A Deep-dive Analysis on WhatsApp Artifacts and their Relevance in Crime Investigation

Nagendar Rao Koppolu

Inspector of Police (In-charge State Cyber Vertical), Telangana Police Department, Hyderabad

---***---

Abstract: *Today, most crime scenes involve Information and Communications Technology (ICT) devices such as mobile phones and tablets. Among them, popular Instant messaging applications such as WhatsApp are used widely for communication purposes. Criminals are taking advantage of its end-to-end encryption feature. Criminals are using the encrypted communication medium to commit a crime. It has become a challenge for Law enforcement agencies (LEA's) to gather the potential evidence from such devices for evidence purposes. Extracting device information is the prime concern of an investigating officer (IO) using forensically sound methods. This paper discusses WhatsApp data obtained from Android and iOS platforms such as account information, contacts and communication link between users and Deleted information.*

Keywords: *Digital Forensics, Mobile Forensics, WhatsApp, Mobile Acquisition, Mobile Extraction*

1. INTRODUCTION

According to a study conducted by Statista, as of January 2021, WhatsApp is the most popular messenger application with 2 billion active users worldwide [7] and India has 390.1 million monthly WhatsApp active users [5]. The majority of individuals, businesses are using WhatsApp for day-to-day communications. Whereas, Criminals and fraudsters are using the WhatsApp application to commit a crime. Therefore, WhatsApp data has become crucial for the investigation. The average WhatsApp user on Android spends 38 minutes per day on the app [9] and more than 100 billion messages are sent each day on WhatsApp in December 2020 [6][10]. Based on Global Web Index data, the WhatsApp worldwide user base consists of 45.5% female users and the remaining 54.5% are males. WhatsApp has a client application and a business application, accessed from mobile devices and desktop computers. One must be connected to the internet to use this application.

WhatsApp messenger provides services like - 1. Sending text messages 2. Audio and video call 3. Multimedia sharing like audio, video, image, and documents 4. Location sharing and 5. Money transfer. WhatsApp communication can be between two users or a group of users or a business to a user. All WhatsApp communications are end-to-end encrypted, which means all communication is encrypted and no one can see what data is exchanged using WhatsApp. A WhatsApp group can contain 256 users as group members [4]. This application is available for both Android and IOS devices and downloaded from both Appstore and Play store.

2. The Technology Used In The WhatsApp Application

The technology used in WhatsApp is Extensible Messaging and Presence Protocol (XMPP) to exchange data. XMPP is the Extensible Messaging and Presence Protocol, a set of open technologies for instant messaging, presence (user's online/ offline status), multi-party chat, voice and video calls, collaboration (users working together from various locations), lightweight middleware, content syndication, and generalized routing of XML data. XMPP specifications were published as RFC 3920 and RFC 3921 in the year 2004. In addition, Internet Engineering Task Force (IETF) has formalized the core XML streaming protocol as an instant messaging and presence technology.

3. WhatsApp Security Architecture

WhatsApp uses end-to-end encryption to secure messages between the sender and recipient devices until they change their device or re-install the application on their device. As mentioned in their technical specifications, WhatsApp uses three different keys for encryption - Public key, Session key and Private key [2].

3.1. Public Keys:

The public key is used to identify individuals. Public keys are generated during installation and are stored in servers for distribution. Different types of Public keys generated are:

i. Identity Key Pair – They are generated during the installation of WhatsApp.

ii. Signed Pre-Key – They are generated during installation time and signed by the Identity Key Pair.

iii. One-Time Pre-Keys – A set of keys are generated for one-time use and a new batch is generated as they are used up.

3.2. Session Keys:

To enable communication among users, the WhatsApp client needs to establish an encrypted session. Session keys are used to create the encrypted session between the user's devices. Different Session keys generated are as below.

i. Root Key – It is used to generate the Chain Key. Root key (root certificate) provides authentication from a legitimate source (certified issuer).

ii. Chain Key – It is used to generate the Message Key.

iii. Message Key – It is used for the encryption of messages.

3.3. Private Key:

If a new session is established between sender and recipient, the sender uses the recipient's public key to encrypt the messages. The recipient uses their private key to decrypt them. Private keys are unique to individuals and are stored in mobile devices. According to WhatsApp policy, servers do not have a user's private key and cannot read any messages that are being exchanged on the platform.

