

Tabla message_quoted_vcard

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ message_row_id	integer
<input checked="" type="checkbox"/>	⌚ vcard	text

Ilustración 75 Esquema de la tabla message_quoted_vcard

Tabla message_revoked

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ message_row_id	integer
<input checked="" type="checkbox"/>	⌚ revoked_key_id	text not null

Ilustración 76 Esquema de la tabla message_revoked

Tabla message_send_count

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ message_row_id	integer
<input checked="" type="checkbox"/>	⌚ send_count	integer

Ilustración 77 Esquema de la tabla message_send_count

la message_streaming_sidecar

Tabla que contiene información sobre aquellos videos que pueden ser visualizados en streaming. La estructura de la tabla se muestra a continuación.

Visible	Name	Details
<input checked="" type="checkbox"/>	① message_row_id	integer
<input checked="" type="checkbox"/>	--- sidecar	blob
<input checked="" type="checkbox"/>	--- chunk_lengths	blob
<input checked="" type="checkbox"/>	--- timestamp	integer

Ilustración 78 Esquema de la tabla message_streaming_sidecar

El contenido de los campos es el siguiente.

Campo	Tipo	Descripción
message_row_id	Entero	Número identificador de mensaje definido en la tabla messages
sidecar	Blob	Campo binario con información del objeto
chunk_lengths	Blob	Campo binario con información del objeto
Timestamp	Entero	Timestamp asociado al registro

Tabla 36 Contenido de la tabla message_streaming_sidecar

Tabla message_system

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	① message_row_id	integer
<input checked="" type="checkbox"/>	--- action_type	integer not null

Ilustración 79 Esquema de la tabla message_system

Tabla message_system_block_contact

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Columns X			Primary Key / Unique / Indexes	Foreign Keys	Check Constraints	Options
Visible	Name	Details				
<input checked="" type="checkbox"/>	message_row_id	integer				
<input checked="" type="checkbox"/>	is_blocked	integer				

Ilustración 80 Esquema de la tabla message_system_block_contact

Tabla message_system_chat_participant

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Columns X			Primary Key / Unique / Indexes	Foreign Keys	Check Constraints	Options
Visible	Name	Details				
<input checked="" type="checkbox"/>	message_row_id	integer				
<input checked="" type="checkbox"/>	user_jid_row_id	integer				

Ilustración 81 Esquema de la tabla message_system_chat_participant

Tabla message_system_device_change

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Columns X			Primary Key / Unique / Indexes	Foreign Keys	Check Constraints	Options
Visible	Name	Details				
<input checked="" type="checkbox"/>	message_row_id	integer				
<input checked="" type="checkbox"/>	device_added_count	integer				
<input checked="" type="checkbox"/>	device_removed_count	integer				

Ilustración 82 Esquema de la tabla message_system_device_change

Tabla message_system_ephemeral_setting_not_applied

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	setting_duration	integer

Ilustración 83 Esquema de la tabla message_system_ephemeral_setting_not_applied

Tabla message_system_group

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	is_me_joined	integer

Ilustración 84 Esquema de la tabla message_system_group

Tabla message_system_number_change

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	old_jid_row_id	integer
<input checked="" type="checkbox"/>	new_jid_row_id	integer

Ilustración 85 Esquema de la tabla message_system_number_change

Tabla message_system_photo_change

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	new_photo_id	text
<input checked="" type="checkbox"/>	old_photo	blob
<input checked="" type="checkbox"/>	new_photo	blob

Ilustración 86 Esquema de la tabla message_system_photo_change

Tabla message_system_value_change

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	old_data	text

Ilustración 87 Esquema de la tabla message_system_value_change

Tabla message_template

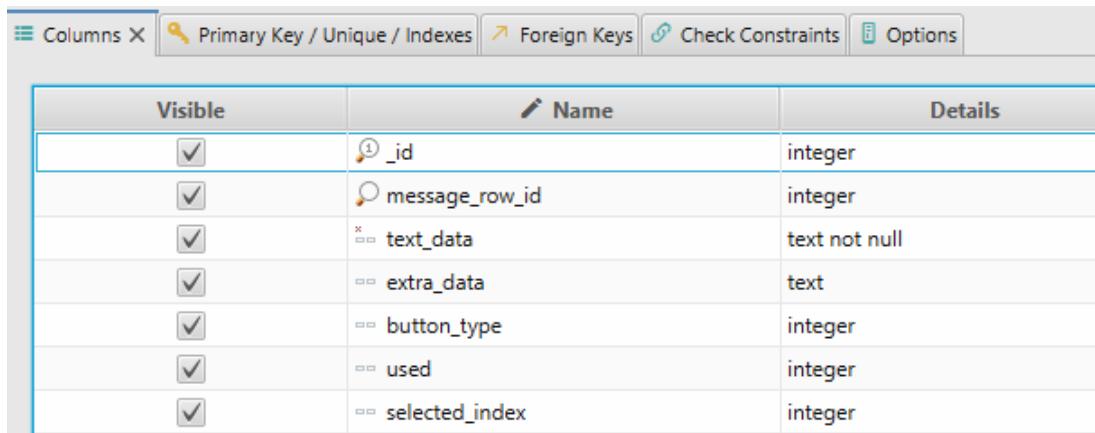
Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	content_text_data	text not null
<input checked="" type="checkbox"/>	footer_text_data	text

Ilustración 88 Esquema de la tabla message_template

bla message_template_button

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

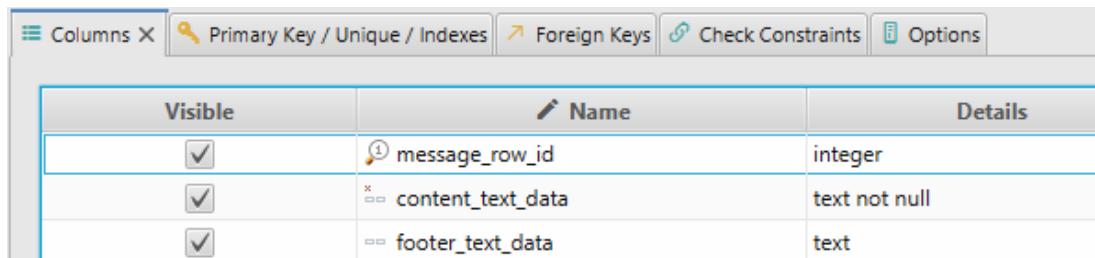


Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ message_row_id	integer
<input checked="" type="checkbox"/>	✉ text_data	text not null
<input checked="" type="checkbox"/>	✉ extra_data	text
<input checked="" type="checkbox"/>	✉ button_type	integer
<input checked="" type="checkbox"/>	✉ used	integer
<input checked="" type="checkbox"/>	✉ selected_index	integer

Ilustración 89 Esquema de la tabla message_template_button

Tabla message_template_quoted

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.



Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ message_row_id	integer
<input checked="" type="checkbox"/>	✉ content_text_data	text not null
<input checked="" type="checkbox"/>	✉ footer_text_data	text

Ilustración 90 Esquema de la tabla message_template_quoted

Tabla message_text

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a table structure for the 'message_text' table. The columns are listed in rows, each with a 'Visible' checkbox (all checked), a 'Name' field, and a 'Details' field. The columns are:

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	description	text
<input checked="" type="checkbox"/>	page_title	text
<input checked="" type="checkbox"/>	url	text
<input checked="" type="checkbox"/>	font_style	integer
<input checked="" type="checkbox"/>	text_color	integer
<input checked="" type="checkbox"/>	background_color	integer
<input checked="" type="checkbox"/>	preview_type	integer

Ilustración 91 Esquema de la tabla message_text

Tabla message_thumbnail

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a table structure for the 'message_thumbnail' table. The columns are listed in rows, each with a 'Visible' checkbox (both checked), a 'Name' field, and a 'Details' field. The columns are:

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	thumbnail	blob

Ilustración 92 Esquema de la tabla message_thumbnail

Tabla message_thumbnails

Tabla que contiene información sobre los thumbnails generados en los objetos enviados y recibidos. A continuación, se muestra su estructura.

The screenshot shows a table structure for the 'message_thumbnails' table. The columns are listed in rows, each with a 'Visible' checkbox (all checked), a 'Name' field, and a 'Details' field. The columns are:

Visible	Name	Details
<input checked="" type="checkbox"/>	thumbnail	blob
<input checked="" type="checkbox"/>	timestamp	datetime
<input checked="" type="checkbox"/>	key_remote_jid	text not null
<input checked="" type="checkbox"/>	key_from_me	integer
<input checked="" type="checkbox"/>	key_id	text not null

Ilustración 93 Esquema de la tabla message_thumbnails

El contenido de los campos es el siguiente

Campo	Tipo	Descripción
thumbnail	Blob	Campo binario con el contenido del thumbnail
timestamp	Datetime	Timestamp de la fecha de generación del thumbnail
key_remote_id	Blob	Identificador del interlocutor remoto con del que se ha recibido o al que se le ha enviado el objeto
key_from_me	Entero	Indica valor 1 si es un envío o 0 si es una recepción
key_id	Texto	Identificador del objeto

Tabla 37 Contenido de la tabla message_thumbnails

Tabla message_vcard

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	vcard	text

Ilustración 94 Esquema de la tabla message_vcard

Tabla message_vcard_jid

Tabla que contiene información sobre las vcards en los objetos enviados y recibidos. A continuación, se muestra su estructura.

Columns X		Primary Key / Unique / Indexes	Foreign Keys	Check Constraints	Options
Visible	Name	Details			
<input checked="" type="checkbox"/>	① <u>_id</u>				integer
<input checked="" type="checkbox"/>	① <u>vcard_jid_row_id</u>				integer
<input checked="" type="checkbox"/>	① <u>vcard_row_id</u>				integer
<input checked="" type="checkbox"/>	① <u>message_row_id</u>				integer

Ilustración 95 Esquema de la tabla message_vcard_jid

El contenido de los campos es el siguiente

Campo	Tipo	Descripción
<u>_id</u>	Entero	Identificador de la tabla, entero incremental
<u>vcard_jid_row_id</u>	Entero	Fila asociada en la tabla vcar_jid
<u>vcard_row_id</u>	Entero	Desconocido, valor -1
<u>message_row_id</u>	Entero	Identificador de la fila de la tabla messages

Tabla 38 Contenido de la tabla message_vcard_jid

Tabla messages

Tabla que contiene la información más importante desde el punto de vista del analista forense ya que incluye los datos relativos a los mensajes enviados y recibidos en la cuenta analizada. A continuación, se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ key_remote_jid	text not null
<input checked="" type="checkbox"/>	⌚ key_from_me	integer
<input checked="" type="checkbox"/>	⌚ key_id	text not null
<input checked="" type="checkbox"/>	↪ status	integer
<input checked="" type="checkbox"/>	↪ needs_push	integer
<input checked="" type="checkbox"/>	↪ data	text
<input checked="" type="checkbox"/>	↪ timestamp	integer
<input checked="" type="checkbox"/>	↪ media_url	text
<input checked="" type="checkbox"/>	↪ media_mime_type	text
<input checked="" type="checkbox"/>	⌚ media_wa_type	text
<input checked="" type="checkbox"/>	↪ media_size	integer
<input checked="" type="checkbox"/>	↪ media_name	text
<input checked="" type="checkbox"/>	↪ media_caption	text
<input checked="" type="checkbox"/>	⌚ media_hash	text
<input checked="" type="checkbox"/>	↪ media_duration	integer
<input checked="" type="checkbox"/>	↪ origin	integer
<input checked="" type="checkbox"/>	↪ latitude	real
<input checked="" type="checkbox"/>	↪ longitude	real
<input checked="" type="checkbox"/>	↪ thumb_image	text
<input checked="" type="checkbox"/>	↪ remote_resource	text
<input checked="" type="checkbox"/>	↪ received_timestamp	integer
<input checked="" type="checkbox"/>	↪ send_timestamp	integer
<input checked="" type="checkbox"/>	↪ receipt_server_timestamp	integer
<input checked="" type="checkbox"/>	↪ receipt_device_timestamp	integer
<input checked="" type="checkbox"/>	↪ read_device_timestamp	integer

<input checked="" type="checkbox"/>	read_device_timestamp	integer
<input checked="" type="checkbox"/>	played_device_timestamp	integer
<input checked="" type="checkbox"/>	raw_data	blob
<input checked="" type="checkbox"/>	recipient_count	integer
<input checked="" type="checkbox"/>	participant_hash	text
<input checked="" type="checkbox"/>	starred	integer
<input checked="" type="checkbox"/>	quoted_row_id	integer
<input checked="" type="checkbox"/>	mentioned_jids	text
<input checked="" type="checkbox"/>	multicast_id	text
<input checked="" type="checkbox"/>	edit_version	integer
<input checked="" type="checkbox"/>	media_enc_hash	text
<input checked="" type="checkbox"/>	payment_transaction_id	text
<input checked="" type="checkbox"/>	forwarded	integer
<input checked="" type="checkbox"/>	preview_type	integer
<input checked="" type="checkbox"/>	send_count	integer

Ilustración 96 Esquema de la tabla messages

La descripción de los campos es la siguiente

Campo	Tipo	Descripción
_id	Entero	Número de secuencia del registro que establece el propio SQLite para cada registro introducido en la tabla
key_remote_jid	Texto	Número identificador de WhatsApp del interlocutor con el que se mantiene la conversación.
key_from_me	Entero	Campo que indica la dirección de la comunicación si es un mensaje enviado por el terminal que aloja la base de datos (valor 1) o si somos los destinatarios del mensaje (valor 1)
key_id	Texto	Identificador único del mensaje
status	Texto	Estado del mensaje que toma un valor entre los siguientes posibles. <ul style="list-style-type: none"> • 0 Indica que el mensaje ha sido recibido

		<ul style="list-style-type: none"> • 3 Indica que no se ha podido entregar el mensaje en el servidor • 4 Indica que el mensaje ha sido enviado al servidor pero todavía no ha sido entregado en destino • 5 Indica que el mensaje ha sido enviado y recibido en el terminal destino • 6 Indica que se trata de un mensaje de control. P.e. que se ha añadido al usuario a un grupo • 13 indica que el mensaje ha sido leído, por ejemplo, al abrir un fichero enviado.
needs_push	Entero	Campo que toma valor 2 en caso de que el mensaje sea un broadcast de una lista de distribución y 0 en caso contrario
Data	Texto	Contenido del mensaje. En las muestras analizadas toma valor cuando media_wa_type toma valor 0 (mensaje de texto) y 4 (Vcard).
Timestamp	Entero	Timestamp en formato UNIX Epoch Time de la fecha de envío/recepción del mensaje

media_url	Texto	URL del fichero transmitido, toma valor cuando media_wa_type toma valor 1, 2 , 3, 9 y 13 en el resto de los casos el valor es nulo.
media_mime_type	Texto	<p>Tipo mime del objeto enviado. En la muestra analizada se han encontrado los siguientes valores</p> <ul style="list-style-type: none"> • image/jpeg • audio/mpeg • audio/ogg; codecs=opus • video/mp4 • application/pdf • image/webp
media_wa_type	Texto	<p>Tipo de mensaje enviado.</p> <ul style="list-style-type: none"> • 0 – Mensaje de texto • 1 – Imagen • 2 – Audio • 3 y 13 – Vídeo • 4 – VCARD • 5 - Ubicación • 6 – Mensaje de control (por ejemplo, creación de grupo) • 7 - Enlace • 8 – Documento • 9 – Fichero pdf • 10 – Control. P.e. Cambio de número de teléfono de cuenta de WhatsApp • 11 – GIF animado • 12 – Mensaje de sistema • 14 – Mensaje grupal eliminado para todos • 15 – Sticker • 16 – Ubicación en tiempo real • 20 imagen (tipo mime image/webp)

media_size	Entero	Tamaño en bytes del objeto enviado, 0 si no es un objeto (p.e. un mensaje de texto)
media_name	Texto	Nombre del fichero que ha sido transmitido
media_caption	Texto	Mensaje de texto que se puede añadir cuando se envía un objeto (fotografía, vídeo, etc.)
media_hash	Blob	Hash del fichero enviado en base 64
media_duration	Entero	Duración del objeto enviado en segundos, si no tiene duración el valor es 0
origin	Entero	En la muestra analizada toma valor 2 en caso de que se trate de un mensaje broadcast (lista de distribución) y 0 en caso contrario
latitude	Real	Valor de la latitud de la ubicación (fija y en tiempo real), en otro caso el valor es 0.0
longitude	Real	Valor de la longitud de la ubicación (fija y en tiempo real), en otro caso el valor es 0.0
thumb_image	Blob	Binario que contiene la imagen thumbnail del objeto (en caso de un

		mensaje que permite generar thumbnail)
remote_resource	Texto	Identificador del remitente (únicamente para mensajes enviados en un grupo)
received_timestamp	Entero	Timestamp que refleja la hora de recepción del mensaje en formato Unix Epoch Time. En caso de un mensaje enviado desde el terminal el valor es -1.
send_timestamp	Entero	En todas las muestras analizadas el valor es -1, se infiere que es un campo no utilizado.
receipt_server_timestamp	Entero	Timestamp que refleja la hora en la que se recibe la confirmación de recepción del mensaje por parte de los servidores de WhatsApp en formato Unix Epoch Time. En caso de un mensaje enviado desde el terminal el valor es -1.
receipt_device_timestamp	Entero	Timestamp que refleja la hora en la que se recibe la confirmación de recepción del mensaje por parte del terminal destinatario de la comunicación en formato Unix

		Epoch Time. En caso de un mensaje enviado desde el terminal el valor es -1.
read_device_timestamp	Entero	Timestamp que refleja la hora de en la que es leído el mensaje en el terminal destino de la comunicación en formato Unix Epoch Time. El valor se toma de la hora del dispositivo. De no aplicar toma valor nulo.
played_device_timestamp	Entero	Timestamp que refleja la hora de en la que un objeto (vídeo, audio, nota de voz) es reproducido en el terminal destino de la comunicación en formato Unix Epoch Time. El valor se toma de la hora del dispositivo. De no aplicar toma valor nulo
raw_data	Blob	En la muestra analizada el valor es nulo
recipient_count	Entero	Número de destinatarios (para mensajes de lista de distribución)

participant_hash	Texto	Desconocido, contiene un hash cuando el mensaje se ha enviado a un grupo
starred	Entero	Valor 0 cuando se trata de un mensaje borrado para todos. En la muestra analizada para el resto de los registros el valor es nulo
quoted_row_id	Entero	Desconocido, en la muestra analizada el valor de este campo es 0
mentioned_jobs	Texto	Desconocido, valor 0
multicast_id	Texto	Desconocido valor 0
edit_version	Entero	Desconocido, valor 0 excepto en mensajes borrados para todos que toma valor 7
media_enc_hash	Texto	Hash cifrado del objeto enviado
payment_transaction_id	Texto	No usado
forwarded	Entero	Valor 0 cuando es un mensaje original y 1 cuando es un mensaje reenviado
preview_type	Entero	Desconocido, valor 0
send_count	Entero	No usado

Tabla 39 Contenido de la tabla messages

Tabla messages_dehydrated_hsm

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	message_elementname	text
<input checked="" type="checkbox"/>	message_namespace	text
<input checked="" type="checkbox"/>	message_lg	text

Ilustración 97 Esquema de la tabla messages_dehydrated_hsm

Tabla messages_fts

Tabla que en las muestras analizadas contiene el contenido de los mensajes de texto enviados y recibidos. FTS es el acrónimo de full text search (Wikipedia, 2020) y es el conjunto de técnicas que permite el análisis del texto de los mensajes para por ejemplo mostrar anuncios publicitarios en los banners. La estructura de la tabla es sencilla

Visible	Name	Details
<input checked="" type="checkbox"/>	content	enum

Ilustración 98 Esquema de la tabla messages_fts

En su único campo tal y como se comenta se detalla el contenido de los mensajes de texto enviados y recibidos por el usuario

Tabla message_fts_content

Tabla que en las muestras analizadas contiene el texto contenido de los mensajes enviados y recibidos y el identificador de la tabla messages que indica el número del registro en el que se encuentra este mensaje. La estructura de la tabla es sencilla

Visible	Name	Details
<input checked="" type="checkbox"/>	docid	integer
<input checked="" type="checkbox"/>	c0content	enum

Ilustración 99 Esquema de la tabla messages_fts_content

La descripción de los campos es la siguiente

Campo	Tipo	Descripción
docid	Entero	Representa el número de registro en la tabla messages que contiene el texto del mensaje
c0content	Enum	Texto del mensaje transmitido

Tabla 40 Contenido de la tabla messages_fts_content

Tabla messages_fts_segdir

Tabla que en las muestras analizadas se encuentra informada, pero se desconoce qué representan los campos que contiene tras al análisis de las muestras utilizadas por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	level	integer
<input checked="" type="checkbox"/>	idx	integer
<input checked="" type="checkbox"/>	start_block	integer
<input checked="" type="checkbox"/>	leaves_end_block	integer
<input checked="" type="checkbox"/>	end_block	integer
<input checked="" type="checkbox"/>	root	blob

Ilustración 100 Esquema de la tabla messages_fts_segdir

Tabla message_fts_segments

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	blockid	integer
<input checked="" type="checkbox"/>	block	blob

Ilustración 101 Esquema de la tabla messages_fts_segments

Tabla message hydrated four row template

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	message_template_id	text

Ilustración 102 Esquema de la tabla messages_hydrated_table

Tabla messages_links

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	key_remote_jid	text
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	link_index	integer

Ilustración 103 Esquema de la tabla messages_links

Tabla message_quotes

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	key_remote_jid	text not null
<input checked="" type="checkbox"/>	key_from_me	integer
<input checked="" type="checkbox"/>	key_id	text not null
<input checked="" type="checkbox"/>	status	integer
<input checked="" type="checkbox"/>	needs_push	integer
<input checked="" type="checkbox"/>	data	text
<input checked="" type="checkbox"/>	timestamp	integer
<input checked="" type="checkbox"/>	media_url	text
<input checked="" type="checkbox"/>	media_mime_type	text
<input checked="" type="checkbox"/>	media_wa_type	text
<input checked="" type="checkbox"/>	media_size	integer
<input checked="" type="checkbox"/>	media_name	text
<input checked="" type="checkbox"/>	media_caption	text
<input checked="" type="checkbox"/>	media_hash	text
<input checked="" type="checkbox"/>	media_duration	integer
<input checked="" type="checkbox"/>	origin	integer
<input checked="" type="checkbox"/>	latitude	real
<input checked="" type="checkbox"/>	longitude	real
<input checked="" type="checkbox"/>	thumb_image	text
<input checked="" type="checkbox"/>	remote_resource	text
<input checked="" type="checkbox"/>	received_timestamp	integer
<input checked="" type="checkbox"/>	send_timestamp	integer
<input checked="" type="checkbox"/>	receipt_server_timestamp	integer
<input checked="" type="checkbox"/>	receipt_device_timestamp	integer
<input checked="" type="checkbox"/>	read_device_timestamp	integer
<hr/>		
<input checked="" type="checkbox"/>	played_device_timestamp	integer
<input checked="" type="checkbox"/>	raw_data	blob
<input checked="" type="checkbox"/>	recipient_count	integer
<input checked="" type="checkbox"/>	participant_hash	text
<input checked="" type="checkbox"/>	starred	integer
<input checked="" type="checkbox"/>	quoted_row_id	integer
<input checked="" type="checkbox"/>	mentioned_jids	text
<input checked="" type="checkbox"/>	multicast_id	text
<input checked="" type="checkbox"/>	edit_version	integer
<input checked="" type="checkbox"/>	media_enc_hash	text
<input checked="" type="checkbox"/>	payment_transaction_id	text
<input checked="" type="checkbox"/>	forwarded	integer
<input checked="" type="checkbox"/>	preview_type	integer
<input checked="" type="checkbox"/>	send_count	integer

Ilustración 104 Esquema de la tabla messages_quotes

Tabla messages_vcards

Tabla que contiene información sobre las VCARDS transmitidas en la cuenta analizada. La estructura de la tabla es la siguiente.

Visible	Name	Type	Details
<input checked="" type="checkbox"/>	_id	integer	
<input checked="" type="checkbox"/>	message_row_id	integer	
<input checked="" type="checkbox"/>	sender_jid	text	
<input checked="" type="checkbox"/>	chat_jid	text	
<input checked="" type="checkbox"/>	vcard	text	

Ilustración 105 Esquema de la tabla messages_vcard

La descripción de los campos es la siguiente

Campo	Tipo	Descripción
_id	Entero	Contiene el identificador del registro en la tabla (definido por SQLite)
message_row_id	Entero	Identificador de la línea de mensaje en la tabla messages
sender_jid	Texto	Identificador del remitente del mensaje
chat_jid	Texto	Identificador del chat en el que se ha enviado el mensaje (coincide con el anterior campo para mensajes individuales y cambia para el caso de chats grupales)
Vcard	Texto	Contenido de la VCARD

Tabla 41 Contenido de la tabla messages_vcard

Tabla messages_vcards_jids

Tabla que contiene información sobre las VCARDS transmitidas en la cuenta analizada. La estructura de la tabla es la siguiente.

The screenshot shows a database schema editor with a toolbar at the top containing buttons for 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. Below the toolbar is a table structure with four columns: 'Visible', 'Name', 'Details', and 'Description'. The table has four rows, each with a checked 'Visible' checkbox. The columns are as follows:

Visible	Name	Details	Description
<input checked="" type="checkbox"/>	⌚ _id	integer	
<input checked="" type="checkbox"/>	⌚ message_row_id	integer	
<input checked="" type="checkbox"/>	⌚ vcard_jid	text	
<input checked="" type="checkbox"/>	⌚ vcard_row_id	integer	

Ilustración 106 Esquema de la tabla messages_vcards_jid

La descripción de los campos es la siguiente

Campo	Tipo	Descripción
_id	Entero	Contiene el identificador del registro en la tabla (definido por SQLite)
message_row_id	Entero	Identificador de la línea de mensaje en la tabla messages
vcard_jid	Texto	Identificador del remitente del mensaje
vcard_row_id	Texto	Número de línea en la tabla messages_vcard que contiene la vcard

Tabla 42 Contenido de la tabla messages_vcards_jid

Tabla missed_call_log_participant

Tabla que contiene información sobre las cuentas que participaron en llamadas perdidas y están reflejados en el log. La estructura de la tabla es la siguiente.

The screenshot shows a database schema editor with a toolbar at the top containing buttons for 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. Below the toolbar is a table structure with four columns: 'Visible', 'Name', 'Details', and 'Description'. The table has four rows, each with a checked 'Visible' checkbox. The columns are as follows:

Visible	Name	Details	Description
<input checked="" type="checkbox"/>	⌚ _id	integer	
<input checked="" type="checkbox"/>	⌚ call_logs_row_id	integer	
<input checked="" type="checkbox"/>	⌚ jid	text	
<input checked="" type="checkbox"/>	⌚ call_result	integer	

Ilustración 107 Esquema de la tabla missed_call_log_participant

La descripción de los campos es la siguiente

Campo	Tipo	Descripción
_id	Entero	Contiene el identificador del registro en la tabla (definido por SQLite)

call_logs_row_id	Entero	Identificador de la tabla call_logs que refleja la llamada
jid	Texto	Identificador del destinatario de la llamada que perdida
call_result	Texto	Resultado de la llamada, en las muestras analizadas se han identificado los siguientes valores <ul style="list-style-type: none">• 2 Llamada no contestada• 5 Llamada rechazada

Tabla 43 Contenido de la tabla missed_call_participants

Tabla missed call logs

Tabla que contiene información sobre las cuentas que participaron en llamadas perdidas y están reflejados en el log. La estructura de la tabla es la siguiente.

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	① message_row_id	integer
<input checked="" type="checkbox"/>	timestamp	integer
<input checked="" type="checkbox"/>	video_call	integer
<input checked="" type="checkbox"/>	group_jid_row_id	integer not null default 0

Ilustración 108 Esquema de la tabla missed_call_logs

La descripción de los campos es la siguiente

Campo	Tipo	Descripción
<code>_id</code>	Entero	Contiene el identificador del registro en la tabla (definido por SQLite)
<code>message_row_id</code>	Entero	Identificador de la tabla messages que refleja la llamada
<code>timestamp</code>	Entero	Timestamp de la llamada en formato UNIX epoch time

video_call	Entero	Valor 1 cuando se trata de una video llamada y 0 cuando es una llamada de audio
group_jid_row	Entero	Fila de la tabla group_jid que incluye el grupo en el que se realizó la llamada, 0 en caso de que no sea una llamada grupal

Tabla 44 Contenido de la tabla missed_call_logs

Tabla pay_transaction

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	remote_jid_row_id	integer
<input checked="" type="checkbox"/>	key_id	text
<input checked="" type="checkbox"/>	interop_id	text
<input checked="" type="checkbox"/>	id	text
<input checked="" type="checkbox"/>	timestamp	integer
<input checked="" type="checkbox"/>	status	integer
<input checked="" type="checkbox"/>	error_code	text
<input checked="" type="checkbox"/>	sender_jid_row_id	integer
<input checked="" type="checkbox"/>	receiver_jid_row_id	integer
<input checked="" type="checkbox"/>	type	integer
<input checked="" type="checkbox"/>	currency_code	text
<input checked="" type="checkbox"/>	amount_1000	enum
<input checked="" type="checkbox"/>	credential_id	text
<input checked="" type="checkbox"/>	methods	text
<input checked="" type="checkbox"/>	bank_transaction_id	text
<input checked="" type="checkbox"/>	metadata	text
<input checked="" type="checkbox"/>	init_timestamp	integer
<input checked="" type="checkbox"/>	request_key_id	text
<input checked="" type="checkbox"/>	country	text
<input checked="" type="checkbox"/>	version	integer
<input checked="" type="checkbox"/>	future_data	blob

Ilustración 109 Esquema de la tabla pay_transaction

Tabla pay_transactions

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a database schema editor interface with a toolbar at the top containing buttons for 'Columns', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. The main area is a table with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains checkboxes, all of which are checked for every row. The 'Name' column lists 20 field names, and the 'Details' column specifies their data types. The fields are:

Visible	Name	Details
<input checked="" type="checkbox"/>	key_remote_jid	text
<input checked="" type="checkbox"/>	key_from_me	integer
<input checked="" type="checkbox"/>	key_id	text
<input checked="" type="checkbox"/>	id	text
<input checked="" type="checkbox"/>	timestamp	integer
<input checked="" type="checkbox"/>	status	integer
<input checked="" type="checkbox"/>	error_code	text
<input checked="" type="checkbox"/>	sender	text
<input checked="" type="checkbox"/>	receiver	text
<input checked="" type="checkbox"/>	type	integer
<input checked="" type="checkbox"/>	currency	text
<input checked="" type="checkbox"/>	amount_1000	enum
<input checked="" type="checkbox"/>	credential_id	text
<input checked="" type="checkbox"/>	methods	text
<input checked="" type="checkbox"/>	bank_transaction_id	text
<input checked="" type="checkbox"/>	metadata	text
<input checked="" type="checkbox"/>	init_timestamp	integer
<input checked="" type="checkbox"/>	request_key_id	text
<input checked="" type="checkbox"/>	country	text
<input checked="" type="checkbox"/>	version	integer
<input checked="" type="checkbox"/>	future_data	blob

Ilustración 110 Esquema de la tabla pay_transactions

Tabla props

Tabla que contiene información sobre la aplicación. Se muestra su estructura

The screenshot shows a database schema editor interface with a toolbar at the top containing buttons for 'Columns', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. The main area is a table with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains checkboxes, all of which are checked for every row. The 'Name' column lists 3 field names, and the 'Details' column specifies their data types. The fields are:

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	key	text
<input checked="" type="checkbox"/>	value	text

Ilustración 111 Esquema de la tabla props

El contenido de los campos es el siguiente

Campo	Tipo	Descripción
<code>_id</code>	Entero	Contiene el identificador del registro en la tabla (definido por SQLite)
<code>key</code>	Entero	Identificador de la propiedad a registrar, por ejemplo: <code>fts_ready</code> , <code>chats_ready</code> , <code>msgstore_db_schema_version</code> , etc.
<code>value</code>	Entero	Valor asignado a la clave anterior

Tabla 45 Contenido de la tabla `props`

Tabla quick_replies

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Columns X			Primary Key / Unique / Indexes	Foreign Keys	Check Constraints	Options
Visible	Name	Details				
<input checked="" type="checkbox"/>	<code>_id</code>	integer				
<input checked="" type="checkbox"/>	<code>title</code>	text not null				
<input checked="" type="checkbox"/>	<code>content</code>	text not null				

Ilustración 112 Esquema de la tabla `quick_replies`

Tabla quick_reply_attachments

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Columns X			Primary Key / Unique / Indexes	Foreign Keys	Check Constraints	Options
Visible	Name	Details				
<input checked="" type="checkbox"/>	<code>_id</code>	integer				
<input checked="" type="checkbox"/>	<code>quick_reply_id</code>	text not null				
<input checked="" type="checkbox"/>	<code>uri</code>	text not null				
<input checked="" type="checkbox"/>	<code>caption</code>	text				
<input checked="" type="checkbox"/>	<code>media_type</code>	integer				

Ilustración 113 Esquema de la tabla `quick_reply_attachments`

Tabla quick_reply_keywords

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	quick_reply_id	text not null
<input checked="" type="checkbox"/>	keyword_id	text not null

Ilustración 114 Esquema de la tabla quick_reply_keywords

Tabla quick_reply_usage

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	quick_reply_id	text not null
<input checked="" type="checkbox"/>	usage_date	date
<input checked="" type="checkbox"/>	usage_count	integer

Ilustración 115 Esquema de la tabla quick_reply_usage

Tabla quoted_message_product

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	message_row_id	integer
<input checked="" type="checkbox"/>	business_owner_jid	integer
<input checked="" type="checkbox"/>	product_id	text
<input checked="" type="checkbox"/>	title	text
<input checked="" type="checkbox"/>	description	text
<input checked="" type="checkbox"/>	currency_code	text
<input checked="" type="checkbox"/>	amount_1000	integer
<input checked="" type="checkbox"/>	retailer_id	text
<input checked="" type="checkbox"/>	url	text
<input checked="" type="checkbox"/>	product_image_count	integer

Ilustración 116 Esquema de la tabla quoted_message_product

Tabla receipt_device

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

<input type="checkbox"/> Columns	<input type="checkbox"/> Primary Key / Unique / Indexes	<input type="checkbox"/> Foreign Keys	<input type="checkbox"/> Check Constraints	<input type="checkbox"/> Options
Visible	Name	Details		
<input checked="" type="checkbox"/>	① _id	integer		
<input checked="" type="checkbox"/>	① message_row_id	integer not null		
<input checked="" type="checkbox"/>	① receipt_device_jid_row_id	integer not null		
<input checked="" type="checkbox"/>	== receipt_device_timestamp	integer		

Ilustración 117 Esquema de la tabla receipt_device

Tabla receipt_orphaned

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

<input type="checkbox"/> Columns	<input type="checkbox"/> Primary Key / Unique / Indexes	<input type="checkbox"/> Foreign Keys	<input type="checkbox"/> Check Constraints	<input type="checkbox"/> Options
Visible	Name	Details		
<input checked="" type="checkbox"/>	① _id	integer		
<input checked="" type="checkbox"/>	① chat_row_id	integer not null		
<input checked="" type="checkbox"/>	① from_me	integer not null		
<input checked="" type="checkbox"/>	① key_id	text not null		
<input checked="" type="checkbox"/>	① receipt_device_jid_row_id	integer not null		
<input checked="" type="checkbox"/>	① receipt_recipient_jid_row_id	integer		
<input checked="" type="checkbox"/>	① status	integer		
<input checked="" type="checkbox"/>	== timestamp	integer		

Ilustración 118 Esquema de la tabla receipt_orphaned

Tabla receipt_user

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

<input type="checkbox"/> Columns	<input type="checkbox"/> Primary Key / Unique / Indexes	<input type="checkbox"/> Foreign Keys	<input type="checkbox"/> Check Constraints	<input type="checkbox"/> Options
Visible	Name	Details		
<input checked="" type="checkbox"/>	① _id	integer		
<input checked="" type="checkbox"/>	① message_row_id	integer not null		
<input checked="" type="checkbox"/>	① receipt_user_jid_row_id	integer not null		
<input checked="" type="checkbox"/>	== receipt_timestamp	integer		
<input checked="" type="checkbox"/>	== read_timestamp	integer		
<input checked="" type="checkbox"/>	== played_timestamp	integer		

Ilustración 119 Esquema de la tabla receipt_user

Tabla receipts

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	① _id	integer
<input checked="" type="checkbox"/>	* key_remote_jid	text not null
<input checked="" type="checkbox"/>	* key_id	text not null
<input checked="" type="checkbox"/>	remote_resource	text
<input checked="" type="checkbox"/>	receipt_device_timestamp	integer
<input checked="" type="checkbox"/>	read_device_timestamp	integer
<input checked="" type="checkbox"/>	played_device_timestamp	integer

Ilustración 120 Esquema de la tabla receipts

Tabla sqlite_sequence

Tabla que contiene información sobre los chats almacenados en la base de datos a través de distintas claves presentes en su estructura. El contenido de los campos es:

Campo	Tipo	Descripción
name	Entero	Identificador de la propiedad a registrar, por ejemplo: props (número de registros de esta tabla), messages (número de mensajes en la tabla messages), jid (identificadores de cuentas registradas en chats), deleted_chat_jobs (número de chats borrados), etc.
seq	Entero	Valor asignado a la clave anterior

Tabla 46 Contenido de la tabla sqlite_sequence

Tabla status

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ jid_row_id	integer
<input checked="" type="checkbox"/>	⌚ message_table_id	integer
<input checked="" type="checkbox"/>	⌚ last_read_message_table_id	integer
<input checked="" type="checkbox"/>	⌚ last_read_receipt_sent_message_table_id	integer
<input checked="" type="checkbox"/>	⌚ first_unread_message_table_id	integer
<input checked="" type="checkbox"/>	⌚ autodownload_limit_message_table_id	integer
<input checked="" type="checkbox"/>	⌚ timestamp	integer
<input checked="" type="checkbox"/>	⌚ unseen_count	integer
<input checked="" type="checkbox"/>	⌚ total_count	integer

Ilustración 121 Esquema de la tabla status

Tabla status_list

Tabla que en las muestras analizadas contiene un único registro con información que no acaba de tener sentido ya que se refiere a un contacto que no existe registrado en el campo key_remote_jid con valor 0@s.whatsapp.net, por lo que se asume que son datos de sistema y únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ key_remote_jid	text
<input checked="" type="checkbox"/>	⌚ message_table_id	integer
<input checked="" type="checkbox"/>	⌚ last_read_message_table_id	integer
<input checked="" type="checkbox"/>	⌚ last_read_receipt_sent_message_table_id	integer
<input checked="" type="checkbox"/>	⌚ first_unread_message_table_id	integer
<input checked="" type="checkbox"/>	⌚ autodownload_limit_message_table_id	integer
<input checked="" type="checkbox"/>	⌚ timestamp	integer
<input checked="" type="checkbox"/>	⌚ unseen_count	integer
<input checked="" type="checkbox"/>	⌚ total_count	integer

Ilustración 122 Esquema de la tabla status_list

Tabla user_device

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	user_jid_row_id	integer
<input checked="" type="checkbox"/>	device_jid_row_id	integer
<input checked="" type="checkbox"/>	key_index	integer not null default 0

Ilustración 123 Esquema de la tabla user_device

Tabla user_device_info

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	user_jid_row_id	integer
<input checked="" type="checkbox"/>	raw_id	integer not null
<input checked="" type="checkbox"/>	timestamp	integer not null

Ilustración 124 Esquema de la tabla user_device_info

5.2.9 ESTRUCTURA DE LA BASE DE DATOS PAYMENTS.DB

Base de datos que contiene información sobre pagos, funcionalidad que actualmente sólo está disponible en la India por lo que se trata de tablas vacías en la muestra analizada. Únicamente se mostrará la estructura de las mismas.

Tabla contacts

Visible	Name	Details
<input checked="" type="checkbox"/>	jid	enum not null
<input checked="" type="checkbox"/>	country_data	text
<input checked="" type="checkbox"/>	merchant	integer
<input checked="" type="checkbox"/>	default_payment_type	integer

Ilustración 125 Esquema de la tabla contacts

Tabla methods

Visible	Name	Details
✓	credential_id	text not null
✓	country	text
✓	readable_name	text
✓	issuer_name	text
✓	type	integer not null
✓	subtype	integer
✓	creation_ts	integer
✓	updated_ts	integer
✓	debit_mode	integer not null
✓	credit_mode	integer not null
✓	balance_1000	integer
✓	balance_ts	integer
✓	country_data	text
✓	icon	blob

Ilustración 126 Esquema de la tabla methods

Tabla tmp_transactions

Visible	Name	Details
✓	tmp_id	text not null
✓	tmp_metadata	text
✓	tmp_ts	integer

Ilustración 127 Esquema de la tabla tmp_transactions

5.2.10 ESTRUCTURA DE LA BASE DE DATOS STICKERS.DB

Esta base de datos contiene información sobre los stickers que contiene la aplicación, no es de información de interés para el análisis pericial por lo que únicamente se refleja una captura de la estructura de las mismas.

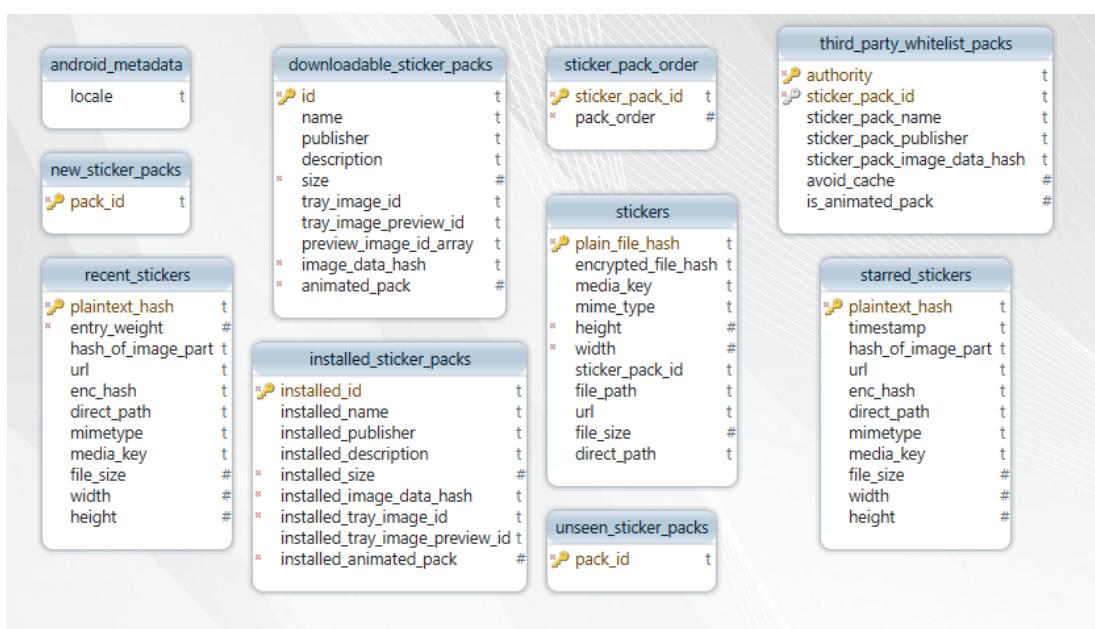


Ilustración 128 Esquema de la base de datos stickers.db

5.2.11 ESTRUCTURA DE LA BASE DE DATOS WA.DB

Esta junto con msgstore es la base de datos más importante desde el punto de vista forense. En la misma se almacena la información sobre los contactos de la cuenta. La estructura de tablas es la siguiente.

Esta base de datos contiene información sobre los stickers que contiene la aplicación, no es de información de interés para el análisis pericial por lo que únicamente se refleja una captura de la estructura de las mismas.

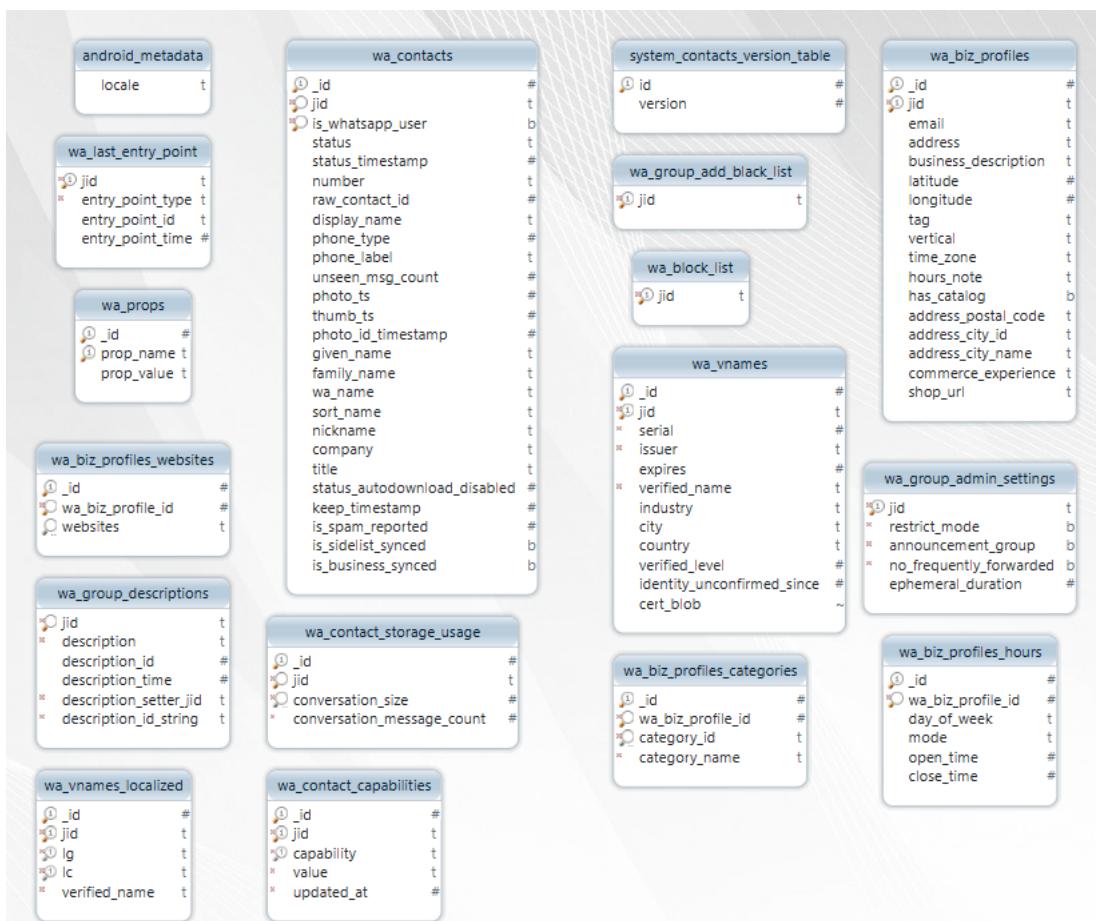


Ilustración 129 Esquema de la base de datos wa_contacts.db

Tabla android_metadata

Esta tabla tiene un único campo y un único registro, guarda el locale de la base de datos, en este caso el registro toma valor es_ES.

Tabla system_contacts_version_table

Tabla que en las muestras analizadas se encuentra informada aunque no se dispone información sobre el significado de sus campos. La estructura es la siguiente.

Columns X	Primary Key / Unique / Indexes	Foreign Keys	Check Constraints	Options
Visible			Name	
<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/> id	
<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/> version	

Ilustración 130 Esquema de la tabla system_contacts_version_table

Tabla wa_biz_profiles

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura. Esta tabla y las tres siguientes guardan información sobre empresas y son utilizadas por cuentas de negocio, en el presente trabajo el análisis se ha realizado sobre 148

cuentas particulares por lo que no se puede aportar información sobre el contenido de la tabla más allá que a través del nombre del campo, que realmente es explicativo en muchos de los casos.

The screenshot shows a database schema editor interface with a toolbar at the top containing buttons for 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. The main area is a table with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains checkboxes, all of which are checked for every row. The 'Name' column lists the field names, and the 'Details' column shows their data types. The columns are:

Visible	Name	Details
✓	_id	integer
✓	jid	text not null
✓	email	text
✓	address	text
✓	business_description	text
✓	latitude	real
✓	longitude	real
✓	tag	text
✓	vertical	text
✓	time_zone	text
✓	hours_note	text
✓	has_catalog	boolean default 0
✓	address_postal_code	text
✓	address_city_id	text
✓	address_city_name	text
✓	commerce_experience	text
✓	shop_url	text

Ilustración 131 Esquema de la tabla wa_biz_profiles

Tabla wa_biz_profiles_categories

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a database schema editor interface with a toolbar at the top containing buttons for 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options'. The main area is a table with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains checkboxes, all of which are checked for every row. The 'Name' column lists the field names, and the 'Details' column shows their data types. The columns are:

Visible	Name	Details
✓	_id	integer
✓	* wa_biz_profile_id	integer not null
✓	* category_id	text not null
✓	* category_name	text not null

Ilustración 132 Esquema de la tabla wa_biz_profiles_categories

Tabla wa_biz_profiles_hours

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	* wa_biz_profile_id	integer not null
<input checked="" type="checkbox"/>	day_of_week	text
<input checked="" type="checkbox"/>	mode	text
<input checked="" type="checkbox"/>	open_time	integer
<input checked="" type="checkbox"/>	close_time	integer

Ilustración 133 Esquema de la tabla wa_biz_profiles_hours

Tabla wa_biz_profiles_websites

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	* wa_biz_profile_id	integer not null
<input checked="" type="checkbox"/>	websites	text

Ilustración 134 Esquema de la tabla wa_biz_profiles_websites

Tabla wa_block_list

Tabla que contiene la lista de usuarios bloqueados, contiene un único campo jid que corresponde con el identificador de usuario de WhatsApp que ha sido bloqueado por el titular de la cuenta. La estructura de la tabla es la siguiente.

Visible	Name	Details
<input checked="" type="checkbox"/>	jid	text not null

Ilustración 135 Esquema de la tabla wa_block_list

Tabla wa_contact_capabilities

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a database schema editor interface with a toolbar at the top featuring 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options' buttons. Below the toolbar is a table structure with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains checkboxes, all of which are checked for every row. The 'Name' column lists the column names, and the 'Details' column lists their data types. The table has five rows:

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ jid	text not null
<input checked="" type="checkbox"/>	⌚ capability	text not null
<input checked="" type="checkbox"/>	⌚ value	text not null
<input checked="" type="checkbox"/>	⌚ updated_at	integer not null

Ilustración 136 Esquema de la tabla wa_contact_capabilities

Tabla wa_contact_storage_usage

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a database schema editor interface with a toolbar at the top featuring 'Columns X', 'Primary Key / Unique / Indexes', 'Foreign Keys', 'Check Constraints', and 'Options' buttons. Below the toolbar is a table structure with three columns: 'Visible', 'Name', and 'Details'. The 'Visible' column contains checkboxes, all of which are checked for every row. The 'Name' column lists the column names, and the 'Details' column lists their data types. The table has four rows:

Visible	Name	Details
<input checked="" type="checkbox"/>	⌚ _id	integer
<input checked="" type="checkbox"/>	⌚ jid	text not null
<input checked="" type="checkbox"/>	⌚ conversation_size	integer not null
<input checked="" type="checkbox"/>	⌚ conversation_message_count	integer not null

Ilustración 137 Esquema de la tabla wa_contact_storage_usage

Tabla wa_contacts

Esta tabla es la más importante desde el punto de vista del análisis forense ya que es la tabla que registra la información de los usuarios. La estructura de la misma es la siguiente.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	jid	text not null
<input checked="" type="checkbox"/>	is_whatsapp_user	boolean not null
<input checked="" type="checkbox"/>	-- status	text
<input checked="" type="checkbox"/>	-- status_timestamp	integer
<input checked="" type="checkbox"/>	-- number	text
<input checked="" type="checkbox"/>	-- raw_contact_id	integer
<input checked="" type="checkbox"/>	-- display_name	text
<input checked="" type="checkbox"/>	-- phone_type	integer
<input checked="" type="checkbox"/>	-- phone_label	text
<input checked="" type="checkbox"/>	-- unseen_msg_count	integer
<input checked="" type="checkbox"/>	-- photo_ts	integer
<input checked="" type="checkbox"/>	-- thumb_ts	integer
<input checked="" type="checkbox"/>	-- photo_id_timestamp	integer
<input checked="" type="checkbox"/>	-- given_name	text
<input checked="" type="checkbox"/>	-- family_name	text
<input checked="" type="checkbox"/>	-- wa_name	text
<input checked="" type="checkbox"/>	-- sort_name	text
<input checked="" type="checkbox"/>	-- nickname	text
<input checked="" type="checkbox"/>	-- company	text
<input checked="" type="checkbox"/>	-- title	text
<input checked="" type="checkbox"/>	-- status_autodownload_disabled	integer
<input checked="" type="checkbox"/>	-- keep_timestamp	integer
<input checked="" type="checkbox"/>	-- is_spam_reported	integer
<input checked="" type="checkbox"/>	-- is_sidelist_synced	boolean default 0
<input checked="" type="checkbox"/>	-- is_business_synced	boolean default 0

Ilustración 138 Esquema de la tabla wa_contacts

El contenido de los campos es el siguiente

Campo	Tipo	Descripción
_id	Entero	Identificador de la tabla, definido por el propio SQLite.
jid	Texto	Identificador del usuario de WhatsApp, formado de la misma manera que se comentaba en apartados anteriores, está compuesto por el número de

		teléfono del usuario, seguido de la cadena “@s.whatsapp.net”, para grupos se compone del número de teléfono del usuario que ha creado el grupo seguido de un “-” y el timestamp de la fecha de creación del grupo seguido de la cadena “@g.us”
is_whatsapp_user	Booleano	Los contactos son importados desde la agenda del teléfono del usuario, en este campo el valor es 1 si el contacto tiene una cuenta de WhatsApp asociada o 0 en caso contrario
status	Texto	Texto que se muestra en la línea de estado del usuario
status_timestamp	Entero	Timestamp en formato UNIX epoch time en el que se ha creado el status
number	Texto	Número de teléfono asociado al usuario
raw_contact_id	Entero	Número de secuencia asignado a un contacto, vacío para el caso de grupos
display_name	Texto	Nombre que se muestra en el contacto
phone_type	Entero	Tipo de teléfono, para las muestras analizadas el campo toma valor 2
phone_label	Texto	Etiqueta del teléfono. En la muestra analizada el valor es nulo excepto para los grupos que cuenta con un valor numérico

unseen_msg_count	Entero	Número de mensajes que han sido enviados por el usuario pero que todavía no han sido leídos por el contacto
photo_ts	Entero	Timestamp en formato UNIX epoch time que refleja la fecha/hora en la que la foto fue añadida por el contacto
thumb_ts	Entero	Timestamp en formato UNIX epoch time que refleja la fecha/hora en la que el thumbnail fue creado a partir de la foto. En la muestra analizada coincide con el valor del campo anterior.
photo_id_timestamp	Entero	Timestamp en formato UNIX epoch time que refleja la fecha/hora en la que la foto del contacto fue descargada al equipo local.
given_name	Texto	Nombre del contacto extraído de la agenda del terminal
family_name	Texto	Apellido del contacto extraído de la agenda del terminal
wa_name	Texto	Nombre de usuario definido en WhatsApp
sort_name	Texto	Nombre completo que se rellena bien con el wa_name si está disponible o con la suma de given_name y family_name (nombre y apellido)
nickname	Texto	Apodo del usuario si está definido en la agenda del terminal.
company	Texto	Empresa en la que trabaja si está definido en la agenda del terminal.

title	Texto	Tratamiento que se aplica al usuario extraído de la agenda del terminal
status_autodownload_disabled	Entero	Desconocido en la muestra analizada este campo está vacío
keep_timestamp	Entero	Desconocido en la muestra analizada este campo está vacío
is_spam_reported	Entero	Campo que refleja si el servidor de WhatsApp ha reportado al contacto como generador de spam toma los siguientes valores <ul style="list-style-type: none"> • 0 en caso negativo • 1 en caso afirmativo • Nulo en caso de grupos
is_sidelist_synced	Booleano	Desconocido, el valor asignado en la muestra analizada es 0
is_bussiness_synced	Booleano	Desconocido el valor asignado en la muestra analiza es 1 para contactos individuales y 0 para grupos

Ilustración 139 Contenido de la tabla wa_contacts

Tabla wa_group_add_black_list

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura. La tabla contiene un único campo que recoge la lista de identificadores de usuario de WhatsApp que han sido añadidos a una blacklist

Visible	Name	Details
<input checked="" type="checkbox"/>	jid	text not null

Ilustración 140 Esquema de la tabla wa_group_add_black_list

Tabla wa_group_admin_settings

Tabla que en las muestras analizadas se encuentra informada con una línea por cada grupo creado, aunque todos los valores de los campos (a parte del identificador del grupo: jid) se

muestran a 0 sin que se pueda determinar su contenido por lo que únicamente se muestra su estructura.

The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	jid	text not null
<input checked="" type="checkbox"/>	restrict_mode	boolean not null
<input checked="" type="checkbox"/>	announcement_group	boolean not null
<input checked="" type="checkbox"/>	no_frequently_forwarded	boolean not null
<input checked="" type="checkbox"/>	ephemeral_duration	integer

Ilustración 141 Esquema de la tabla wa_group_admin_settings

Tabla wa_group_descriptions

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	jid	text not null
<input checked="" type="checkbox"/>	description	text not null
<input checked="" type="checkbox"/>	description_id	integer
<input checked="" type="checkbox"/>	description_time	integer
<input checked="" type="checkbox"/>	description_setter_jid	text not null
<input checked="" type="checkbox"/>	description_id_string	text not null

Ilustración 142 Esquema de la tabla wa_group_descriptions

Tabla wa_last_entry_point

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

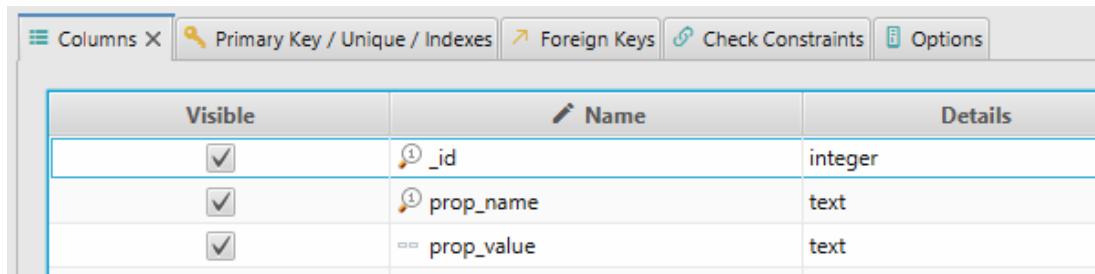
The screenshot shows a table structure with the following columns:

Visible	Name	Details
<input checked="" type="checkbox"/>	jid	text not null
<input checked="" type="checkbox"/>	entry_point_type	text not null
<input checked="" type="checkbox"/>	entry_point_id	text
<input checked="" type="checkbox"/>	entry_point_time	integer

Ilustración 143 Esquema de la tabla wa_last_entry_point

Tabla wa_props

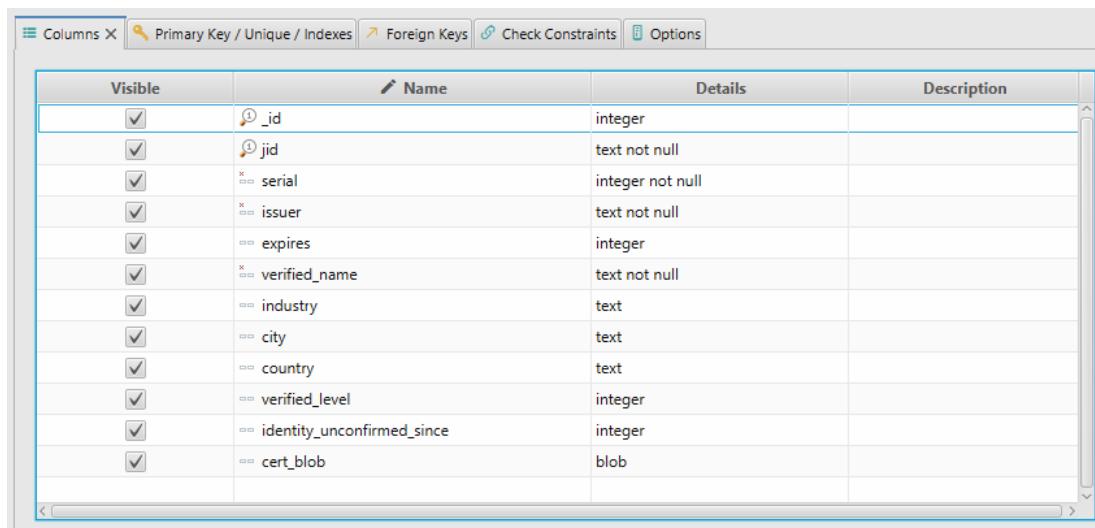
Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.



Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	prop_name	text
<input checked="" type="checkbox"/>	prop_value	text

Tabla wa_vnames

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.



Visible	Name	Details	Description
<input checked="" type="checkbox"/>	_id	integer	
<input checked="" type="checkbox"/>	jid	text not null	
<input checked="" type="checkbox"/>	serial	integer not null	
<input checked="" type="checkbox"/>	issuer	text not null	
<input checked="" type="checkbox"/>	expires	integer	
<input checked="" type="checkbox"/>	verified_name	text not null	
<input checked="" type="checkbox"/>	industry	text	
<input checked="" type="checkbox"/>	city	text	
<input checked="" type="checkbox"/>	country	text	
<input checked="" type="checkbox"/>	verified_level	integer	
<input checked="" type="checkbox"/>	identity_unconfirmed_since	integer	
<input checked="" type="checkbox"/>	cert_blob	blob	

Ilustración 144 Esquema de la tabla wa_vnames

Tabla wa_vnames_localized

Tabla que en las muestras analizadas se encuentra vacía por lo que únicamente se muestra su estructura.

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	jid	text not null
<input checked="" type="checkbox"/>	lg	text not null
<input checked="" type="checkbox"/>	lc	text not null
<input checked="" type="checkbox"/>	verified_name	text not null

Ilustración 145 Esquema de la tabla wa_vnames_localized

5.2.12 ESTRUCTURA DE LA BASE DE DATOS WEB_SESSIONS.DB

En la muestra analizada esta base de datos está compuesta por tablas que están vacías. Se muestra su estructura.

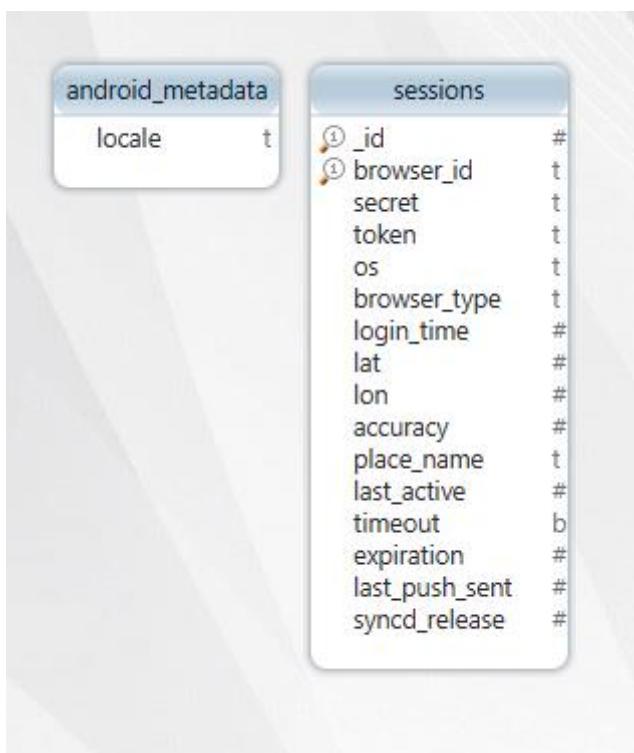


Ilustración 146 Esquema de la base de datos web_sessions.sqlite

Tabla android_metadata

La estructura de la tabla es la siguiente

Visible	Name	Details
<input checked="" type="checkbox"/>	locale	text

Ilustración 147 Esquema de la tabla android_metadata

Tabla sessions

La estructura de la tabla es la siguiente

Visible	Name	Details
<input checked="" type="checkbox"/>	_id	integer
<input checked="" type="checkbox"/>	browser_id	text
<input checked="" type="checkbox"/>	secret	text
<input checked="" type="checkbox"/>	token	text
<input checked="" type="checkbox"/>	os	text
<input checked="" type="checkbox"/>	browser_type	text
<input checked="" type="checkbox"/>	login_time	integer
<input checked="" type="checkbox"/>	lat	real
<input checked="" type="checkbox"/>	lon	real
<input checked="" type="checkbox"/>	accuracy	real
<input checked="" type="checkbox"/>	place_name	text
<input checked="" type="checkbox"/>	last_active	integer
<input checked="" type="checkbox"/>	timeout	boolean
<input checked="" type="checkbox"/>	expiration	integer
<input checked="" type="checkbox"/>	last_push_sent	integer
<input checked="" type="checkbox"/>	syncd_release	integer

Ilustración 148 Esquema de la tabla sessions

5.3 TIPOS DE COMUNICACIÓN Y SUS IDENTIFICADORES

Básicamente existen en WhatsApp cuatro tipos de comunicación distintas.

- Chats entre contactos individuales. Este tipo de comunicación se realiza entre dos contactos particulares, se trata de una comunicación 1 a 1
- Chats entre contactos grupales. Consiste en la definición de un grupo de usuarios que mantienen una conversación entre ellos, en la misma se pueden añadir o borrar usuarios en el momento que se estime oportuno. Se trata de una comunicación muchos a muchos, un usuario que envía o responde a un mensaje lo hace a todos los miembros del grupo.
- Listas de distribución. Se trata de un tipo especial de comunicación grupal, el funcionamiento es muy similar a los grupos, pero en este caso la entrega del mensaje

únicamente se realiza en caso de que el usuario destino tenga en su agenda de contactos al remitente, en otro caso el mensaje no será entregado. Se trata de una comunicación 1 a muchos. El remitente envía la comunicación a todos los miembros de la lista de distribución y la respuesta de los destinatarios (en caso de que haya una) llega sólo al remitente

- Llamadas (audio y vídeo).

No se profundiza ahora mismo en estos puntos ya que serán tratados en apartados posteriores.

En WhatsApp no se crean conversaciones en fechas y días que se almacenan en base a un calendario, sino que se establece un “chat” entre remitente y destinatario y en este “chat” se mantienen las conversaciones entre las distintas partes. De esta forma un chat se identifica con el identificador de remitente de la misma.

En ambas plataformas, como no debiera ser de otro modo, el origen y destino de la comunicación se establece a través de un elemento definido como “jid” que puede encontrarse como campo en múltiples tablas del modelo de datos de ambas plataformas.

Existen varios tipos distintos de jid:

Identificador de usuario individual: Se trata de un jid que identifica a un número de teléfono asociada a una SIM concreta (que está asociado a un usuario específico), está anunciada la funcionalidad de permitir una misma cuenta en distintos terminales, pero a la fecha de finalización y entrega de este trabajo no está operativa.

Este identificador se compone de una cadena de número que corresponden con el número de teléfono del titular de la cuenta seguido de la cadena @s.whatsapp.net, de esta forma un ejemplo de jid sería 3466666666@s.whatsapp.net.

Identificador de usuario grupal: Este identificador corresponde a un grupo (comunicación muchos a muchos). Respecto al identificador del grupo es algo diferente del identificador individual. El mismo se compone por el número de teléfono del creador del grupo, seguido de un guión y el timestamp en el que el grupo fue creado en formato UNIX Epoch time (también para grupos creados en plataformas Apple que utilizan el formato Apple Absolute Time para sus timestamps. Finalmente, se le añade la cadena @g.us. Un ejemplo sería el siguiente 3466666666-1598211062@g.us, esto nos aporta la información que el grupo fue creado por el usuario con teléfono 3466666666 el 23 de agosto de 2020 a las 19:31:02

Identificador de comunicación broadcast: Este identificador corresponde a un envío de comunicación tipo lista de distribución (uno a muchos). Cuando un usuario envía una comunicación a una lista de distribución le escribe al jid de esta lista. Posteriormente la

aplicación se encarga de remitir la comunicación a todos los miembros de la lista de distribución. En este caso el jid se forma con el timestamp (en formato UNIX Epoch time en ambas plataformas) del momento en el que se creó la conversación seguido del texto @broadcast. Por ejemplo 1598534166@broadcast

Se han encontrado algún mensaje con unos identificadores especiales, concretamente status@broadcast y 0@s.whatsapp.net, estos identificadores son utilizados internamente por la aplicación WhatsApp.

6 EXPERIMENTACIÓN Y RESULTADOS

Como resultado de la ejecución de los casos de prueba anteriormente mencionados se pueden describir los siguientes resultados

6.1 ANÁLISIS FORENSE DEL COMPORTAMIENTO DE LA APLICACIÓN

De cara a estudiar el comportamiento de la aplicación desde el punto de vista forense se plantean los siguientes casos de estudio.

6.1.1 CU.01 CONTACTOS EN WHATSAPP

Este caso de uso analiza el comportamiento de los contactos en WhatsApp, su origen, datos, etc.

6.1.2 CU.02 ENVÍO DE MENSAJES.

El presente caso de uso pretende analizar el comportamiento a nivel de datos del envío de los siguientes tipos de mensajes.

- Mensaje de texto
- Mensaje de Vídeo
- Mensaje de Audio
- Fotografía
- Fichero adjunto (documento)
- Contacto del teléfono

Para el caso analizado se busca verificar la forma en la que los datos son almacenados en el modelo de datos. Se analizará el proceso de entrega, verificando los cambios cuando el mensaje se entrega de forma diferida por no estar el teléfono disponible.

6.1.3 CU.03 LLAMADAS

Se realizarán pruebas de los siguientes tipos de llamadas.

- Llamadas de audio
- Video llamadas
- Llamadas grupales.

Para todos los casos se realizarán pruebas de llamada realizada, llamada recibida, llamada perdida y llamada rechazada. Se analizará el reflejo del proceso en el modelo de datos.

6.1.4 CU.04 GRUPOS

Se realizará la siguiente batería de pruebas dentro del caso de uso.

- 1.- Creación del grupo
- 2.- Agregación de usuarios
- 3.- Envío de mensajes al grupo

6.1.5 CU.05 BLOQUEO

Se analizará el resultado del bloqueo de usuarios a nivel individual. Adicionalmente se verificará el comportamiento del modelo de datos para con usuarios bloqueados tanto en lo que se refiere a la recepción de mensajes a nivel individual como a la recepción de mensajes enviados a un grupo al que pertenece.

Se realizará un desbloqueo del usuario y se analizará el comportamiento.

6.1.6 CU.06 BORRADO DE MENSAJES

Dentro de la ejecución de este caso de uso se realizará un borrado de un mensaje a nivel individual y en un grupo, dentro del grupo se procederá al borrado del mensaje únicamente para el usuario y de forma global para todos los miembros del grupo. Por su importancia se realizarán pruebas adicionales para verificar como se refleja en el modelo de datos el borrado de mensajes que han sido entregados en el teléfono móvil y el borrado de mensajes con anterioridad a su entrega en el teléfono móvil.

6.1.7 CU.07 WHATSAPP WEB

Análisis del envío de mensajes desde la aplicación WhatsApp para teléfonos móviles y desde la aplicación WhatsApp Web, tanto a nivel mensaje individual como mensaje de grupo.

6.1.8 CU.08 UBICACIÓN EN TIEMPO REAL

Análisis de la compartición por parte del usuario de la ubicación en tiempo real y su reflejo en el modelo de datos.

6.2 CONTACTOS EN WHATSAPP

Uno de los elementos más importantes en WhatsApp son los contactos que se encargan de establecer el origen y el destino de la comunicación. Cada contacto tiene asociado su jid de la forma que se mencionaba en apartados anteriores. Desde el punto de vista forense a través del análisis de estos identificadores se puede llegar a identificar al autor de un hecho investigado.

6.2.1 ALMACENAMIENTO DE INFORMACIÓN DE CONTACTOS

Hay bastantes diferencias en la manera que se almacenan los datos en las distintas plataformas analizadas IOS y Android. En ambos casos es importante indicar que la mayor parte de los datos de contacto se extraen de la agenda de contactos del dispositivo móvil, aunque la aplicación permite agregar nuevos usuarios, aunque no estén en la agenda.

Entorno IOS

En las pruebas realizadas en la plataforma IOS, se han utilizado, tal y como se ha mencionado en secciones anteriores terminales con dos versiones de sistema operativo distinto, versión 12 y versión 13. En la versión 12 se ha podido constatar que los datos de los contactos son recuperados de la agenda de direcciones del teléfono y guardadas en la base de datos “ContactsV2.sqlite”, concretamente en la tabla ZWADDRESSBOOKCONTACT. La lista de campos está descrita en el apartado 5.1.5, la mayor parte de los campos se rellenan directamente de la agenda del teléfono, como datos que se llenan por parte de la aplicación WhatsApp hay que destacar

ZPHONESTATUS y ZSPOTLIGHSTATUS, que toman valor “1” cuando se trata de una cuenta activa en la red social WhatsApp. Adicionalmente está rellenado el campo ZABOUTTIMESTAMP y ZABOUTTEXT que representan el texto que se muestra en la cuenta del contacto y la fecha en la que este texto fue cambiado. En la misma versión de la aplicación, pero instalada en un dispositivo con sistema operativo IOS 13.6.1 esta base de datos no contiene los datos de toda la información de la libreta de direcciones. Para ambos casos se puede localizar la información de los usuarios en dos tablas pertenecientes a la base de datos ChatStorage.sqlite. En ella podemos localizar dos tablas ZWPROFILEPUSHNAME y ZWPROFILEPICTUREITEM. En su contenido se puede localizar el jid (que nos proporcionaría

el número de teléfono asociado a la cuenta) y el nombre que figura en la cuenta de WhatsApp y por otro lado en la segunda tabla la foto asociada al perfil (que puede servir para identificar al titular de la cuenta) y que es guardada en la ruta /Media/profile. Un campo que puede resultar interesante es ZREQUESTDATE ya que nos indica en un timestamp cuando fue la última vez que la imagen del contacto se descargó en el terminal analizado. Se muestra una captura de ambas tablas (se oculta los datos del número de teléfono para proteger la privacidad de los contactos)

ZWAPROFILEPUSHNAME Table:

Z_PK	Z_ENT	Z_OPT	ZJID	ZPUSHNAME
4	4	13	2	34 [REDACTED]@s.whatsapp.net
5	5	13	3	34 [REDACTED]@s.whatsapp.net
6	6	13	1	34 [REDACTED]@s.whatsapp.net

ZWAPROFILEPICTUREITEM Table:

Z_PK	Z_ENT	Z_OPT	ZREQUESTDATE	ZJID	ZPATH	ZPICTUREID
1	710	12	619528286.283931	34 [REDACTED]@s.whatsapp.net	Media/Profile/34607887589-1597833428	1597833428
2	711	12	619654173.514061	34 [REDACTED]@s.whatsapp.net	Media/Profile/34669399888-1597961094	1597961094
3	712	12	619698583.585138	34 [REDACTED]@s.whatsapp.net	Media/Profile/34665543996-1595456590	1595456590

Ilustración 149 Contenido de las tablas ZWAPROFILEPUSHNAME Y ZWAPROFILEPICTUREITEM

Desde el punto de vista forense es fundamental asegurarse (normalmente a través de documentación externa) que los datos del teléfono asociado al jid corresponden a los datos del contacto que se refleja en ZPUSHNAME, en la foto indicada en ZPATH. Esto es así ya que excepto del jid, se trata de información editable. Es posible en una agenda de direcciones de un terminal móvil asociar un número de teléfono a un nombre de una persona que no es la verdadera titular de la línea. En caso de la no verificación de este hecho toda la pericia podría ser puesta en entredicho dado que no se tiene constancia real de que el chat que se está analizando pertenezca a una persona concreta.

Entorno Android

Respecto al entorno Android, la ubicación es totalmente distinta respecto a lo que se ha mostrado en el entorno Apple. Aquí la información se encuentra localizada en la base de datos wa.db, en la misma podemos acceder a los datos de los contactos a través de la tabla wa_contacts. El contenido de la misma se está descrito en el apartado 5.2.11. Al igual que en el entorno IOS la mayor parte de los datos se extraen de la agenda de direcciones del teléfono (aunque un usuario puede ser añadido manualmente en la propia aplicación). Como información que es generada directamente por WhatsApp, por supuesto el “jid”, el campo “is_whatsapp_user” que indica si el usuario de la lista de contactos tiene una cuenta activa

en WhatsApp, “status” y “status_timestamp” que corresponden a los campos ZABOUTTEXT y ZABOUTTIMESTAMP en IOS. Relacionado con el contacto existen dos timestamps que se encuentran en los campos “thumb_ts” y “photo_id_timestamp” que representan cuando el usuario estableció su foto de perfil y cuando esta foto de perfil fue descargada al terminal analizado. Adicionalmente el usuario puede definir su nombre en la aplicación que se guardaría en el campo “wa_name”.

En esta tabla existe un campo adicional que nos proporciona no información sobre la identidad del contacto sino sobre su actividad que es “unseen_msg_count”, este campo nos muestra el número de mensajes que hemos enviado al usuario y en nuestro terminal tenemos registrados que permanecen sin leer. Cruzando esta información con otra identificada en la base de datos ChatStorage.db podemos saber si los mensajes han sido entregados en el terminal de destino y el usuario no los ha leído o por otro lado si el terminal no se ha conectado a los servidores de WhatsApp desde el envío del mensaje.

Table: wa_contacts									
	_id	jid	is_whatsapp_user	status	status_timestamp	number	raw_contact_id	display_name	phone_type
1	6	34 [REDACTED]@s.whatsapp.net	1	Hey there! I a...	1598257599000	6 [REDACTED]	3	Android 1	2
2	7	34 [REDACTED]@s.whatsapp.net	1	NULL	0	6 [REDACTED]	11	IOS 1	2
3	9	34 [REDACTED]@s.whatsapp.net	1	iHola! Estoy u...	1595948825000	6 [REDACTED]	7	IOS 2	2
4	11	34 [REDACTED]@s.whatsapp.net	1	Hey there! I a...	1598200517000	6 [REDACTED]	10	Android 2	2

Ilustración 150 Contenido de la tabla wa_contacts

Las mismas consideraciones respecto a la autenticidad del usuario mencionadas anteriormente para el entorno IOS deben ser tenidas en cuenta para el entorno Android.

6.2.2 CREACIÓN Y BORRADO DE USUARIOS

No se registra en IOS ni en Android en el modelo de datos información sobre cuando un usuario fue añadido o eliminado. No obstante, es posible obtener información al respecto. Referente a los usuarios añadidos en Android la operación de creación de un usuario es registrada en el log de la aplicación (y probablemente en IOS, aunque con la metodología utilizada no ha sido posible recuperar el fichero de log de la copia de seguridad generada en iTunes). En dicho fichero se guarda entradas que nos aporta información sobre cuando un usuario fue añadido (en caso de que no estuviera en nuestra agenda con anterioridad) aunque esta investigación excede el alcance de este trabajo.

Respecto a borrado de usuarios, existen varios métodos para averiguar si un contacto ha sido borrado, en primer lugar, tanto para Android como para IOS la revisión de los campos ZPK y

_id de las tablas mencionadas en este apartado nos mostrará posibles discontinuidades (estos valores los genera secuencialmente de forma automática SQLite y una discontinuidad indica un borrado de un registro). Adicionalmente comparando la información de creación de usuarios recogida en los logs (en el caso de Android), con el contenido wa_contacts nos proporcionaría el jid del usuario que ha sido eliminado. Por último, existen mecanismos para recuperar registros borrados de la base de datos, tal y como veremos más adelante en este documento, que nos permitirían intentar recuperar la información borrada.

6.3 ENVÍO DE MENSAJES.

En primera instancia, tras el análisis de las evidencias obtenidas en la realización del presente trabajo en primer lugar es relevante analizar la forma en la que funciona WhatsApp. Este funcionamiento, desde el punto de vista del almacenamiento de los datos, está mucho más claramente definido en el modelo de base de datos de Android, omitiéndose parte de los datos en el modelo de iOS.

Cuando un usuario envía un mensaje de WhatsApp se sigue la siguiente secuencia

- 1.- En primer lugar, se almacena el mensaje en la base de datos.
- 2.- Si el terminal está conectado a la red se procede a enviar el mensaje a los servidores de WhatsApp.
- 3.- Los servidores de WhatsApp reciben el mensaje y envían una confirmación de recepción del mensaje.
- 4.- Los servidores de WhatsApp intentan enviar el mensaje al terminal de la cuenta del destinatario
- 5.- En caso de que el terminal destinatario esté online se almacena el mensaje en su base de datos.
- 6.- El servidor de WhatsApp envía información sobre cuándo el mensaje ha sido entregado en el terminal destino.

En este momento el mensaje está entregado en destino. Aquí en base al tipo de mensaje enviado o recibido se completarán unas tablas u otras. Adicionalmente con posterioridad los registros de los mensajes pueden ser actualizados cuando se produzcan distintas acciones como la descarga de un objeto adjunto a un mensaje o la lectura del propio mensaje.

La forma en la que los datos son almacenados en los distintos entornos es totalmente distinta. Por ello se explicará de forma independiente.

6.3.1 ENVÍO Y RECEPCIÓN DE MENSAJES EN DISPOSITIVOS ANDROID

En este caso los mensajes se almacenan en la base de datos msgstore.db en la tabla messages.

Se procede a comentar los pasos indicados anteriormente.

1.- En primer lugar, se almacena el mensaje en la base de datos.

Para ello en primer lugar WhatsApp define un identificador de mensaje que es almacenado en el campo “key_id”, este identificador es único y es una cadena de caracteres que define internamente la aplicación. A continuación, en nuestro caso, como somos los remitentes del mensaje el campo “key_from_me” toma valor 1 dado que somos el identificador de WhatsApp del remitente del mensaje, también se rellena el destinatario de la comunicación que se guarda en “remote_resource” que corresponde a su jid. A continuación, se define el campo “status” como 0 (que significa que el mensaje no ha sido entregado en el servidor, también se rellena el campo “timestamp”. Adicionalmente se llenan los campos relativos al contenido del mensaje. Este punto depende del tipo de mensaje.

- A. Mensajes de tipo texto. Entre estos mensajes se encuentran los mensajes de texto estándar. Para estos mensajes se establece el campo “media_wa_type” a 0 y en el campo “data” se inserta el texto del mensaje a enviar.
- B. Mensaje tipo imagen: Para estos mensajes se rellena el campo “media_wa_type” a 1, se establece el tipo mime en “media_mime_type”, el tamaño en “media_size”, el hash del fichero en base 64 “media_hash”, el nombre original del fichero se almacena en el campo “media_name”, la imagen thumbnail en “thumb_image”.
- C. Mensaje tipo audio: Para estos mensajes se rellena el campo “media_wa_type” a 2, el resto de los campos son similares excepto que adicionalmente se rellena la duración en el campo “media_duration”
- D. Mensaje tipo vídeo: Igual que los anteriores pero el campo “media_wa_type” toma valor 3 o 13 dependiendo del media_type. En el campo “longitude” y “latitude” se guarda el tamaño en pixels del ancho y alto del vídeo.
- E. Mensaje tipo vcard: En este caso “media_wa_type” toma valor 4 y el texto de la vcard se guarda en el campo “data”, en “media_name” se introduce el nombre del contacto
- F. Envío de ubicación: El campo “media_wa_type” toma valor 5, y los datos de la ubicación se guardan en el campo “latitude” y “longitude”

- G. Envío de un enlace: El campo “media_wa_type” toma valor 7, en “data” se guarda el texto del enlace y la url, así como el texto que se adjunta al mensaje.
- H. Envío de un fichero: En el campo de “media_wa_type” se guarda el valor 9,
- I. Envío de un fichero animado: En el campo de “media_wa_type” se guarda el valor 11, por ejemplo, para el envío de un Gif animado. El resto de los campos son igual que un vídeo.
- J. Envío de un sticker: En el campo “media_wa_type” se guarda el valor 15, el resto de los campos son igual que una imagen
- K. Envío de ubicación en tiempo real: En este caso el campo “media_wa_type” toma valor 16.

2.- Si el terminal está conectado a la red se procede a enviar el mensaje a los servidores de WhatsApp.

Para ello para mensajes que incluyan ficheros de media o urls, se procede a subir el fichero al servidor de WhatsApp. Éste procede a cifrar la url que se enviará al destino que además es almacenada en el campo “media_url” (por ejemplo <https://mmg-fna.whatsapp.net/d/f/Ah-Mdndyut0tW6N8xxuXmwmBZZNv4o4-aTq9H01O5bK6.enc>) la extensión .enc indica que es una url cifrada. En caso de que el fichero no se pudiera subir al servidor el campo “status” cambiaría a 3 en otro caso permanece igual hasta que el siguiente paso.

3.- Los servidores de WhatsApp reciben el mensaje y envían una confirmación de recepción del mensaje.

En este punto se rellena el campo “receipt_server_timestamp” con la fecha y hora de recepción del acuse de recibo del servidor y el “status” cambia a 4 que indica que el mensaje ha sido recibido en el servidor.

4.- Los servidores de WhatsApp intentan enviar el mensaje al terminal de la cuenta del destinatario.

5.- En caso de que el terminal destinatario esté online se almacena el mensaje en su base de datos. Los campos de la base de datos se llenan de la misma forma que en el remitente con las siguientes consideraciones.

- A. “key_id”, contiene exactamente el mismo valor que la base de datos del remitente.
- B. “key_from_me” toma valor 0 dado que somos el identificador de WhatsApp del destinatario del mensaje,
- C. “remote_resource” pasa a contener el jid del remitente
- D. “status” toma el valor 4 ya que ha sido entregado

- E. El campo “media_name” que contiene en el remitente el nombre del fichero enviado en el sistema de ficheros del remitente queda vacío.
- F. El campo “timestamp” contiene el mismo valor que el de la base de datos del remitente.
- G. El campo “received_timestamp” se rellena con la fecha/hora de recepción. Se rellena el campo “timestamp”. Adicionalmente se llenan los campos relativos al contenido del mensaje. Este punto depende del tipo de mensaje.
- H. Los campos “receipt_server_timestamp” y “receipt_device_timestamp” se llenan con valor -1 y “read_device_timestamp” queda vacío.

6.- El servidor de WhatsApp envía información sobre cuándo el mensaje ha sido entregado en el terminal destino. En este momento se guarda en el remitente en el campo “receipt_device_timestamp” y “status” cambia a valor 5

7.- En el momento que el mensaje es leído en el terminal de destino en el remitente y destinatario se actualiza el campo “read_device_timestamp”

Por último, hay que indicar que cuando un mensaje es reenviado se almacena los datos del mensaje en la tabla message_forwarded.

6.3.2 ENVÍO Y RECEPCIÓN DE MENSAJES EN DISPOSITIVOS IOS

En este caso los mensajes se almacenan en la base de datos ChatStorage.sqlite. La respuesta funcional, respecto al procedimiento para la comunicación es el mismo, pero cambian los valores que se guardan y cambia las tablas y los campos en los que se guarda. Esta vez se utilizan varias tablas para el almacenamiento por un lado la tabla ZWAMESSAGE guarda la información de los mensajes. En la tabla ZWAMEDIAITEM se guarda la información de los ficheros enviados. En la tabla ZWACHATSESSION se guarda información sobre los chats a los que pertenecen los mensajes. En la tabla ZWMESSAGEDATAITEM, contiene información sobre los mensajes enviado que contienen enlaces a contenidos en internet. En la tabla ZWAMEDIAITEM contiene información sobre los ficheros enviados y recibidos.

Se procede a comentar los pasos indicados anteriormente.

1.- En primer lugar, se almacena el mensaje en la base de datos.

Para ello en primer lugar WhatsApp define un identificador único de mensaje que es almacenado en el campo “ZSTANZAID” de la tabla ZWAMESSAGE (al igual que el resto de los campos en este párrafo), al igual que en Android este identificador es único y es una cadena de caracteres que define internamente la aplicación. A continuación, en nuestro caso, como

somos los remitentes del mensaje el campo "ZISFROMME" toma valor 1 dado que somos el identificador de WhatsApp del remitente del mensaje, también se rellena el destinatario de la comunicación que se guarda en "ZTOJID" que corresponde a su jid. A continuación, se define el campo "ZMESSAGESTATUS" de la tabla ZWAMESSAGE como 0 (que significa que el mensaje no ha sido entregado en el servidor), también se rellena el campo "ZMESSAGEDATE". Adicionalmente se rellena el campo "ZCHATSESSION" que nos proporciona la clave que identifica el chat al que pertenece el mensaje en la tabla ZWACHATSESSION. Adicionalmente se llenan los campos relativos al contenido del mensaje. Este punto depende del tipo de mensaje.

- A. Mensajes de tipo texto. Entre estos mensajes se encuentran los mensajes de texto estándar. Para estos mensajes se establece el campo "ZMESSAGETYPE" de la tabla ZWAMESSAGE a 0 y en el campo "ZTEXT" de la misma tabla se inserta el texto del mensaje a enviar.
- B. Mensaje tipo imagen: Para estos mensajes se rellena el campo "ZMESSAGETYPE" de la tabla ZWAMESSAGE a 1, se guarda la sección en el terminal en la que se va a guardar la imagen en el campo "ZMEDIASECTIONID", incluye en "ZMEDIAITEM" el número de fila en la tabla ZWAMEDIAITEM que contiene la información del elemento, en esta tabla guarda adicionalmente se guarda la información establece el tamaño de la imagen en "ZLONGITUDE" y "ZLATITUDE", el tipo mime en "ZVCARDSTRING", el tamaño en "ZFILESIZE", el hash del fichero en base 64 "ZVCARDNAME", el nombre original del fichero se almacena en el campo "ZMEDIALOCALPATH", la imagen thumbnail en "ZMPPTHUMBPATH", además en IOS se almacenan metadatos del fichero en el campo "ZMETADATA"
- C. Mensaje tipo audio: Para estos mensajes se rellena el campo "ZMESSAGETYPE" de la tabla ZWAMESSAGE a 2, el resto de los campos son similares excepto que adicionalmente se rellena la duración en el campo "ZMOVIEDURATION"
- D. Mensaje tipo vídeo: Igual que los anteriores pero el campo "ZMESSAGETYPE" de la tabla ZWAMESSAGE toma valor 3 o 13 dependiendo del tipo mime. En el campo "ZLONGITUDE" y "ZLATITUDE" en la tabla ZWAMEDIAITEM se guarda el tamaño en pixels del ancho y alto del vídeo.
- E. Mensaje tipo vcard: En este caso "ZMESSAGETYPE" de la tabla ZWAMESSAGE toma valor 4 y el texto de la vcard se guarda en la tabla ZWAMEDIAITEM en el campo "ZVCARDNAME" guarda el nombre del contacto y en "ZVCARDSTRING" se guarda el contenido de la VCARD.

- F. Envío de ubicación: El campo “ZMESSAGETYPE” de la tabla ZWAMESSAGE toma valor 5, y los datos de la ubicación se guardan en el campo “ZLATITUDE” y “ZLONGITUDE” en la tabla ZWAMEDIAITEM
- G. Envío de un enlace: El campo “ZMESSAGETYPE” de la tabla ZWAMESSAGE toma valor 7, en la tabla ZWAMEDIAITEM en el campo “ZMEDIAURL” se guarda la url del mensaje, mientras que en el campo “ZTITLE” el título de la página. Además, la localización en el sistema local de la imagen thumbnail se guarda en “ZXMPPTHUMBPATH”.
- H. Envío de un fichero: En el campo de “ZMESSAGETYPE” de la tabla ZWAMESSAGE se guarda el valor 8,
- I. Envío de un fichero animado: En el campo de “ZMESSAGETYPE” de la tabla ZWAMESSAGE se guarda el valor 11, por ejemplo, para el envío de un Gif animado. El resto de los campos son igual que un vídeo.
- J. Envío de un sticker: En el campo “ZMESSAGETYPE” de la tabla ZWAMESSAGE se guarda el valor 15, el resto de los campos son igual que una imagen
- K. Envío de ubicación en tiempo real: En este caso el campo “ZMESSAGETYPE” de la tabla ZWAMESSAGE toma valor 16.

2.- Si el terminal está conectado a la red se procede a enviar el mensaje a los servidores de WhatsApp.

Para ello para mensajes que incluyan ficheros de media o urls, se procede a subir el fichero al servidor de WhatsApp. Éste procede a cifrar la url que se enviará al destino que además es almacenada en el campo “ZMEDIAURL” (por ejemplo <https://mmg-fna.whatsapp.net/d/f/Ah-Mdndyut0tW6N8xxuXmwmBZZNv4o4-aTq9H01O5bK6.enc>) la extensión .enc indica que es una url cifrada. En caso de que el fichero no se pudiera subir al servidor el campo “ZMESSAGESTATUS” de la tabla ZWAMESSAGE cambiaría a 3 en otro caso permanece igual hasta que el siguiente paso y se rellena el campo “ZSENTDATE”.

3.- Los servidores de WhatsApp reciben el mensaje y envían una confirmación de recepción del mensaje.

En este punto en la tabla ZWAMESSAGE se guarda se rellena el campo “ZMESSAGEINFO” que nos indica el registro de esta tabla asociado a este registro que contiene información sobre la entrega en el campo “ZRECEIPTINFO” que contiene un fichero plist con los datos del

destinatario y el timestamp del del acuse de recibo del servidor y el “ZMESSAGESTATUS” de la tabla ZWAMESSAGE cambia a 4 que indica que el mensaje se ha recibido en el servidor.

4.- Los servidores de WhatsApp intentan enviar el mensaje al terminal de la cuenta del destinatario.

5.- En caso de que el terminal destinatario esté online se almacena el mensaje en su base de datos. Los campos de la base de datos se rellenan de la misma forma que en el remitente con las siguientes consideraciones.

- I. “ZSTANZAID”, contiene exactamente el mismo valor que la base de datos del remitente.
- J. “ZISFROMME” toma valor 0 dado que somos el identificador de WhatsApp del destinatario del mensaje,
- K. “ZFROMJID” pasa a contener el jid del remitente
- L. “ZMESSAGESTATUS” de la tabla ZWAMESSAGE toma el valor 4 ya que ha sido entregado
- M. El campo ““ZMEDIALOCALPATH” de la tabla ZMEDIAITEM que contiene en el remitente el nombre del fichero enviado en el sistema de ficheros del remitente queda vacío.
- N. El campo “ZSENDDATE” contiene el mismo valor que el de la base de datos del remitente.
- O. No se guarda información en la tabla ZWAMESSAGEINFO. Adicionalmente se rellenan los campos relativos al contenido del mensaje. Este punto depende del tipo de mensaje en ZWAMEDIAITEM.

6.- El servidor de WhatsApp envía información sobre cuándo el mensaje ha sido entregado en el terminal destino. En este momento se guarda en el remitente en el campo “ZRECEIPTINFO” de la tabla ZMESSAGEINFO y “ZMESSAGESTATUS” de la tabla ZWAMESSAGE cambia a valor 5

6.3.3 LLAMADAS EN WHATSAPP

Tras una revisión de las bases de datos no se ha identificado dentro del modelo de datos de iOS información sobre las llamadas realizadas en WhatsApp. No obstante, dentro del teléfono existen ficheros de log que aportan información sobre las llamadas recibidas y realizadas por el terminal, pero no se profundizará en el tema por exceder el alcance del presente trabajo. Cuando hablamos de terminales IOS, las llamadas pueden ser analizadas en /private/var/mobile/Applications/net.whatsapp.WhatsApp/Documents/ el fichero calls.log así como versiones antiguas comprimidas del mismo fichero. Se trata de un fichero

PLIST. Respecto a Android, en la base de datos MsgStore.db existe la tabla call_log que guarda información sobre el otro participante de la llamada en jid_row_id que indica la fila de la tabla jid que contiene los datos del otro interlocutor de la llamada, la fecha y hora de la llamada en el campo “timestamp”, si se trata de una llamada de vídeo (valor 1) o de audio (valor 0) en el campo “video_call”, la duración en “duration” y el resultado de la llamada en “call_result” con valores 5 llamada finalizada, 4 llamada rechazada o perdida siendo remitente de la llamada, 3 error en la llamada y 2 llamada sin respuesta siendo destinatario de la llamada. Adicionalmente, en caso de que se trate de una llamada múltiple en la tabla call_log_participant_v2 guarda los datos de todos los participantes “jid_row_id” asociados a una llamada concreta “jid_row_id” y el resultado de la llamada para cada participante “call_result”.

Se puede diferenciar cuando una llamada fue rechazada de cuando fue no contestada porque cuando no se puede contactar con el destinatario en la base de datos de éste se introduce un registro en la tabla messages con “status” con valor 6 y “wa_media_type” igual a 10 que representa una llamada perdida.

No obstante, tanto en IOS como en Android existe el fichero de log de operaciones denominado whatsapp.log, en el cual podemos encontrar información como la siguiente

```
17248 2020-08-23 23:00:06.745 LL_I W [786:VoIP Signaling Thread] wa_call_signal Received kMessageTypeInfo with 4 participants,  
17249 transaction id 13, rekey 0, media type video relay_transaction_id -1  
17250 2020-08-23 23:00:06.745 LL_I W [786:VoIP Signaling Thread] wa_group_call. call_update_participants 34 [REDACTED]@s.whatsapp.net,  
17251 state[connected->connected] is_invited_by_self 0, call state Calling, device [REDACTED]  
17252 2020-08-23 23:00:06.746 LL_I W [786:VoIP Signaling Thread] wa_group_call. call_update_participants 34 [REDACTED]@s.whatsapp.net,  
17253 state[outgoing->outgoing] is_invited_by_self 1, call state Calling, device [REDACTED]  
17254 2020-08-23 23:00:06.746 LL_I W [786:VoIP Signaling Thread] wa_group_call. call_update_participants 34 [REDACTED]@s.whatsapp.net,  
17255 state[outgoing->receipt] is_invited_by_self 1, call state Calling, device [REDACTED]
```

Ilustración 151 Información de llamadas en whatsapp.log en android

En la misma se puede observar que en la primera línea indica que la llamada tiene cuatro participantes, se indica que la llamada es una llamada de vídeo, marcado con el recuadro a la derecha se muestra los tres jid de los destinatarios de las llamadas.

A la izquierda se muestra el estado para el primer recuadro es “connected” o sea que el jid se ha unido a la video llamada, el segundo es “outgoing” que significa que el destinatario tiene el terminal no operativo (en este caso se le había quitado la conexión de red), y el tercero es “receipt” que recibe la llamada, pero no la coge o la rechaza.

Adicionalmente en el log se muestra todo tipo de información técnica sobre la llamada que nos puede aportar información adicional.

6.4 GRUPOS

Un grupo es un modo de comunicación muchos a muchos en la que un remitente escribe un mensaje que es recibido por todos los miembros del grupo y la respuesta a un mensaje de un usuario concreto también va dirigido a todos los miembros del grupo. El envío y recepción de mensajes sigue el mismo procedimiento definido en el apartado 6.2, pero con alguna particularidad.

6.4.1 ENVÍO DE MENSAJES EN GRUPOS

En primer lugar, hay que hablar del jid del registro del mensaje. Cuando se envía un mensaje a un grupo el jid del mensaje no es el del remitente del mensaje sino el del grupo, el jid de un grupo se construye con el número de teléfono del creador del grupo seguido de “-” el timestamp de creación del grupo seguido de la cadena “@g.us”, por ejemplo 34666666666-1598211062@g.us.

En dispositivos Android en un mensaje enviado el jid se guarda en “key_remote_id” de la tabla messages de la base de datos msgstore.db. Adicionalmente en el campo “remote_resource” se guarda el remitente del grupo que ha enviado el mensaje.

Operativamente la aplicación registra un mensaje que identifica el mensaje del grupo (que tiene “remote_resource” con valor nulo y adicionalmente un mensaje a cada uno de los miembros del grupo).

En la tabla group_participants se puede observar que se guardan $n+1$ registros para cada grupo, siendo n el número de participantes. Se guarda un registro que identifica al grupo (incluye el campo gid o identificador del grupo, pero no jid identificador del miembro del grupo), y para el resto de los registros ambos campos están llenos. El administrador del grupo se identifica porque cuenta un valor 2 en el campo “admin” siendo este usuario el que se encarga de la gestión de las claves para la comunicación segura en el grupo. Una información similar se encuentra en android en la tabla group_participant_user y por último indicar que si queremos conocer el nombre asociado al grupo es necesario consultar la tabla wa_contacts de la base de datos wa.db como si se tratara de cualquier otro usuario.

Para terminales IOS el funcionamiento es similar el jid del grupo se guarda en el campo “ZTOJID” de la tabla ZWAMESSAGE en los mensajes enviados, el número del chat se encuentra en el campo “ZCHATSESSION”. En la tabla ZWACHATSESSION se identifica al grupo al que pertenece en el campo “ZGROUPINFO”, la información del grupo se localiza en el

registro cuyo campo “ZCHATSESSION” coincide con el definido en el mensaje y el campo “ZPK” coincide con el campo “ZGROUPINFO”.

En la tabla ZWAGROUPMEMBERS se puede observar al igual que en Android que se guardan un registro para cada miembro del grupo. Se guarda un registro que identifica al grupo (incluye el campo “ZCHATSESSION” que identifica el grupo en la tabla ZWACHATSESSION), y el resto de los datos que identifican al miembro del grupo. El administrador del grupo se identifica porque cuenta un valor 1 en el campo “ZISADMIN” siendo este usuario el que se encarga de la gestión de las claves para la comunicación segura en el grupo.

6.4.2 CREACIÓN DE UN GRUPO

La creación de un grupo es un proceso a través del cual el usuario define en su aplicación el nombre del grupo y asigna los miembros del grupo. Desde el punto de vista del modelo de datos en Android el usuario envía un mensaje a cada uno de los miembros del grupo en el cual el campo “status” de la tabla messages toma valor 6, y en el campo “media_size” toma valor 1, el nombre del grupo se almacena en el campo “data” y la fecha de creación del grupo en el campo “timestamp”. Envía un mensaje de este tipo a cada uno de los nuevos miembros del grupo.

Remotamente el destinatario recibe el mensaje y el servidor le envía la información de los miembros del grupo.

Para terminales IOS el funcionamiento es similar, en este caso en los datos se almacenan con el mismo valor en la tabla ZWAMESSAGE en el campo “ZMESSAGESTATUS” que toma valor 6, se identifica el registro de la tabla ZWMEDIAITEM en el campo “ZMEDIAITEM”, y en dicha tabla en el campo ZMOVEDURATION toma valor 1.

6.4.3 AÑADIR Y ELIMINAR USUARIOS A UN GRUPO

Para añadir usuarios a un grupo de WhatsApp sólo lo puede realizar el administrador del mismo. En dispositivos Android desde el punto de vista del modelo de datos, se envía un mensaje similar al mensaje que se indicaba en el apartado anterior para la creación de un grupo, pero esta vez el campo “status” toma valor 6 y “media_size” toma valor 4.

La operación de eliminación de un usuario la puede realizar el administrador o cualquier miembro del grupo (respecto a sí mismo). En el modelo de datos los registros son iguales al de añadir a un miembro, pero el campo “media_size” toma valor 5

Para terminales IOS el funcionamiento es similar, en este caso en los datos se almacenan con el mismo valor en la tabla ZWAMESSAGE en el campo “ZMESSAGESTATUS” que toma valor 6, se identifica el registro de la tabla ZWAMEDIAITEM en el campo “ZMEDIAITEM”, y en dicha tabla en el campo ZMOVIEDURATION toma valor 4 para añadir usuarios y 5 para eliminarlos.

6.5 LISTAS DE DISTRIBUCIÓN

Este tipo de comunicación tiene un comportamiento distinto de las otras analizadas, se trata de una comunicación 1 a muchos tal y como se describe en el apartado 6.1.

El envío de mensajes de una lista de distribución desde el punto de vista del modelo de datos supone la gestión de varios mensajes. De hecho, anteriormente indicábamos que el jid de una comunicación de este tipo se componía por el timestamp de la creación de la lista seguida de la cadena @broadcast, en la siguiente imagen se observa la captura de la lista en un registro de la tabla “chat_list” de la base de datos MsgStore.db en Android ,

Table: chat_list							New Record	Delete R	
_id	key_remote_jid	message_table_id	subject	creation	last_read_message_table_id	d_receipt_sent_message_	Filter	Filter	Filter
1	broa	68	NULL	1598651941655	71	61			

Ilustración 152 Captura de registro de la tabla chatlist con mensaje de una lista de distribución

mientras que en IOS se almacena en la tabla ZWACHATSESSION

Table: ZWACHATSESSION								New Record	Delete	
ERTIES	ZMESSAGEDATE	IONSHARINGEN	ONTACTIDENTIF	ZCONTACTJID	ZETAG	ZMESSAGETE	ZPARTNERNAME	Filter	Filter	Filter
1	620482853.34...	NULL	NULL	1598643020@broadcast	NULL	NULL	Lista distribución IOS 2			

Ilustración 153 Captura de registro de la tabla ZWACHATSESSION con mensaje de una lista de distribución

Para crear una lista de distribución y asignar miembros, WhatsApp comprueba que los destinatarios de los mensajes tengan al remitente en su libreta de direcciones, de otra forma no permite la entrega del correo. En base de datos el proceso de envío de mensaje implica varios registros, en primer lugar se guarda un mensaje de control con tipo de mensaje con valor 6 que es el que envía el mensaje en sí. De hecho en caso de que no exista la lista de distribución la crea (el jid destinatario es el de la lista de distribución). En el campo ZFILTEREDRECIPIENTCOUNT guarda la cantidad de mensajes de la lista de distribución han sido realmente entregados. Adicionalmente se crea un registro adicional para cada uno de los registros entregados con vistas a guardar la información de recepción del mismo. Estos registros aunque tienen con valor 1 el campo ZISFROMME y su correspondiente en Android, no tienen rellenado el campo “ZSENDDATE”, sí tienen rellenado el valor “ZMESSAGEDATE”, como identificador de mensaje tienen **todos el mismo identificador de mensaje** y en

“ZPARENTMESSAGE” guarda el número de registro del mensaje que envió el mensaje. cada uno guarda el status.

El envío de mensajes es similar a los grupos, por parte del remitente se envía un mensaje que como jid de origen tiene el valor de la lista de distribución (xxxxxx@broadcast) a cada miembro de la lista de distribución, estos registros guardan en Android en el campo “key_remote_jid” de la tabla messages el jid del destinatario y en IOS en el campo “ZTOJID” de la tabla ZWAMESSAGE. Adicionalmente en el campo “need_push” se guarda el valor 2 (sólo para este tipo de mensajes) y por último el campo “recipient_count” indica el número de destinatarios del mensaje en Android y en “ZTEXT” en IOS.

De cara al destinatario la comunicación es transparente, recibe un mensaje estándar que no refleja que se trate de un mensaje de una lista de distribución, se trata de un mensaje con el jid del remitente en vez del jid de la lista de distribución.

6.6 BLOQUEOS DE USUARIOS

Aquí tenemos que diferenciar dos visiones diferentes por un lado la situación desde el punto del usuario que ha sido bloqueado y por otro lado la situación del usuario que realiza el bloqueo.

Respecto al usuario bloqueado, el bloqueo es transparente para él, no se ha encontrado reflejo en el modelo de datos. Sólo hay un hecho que indica al usuario que ha sido bloqueado por otro usuario y es que desde la aplicación no tiene acceso a la información del contacto. No verá ni su status ni su foto de perfil que será borrada de su sistema de ficheros.

Respecto al usuario que bloquea, en el entorno Android se guarda la lista de usuarios bloqueados en la tabla “wa_blocklist” en la tabla wa.db. Por otro lado, en IOS se guarda un fichero en el directorio /private/var/mobile/Applications/net.whatsapp.WhatsApp/Documents/ denominado blockedcontacts.dat, se trata de un archivo .plist.

Podemos inferir que la lista de usuarios está actualizada en el servidor revisando los logs de sistema vemos que el programa periódicamente realiza una petición para conseguir que le envíe la lista de usuarios bloqueados.

```
07/10 1:37:0 11:1 W [1092:main] unacknowledgedmessages/getunacknowledgedmessages: v
37311 1:378 LL I W [1092:WhatsApp Worker #126] getblocklistprotocolhelper/sendGetBlocklistRequest
```

Ilustración 154 Solicitud en el log de la lista de bloqueados

6.7 BORRADO DE DATOS

Existen tres ámbitos de investigación en cuanto al borrado de datos en WhatsApp. Por un lado, se pueden analizar el propio fichero de base de datos, en segundo lugar, es posible analizar los ficheros temporales asociados a la base de datos (en caso de que existan) y en tercer lugar el análisis de los propios datos contenidos en el modelo de datos.

Una base de datos SQLite cuenta con una estructura de fichero que está definida en la propia documentación de la herramienta (SQLite, Fecha no reseñada). En la misma se puede observar que el fichero se almacena en páginas. En las páginas la información se almacena desde el final hacia el principio. Cada vez que se almacena un registro se guarda el offset en el que él se ha almacenado dentro de la página en el denominado “Cell Pointer Array”. Cada vez que se borra un registro la información no se destruye sino se elimina el offset del “Cell Pointer Array” de la página, pero la información (al menos inicialmente) sigue estando ahí.

La cabecera de la base de datos aporta información diversa sobre la base de datos como por ejemplo el tamaño de las páginas. Directamente ejecutando la sentencia `select * from sqlite_master` obtenemos información sobre la página en la que se encuentra una tabla concreta.

De esta forma podemos indicar que en una base de datos existen tres zonas en las cuales se encuentra información que puede ser recuperada. Por un lado, está el espacio no utilizado de la página (teóricamente no debería contener datos, pero lo cierto es que una página puede haber sido borrada y reutilizada por lo que el espacio no usado puede contar con información), la segunda zona son los freeblocks que corresponden a los registros utilizados que han sido borrados en la base de datos y el último elemento es lo que se conoce como freelists que son páginas enteras que han sido eliminadas. A partir de la información obtenida de la ubicación de las tablas en las páginas, los cell pointer array, el tamaño de las páginas y otra información disponible se puede explorar los ficheros para recuperar información borrada. Actualmente existen herramientas que realizan esta tarea por nosotros como <https://github.com/ST2Labs/DFIR/tree/master/SQLite> publicada por [ST2labs](#) o <https://github.com/mdegrazia/SQLite-Deleted-Records-Parser> publicada por [Maria de Gracia](#). A partir de ahí es labor del investigador analizar la información para averiguar si realmente es relevante.

Los archivos temporales de Sqlite se localizan en el mismo directorio que las bases de datos, la estructura y detalle de los mismos se puede encontrar en la documentación de los ficheros temporales de la herramienta (SQLite, Fecha no reseñada)), los archivos -WAL o -JOURNAL pueden guardar información de registros borrados.

Por último, estaría el análisis de los datos para obtener información. En primer lugar, hay un hecho que nos puede indicar que algunos registros han sido borrados y es el análisis de los campos `Z_PK` en tablas IOS y `_id` en tablas Android. Estos registros se rellenan automáticamente al insertar registros en las tablas de forma secuencial, de forma que la ausencia de registros indica que alguno de ellos ha sido borrado.

En el caso de los contactos podría ser posible obtener información a partir de la información de los grupos. Si el usuario borrado pertenecía a algún grupo es posible analizar los mensajes que se enviaron a ese grupo revisando los destinatarios del mismo. En el momento que el número de destinatarios cambie podremos averiguar cuál es el contacto borrado y un intervalo temporal en el cual el contacto fue borrado.

Adicionalmente hay otras tablas que nos pueden aportar información sobre borrado o incluso manipulación de mensajes, cuando se envía o se recibe un mensaje WhatsApp guarda el contenido del mismo para usarlo para obtener palabras clave que usar en campañas publicitarias, se muestra una captura de la tabla `message_ftsv2_content`. Tal y como se comentaba anteriormente es el acrónimo full text search ¹y es la funcionalidad que permite el análisis del texto de los mensajes para por ejemplo mostrar anuncios publicitarios en los banners.

Table: `message_ftsv2_content`

	docid	c0content	c1fts_jid	:2fts_namespace
	Filter	Filter	Filter	Filter
1	18	envio mensaje de texto	1 f	
2	21	android 1	1 f	
3	24	envio de mensaje previo a borrado solo para mi	1 f	
4	26	envio de mensaje previo a borrado para todos	1 f	
5	30	respuesta a mensaje	f e	

Ilustración 155 Contenido de la tabla `message_ftsv2_content`

El valor de `docid` coincide con el valor del índice del registro de mensaje en la tabla `messages`, por lo que es posible encontrar mensajes que se han borrado o incluso modificado revisando estas tablas y otras similares. De hecho, el valor de la última columna nos proporciona

¹ https://en.wikipedia.org/wiki/Full-text_search full text search en wikipedia

información sobre el tipo de contenido que tenía el mensaje, así si el campo está en blanco contiene mensajes de texto, “fv” para mensaje de vídeo, “fa” para mensajes de audio, “fi” para ubicación y “fd” para documentos

6.8 ENVÍO DESDE DISTINTOS TERMINALES

WhatsApp tiene anunciado la funcionalidad de instalación de una misma cuenta en distintos terminales, pero en la fecha de entrega de este trabajo todavía no estaba operativa. Actualmente se permite el envío de mensajes desde el propio terminal y desde la aplicación de escritorio WhatsApp Web. La forma de identificar los mensajes de WhatsApp web es a través del identificador del mismo. Se ha podido observar que el identificador de mensaje en el caso de mensajes enviados desde WhatsApp Web comienza con el código “3EB0”. Se muestra una captura de un entorno IOS donde el campo “ZSTANZAID” de la tabla “ZWAMESSAGE” muestra esta información. En un entorno Android esta información se puede observar en el campo “key_id” de la tabla messages.

ZSTANZAID	ZTEXT	ZTOJID
3eb	Filter	Filter
3EB06A4B35C9F025E791	Mensaje Whatsappweb 1	34660351283@s.whatsapp.net
3EB0D28E3041EDCB7141	Mensaje Whatsappweb 2	34660351283@s.whatsapp.net
3EB0250B6DE8A8A93B83	Mensaje Whatsapp web 3	34660351283@s.whatsapp.net
3ADB3EB8A3E2CE08ECA3	Envío mensaje texto	34660351283@s.whatsapp.net
3A9843EBB3C2E72618B5	NULL	34660351283@s.whatsapp.net

Ilustración 156 Contenido de la tabla ZWAMESSAGE con mensajes enviados vía whatsappweb

6.9 UBICACIÓN EN TIEMPO REAL

WhatsApp ha incorporado una funcionalidad adicional que es la compartición de la ubicación entre usuarios en tiempo real. En este caso se trata de una información más compleja de incluir en un análisis pericial por tratarse al menos parcialmente de una información volátil. El usuario decide durante cuánto tiempo comparte la ubicación y pasado este tiempo la información es parcialmente borrada de la base de datos.

Cuando un usuario decide compartir su ubicación en tiempo real, se envía un mensaje que se guarda en la tabla ZWAMESSAGE en IOS o en messages en Android con tipo (campos “ZMESSAGETYPE” y “wa_media_type”) con valor 16. Pasado el tiempo en el cual el remitente ha permitido compartir su ubicación, el registro permanece en base de datos como tipo 5 (ubicación en vez de ubicación en tiempo real). Los datos sobre la ubicación se guardan en base de datos igual que en un mensaje de ubicación estándar por ejemplo en android se guarda en latitude y longitude.

Existen otras tablas que guardan información respecto a la localización en tiempo real que se encuentran en la base de datos location.db en Android son las tablas “location_sharer” que muestra información sobre el usuario con el que se comparte o está compartiendo la ubicación (campos “remote_jid” y campo “from_me”), el identificador del mensaje (campo “message_id” y fecha de expiración de la compartición (timestamp en el campo “expires”), adicionalmente la tabla “location_cache” en Android que no sólo guarda la información sobre la ubicación sino otros datos como la precisión, velocidad, y otros parámetros que permiten hacer un seguimiento de la posición del usuario. Esta es una tabla volátil, pasado el tiempo en el que se comparte la ubicación los datos son borrados. No se ha localizado una tabla similar en iOS.

7 CONCLUSIONES

En el desarrollo de este trabajo se ha realizado una revisión completa y detallada del modelo de datos de WhatsApp de cara a su análisis forense, incluyendo en el análisis otros artefactos que aportaban información relevante para una investigación. Se han analizado los modelos de datos en ambas plataformas Android e IOS, pudiendo constatar que el modelo de datos en terminales Apple es más estructurado y normalizado, pero al mismo tiempo ofrece algo menos de información de cara al análisis forense que Android. La existencia de información duplicada en esta plataforma en algunas tablas, aporta información adicional que puede ser útil en una investigación. Probablemente estas diferencias estén motivadas por la necesidad de dar soporte a distintos terminales y sistemas operativos (hecho que se ha podido observar en también IOS, pero con menor impacto probablemente por el menor número de modelos de terminales disponibles) así como por restricciones del propio sistema operativo. Adicionalmente hay que indicar que el análisis de las bases de datos ha permitido detectar la presencia de tablas que identifican funcionalidades que están siendo desarrolladas y/o que todavía no han sido puestas a disposición de los usuarios, como puede ser el pago a través de la aplicación.

Además de lo anterior, se ha podido constatar que un análisis forense puede aportar una visión completa de las comunicaciones realizadas con la aplicación, proporcionando información no solo sobre los mensajes enviados y recibidos, sino sobre los contactos que los recibieron, su lectura, descarga y almacenamiento, reenvío, etc. Todo ello pudiendo establecer una cronología y una línea de tiempo de los hechos investigados.

No obstante, la información aportada en ambos modelos es similar, así como el funcionamiento de las comunicaciones en todos los tipos analizados, tanto en lo que se refiere al tipo de comunicación, como al tipo de contenido compartido en ambas plataformas. Aunque algunas funcionalidades en entornos iOS recaen en el sistema operativo (como la gestión de ubicaciones) por lo que la información que se guarda en base de datos es menor.

El trabajo muestra la forma en la que los datos que se almacenan en la base de datos y otros ficheros mencionados en el mismo pueden interpretados para obtener conclusiones que nos aporten las evidencias que se necesitan en una investigación. Listas de distribución, grupos, contactos y mensajes son relacionados mostrando la forma en la que todos estos elementos

interactúan y aportando una visión por un lado detallada y por otro global y conjunta de las comunicaciones investigadas (incluyendo incluso el borrado y destrucción de información). Se ha podido observado que los modelos de datos analizados ya cuentan con tablas que parecen destinadas a contener futuras funcionalidades anunciadas por WhatsApp, pero todavía no abiertas al público lo que abre un abanico de posibilidades de investigación de cara al futuro.

8 TRABAJOS FUTUROS

WhatsApp es una herramienta en constante evolución, cada mes surge una nueva versión que implica cambios a nivel funcional y/o modelo de datos. Esto supone por parte del profesional forense una constante revisión del trabajo realizado para verificar, por un lado, que no se han producido cambios sobre las conclusiones de los trabajos previos y por otro lado la necesidad de investigar las nuevas funcionalidades publicadas.

A fecha de entrega del presente trabajo distintos medios han anunciado para 2020 la publicación de una funcionalidad que puede tener una enorme importancia para el análisis forense. Se trata de la programación de borrado de mensajes.

Desde el punto de vista funcional se infieren dos posibles alternativas, por un lado, que el mensaje en pantalla se muestre con el texto “mensaje borrado” del mismo modo que se muestran los mensajes actuales y, por otro lado, la opción es que desaparezca totalmente de la conversación. Desde el punto de vista del análisis forense es importante averiguar como a nivel de modelo de datos se comporta esta funcionalidad, ¿quedá rastro del mensaje? ¿Se podría recuperar información sobre cuándo se programó el borrado o cuando estaba prevista o se ha ejecutado el borrado? Esto puede suponer intencionalidad para cometer una acción y puede ser importante en el desarrollo de investigaciones por lo que se trata de un trabajo pendiente que debiera ser realizado cuando la funcionalidad estuviera disponible.

Del mismo modo en la realización del trabajo se han encontrado tablas que parecen destinadas a almacenar datos de pagos a través de la plataforma, funcionalidad que actualmente se está probando en India, pero no está disponible en otros países y que es importante analizar.

Por último, otra funcionalidad inicialmente prevista para este año es la posibilidad de usar la misma cuenta en distintos dispositivos. Sin duda esto supondrá una necesidad de revisión del modelo de datos, así como de la información que contiene para verificar la información recogida en este trabajo e incluir los cambios e incorporaciones que sean pertinentes.

9 BIBLIOGRAFÍA

- (12, 02 2020). Retrieved from Dos mil millones de usuarios - Conectando al mundo de manera privada: <https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately>,
- Anglano, C. (2015). *Forensic Analysis of WhatsApp Messenger on Android Smartphones*. . Alessandria (Italy): Universit_a del Piemonte Orientale.
- Calvo, D. (2019, 06 11). *Qué son ADB y Fastboot, cómo instalarlos y sus comandos más importantes*. Retrieved from <https://www.nextpit.es/que-es-adb-comandos-mas-importantes#adbfastboot>
- Celebrite. (Fecha no reseñada). UFED Ultimate. Retrieved from <https://www.cellebrite.com/es/ufed-ultimate-2/>
- ClickaTell. (Fecha no reseñada). *What are WhatsApp Template Messages? (a)*. Obtenido de . Retrieved from <https://www.clickatell.com/faqs/answer/whatsapp-template-messages/>
- Elcomsoft. (Fecha no reseñada). *Elcomsoft Explorer for WhatsApp*. Retrieved from <https://www.elcomsoft.es/exwa.html>
- Elcomsoft. (Fecha no reseñada). *Elcomsoft Mobile Forensics Bundle*. Retrieved from <https://www.elcomsoft.es/emfb.html>
- Europol. (2019, 10 09). *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019*. Retrieved from Europol: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf
- Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*. (2011, 03). Retrieved from <https://tools.ietf.org/html/rfc6121>
- Fernández, Samuel. (2020, 04 29). *WhatsApp funcionará pronto en varios dispositivos a la vez con la misma cuenta*. Retrieved from <https://www.xatakamovil.com/aplicaciones/whatsapp-funcionara-pronto-varios-dispositivos-a-vez-cuenta>
- Guidance Software. (Fecha no reseñada). *Encase Forensics*. Retrieved from <https://www.guidancesoftware.com/encase-forensic>
- Internet Engineering Task Force (IETF) . (2012, 03). *Extensible Messaging and Presence Protocol (XMPP): Core*. Retrieved from <https://tools.ietf.org/html/rfc6120>

- Internet Engineering Task Force (IETF) . (2015, 09). *Extensible Messaging and Presence Protocol (XMPP): Address Format* (Marzo 2011) Obtenido de <https://tools.ietf.org/html/rfc6121>. Retrieved from <https://tools.ietf.org/html/rfc7622>
- Internet Engineering Task Force (IETF) . (2017, 01 10). *FunXMPP Protocol*. Retrieved from <https://github.com/mgp25/Chat-API/wiki/FunXMPP-Protocol>
- Magnet forensics. (Fecha no reseñada). *Magnet Axiom*. Retrieved from <https://www.magnetforensics.com/products/magnet-axiom/>
- Mehta, I. (2020, 07 26). *WhatsApp might soon work with the same phone number across multiple phones.* Retrieved from <https://thenextweb.com/apps/2020/07/27/whatsapp-might-soon-work-with-the-same-phone-number-across-multiple-phones/>
- Mikhailov, I. (2019, 11 07). *WhatsApp in Plain Sight: Where and How You Can Collect Forensic Artifacts.* Retrieved from https://www.group-ib.com/blog/whatsapp_forensic_artifacts
- MobilEdit. (Fecha no reseñada). *MobilEdit Forensics Express*. Retrieved from <https://www.mobiledit.com/forensic-express>
- Oxygen Forensics. (Fecha no reseñada). *Oxygen Forensics Detective*. Retrieved from <https://www.oxygen-forensic.com/es/products/oxygen-forensic-detective>
- Pratama, A. R. (2013). *WHATSAPP FORENSICS: EKSPLORASI SISTEM BERKAS DAN BASIS DATA PADA APLIKASI ANDROID DAN IOS*. . Indonesia: Fakultas Teknologi Industri, Universitas Islam.
- SQLite. (Fecha no reseñada). *Database File Format*. Retrieved from https://www.sqlite.org/fileformat.html#varint_format
- SQLite. (Fecha no reseñada)). *Temporary Files Used By SQLite*. Retrieved from <https://sqlite.org/tempfiles.html>
- WhatsApp. (2018, 01 18). *Te presentamos la aplicación WhatsApp Business (WhatsApp para Negocios)* . Retrieved from <https://blog.whatsapp.com/introducing-the-whats-app-business-app>
- WhatsApp. (2019, 04 04). *WhatsApp Business ahora disponible para iPhone*. Retrieved from <https://blog.whatsapp.com/bringing-the-whats-app-business-app-to-i-phone>
- Wikipedia. (2020, 09 20). *Full Text Search*. Retrieved from https://en.wikipedia.org/wiki/Full-text_search

XMPP. (Fecha no reseñada). Retrieved from Instant Messaging:

<https://xmpp.org/uses/instant-messaging.html>