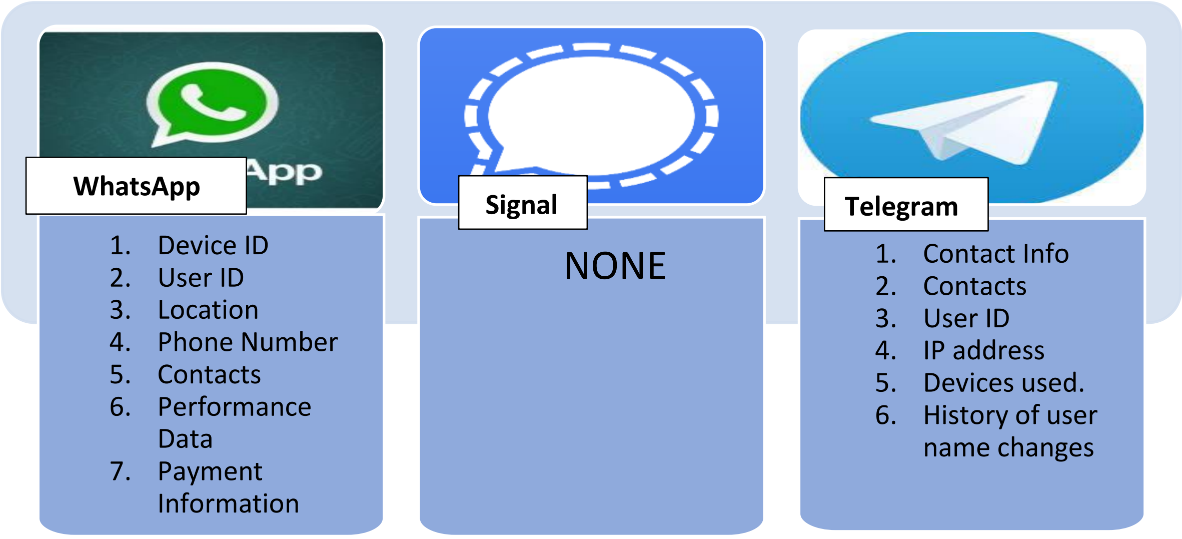


Fig-1: Type of data collected by different messengers.

WhatsApp uses Curve 25519 encryption standard and SHA256 hashing algorithm to generate these public and private keys. Messages and notifications are stored temporarily on the server if the recipient did not answer the call or the recipient is not connected to the internet. Once the recipient device is online, messages and calls are delivered, and the stored information is deleted from the WhatsApp server.

Similar instant messaging applications are Telegram, Signal, spike, wire, etc., and all these services require a mobile number to use.

4. Reasons For WhatsApp Becoming A Very Popular Application

WhatsApp was the first to come up with free internet-based messaging among the private messaging applications. Pre-WhatsApp messaging was carrier-based and chargeable. However, as WhatsApp is adding new functionality and is providing encrypted messaging and calling, users who look for privacy have started using WhatsApp as an effective means of communication.

4.1 Timeline of WhatsApp:

Year	Date and Month	Developments
2009	24 February	Incorporation of WhatsApp
2013	16 July	WhatsApp goes free
2013	August	Voice messaging introduced
2014	19 February	Facebook, Inc. acquired WhatsApp
2014	November	Read Receipts feature introduced, which alerts senders when recipients read their messages.
2015	21 January	Launched WhatsApp Web used to sync with mobile devices.
2015	March	Added voice calls between two accounts
2016	2 March	Introduces document-sharing feature
2016	5 April	End-to-end encryption is enabled
2016	November	Feature of video calls between two accounts introduced
2017	July	Peer-to-peer money transfer feature using UPI
2018	July	Introduced group voice and video call up to four users or accounts.
2020	April	Enhanced group calls up to 8 users or accounts.
2020	November	Disappearing message feature introduced. If it is enabled, the chats will disappear after seven days.
2020	December	WhatsApp Pay is a payment feature that allows users to make transactions to their contact list only using UPI payments

Table-1: Timeline of WhatsApp [8]

5. WhatsApp Features

WhatsApp application is not just a platform to send and receive simple text messages like a short message service (SMS). WhatsApp being an internet-based communication platform provides us far more additional features like:

WhatsApp Feature	Description of Feature
Text messaging	Text messaging to a user or a group of users can contain up to 256 users.
Broadcast messaging to a group	Broadcast a message to a selected list of contacts. These contacts need not be explicitly added to a group. It is a one-way communication, and the recipient can only reply to the sender of the message.
Audio and video calls	Audio and video call up to 8 users.
Sharing images	Sharing images either from the mobile device storage or directly clicking them using the mobile device camera to a user or a group of users.

Sharing video files	Sharing a video either from the mobile device storage or directly clicking them using the mobile device camera to a user or a group of users.
Sharing audio files	Sharing an audio clip from the mobile device storage or directly recording using the mobile device microphone to a user or a group of users.
Sharing documents	Sharing a document like text, doc, ppt, pdf, xls from the mobile device storage to a user or a group of users.
Sharing contact numbers	Sharing a contact saved in the mobile device to a user or a group of users.
Location sharing	Sharing the person's location using GPS coordinates captured through an onboard GPS receiver on the mobile device to a user or a group of users. Location sharing can be used to share the location of a particular spot or the live location of a user for a duration of 15minutes or 1 hour or 8 hours.
UPI Payments	Payment can be made to send money to a user's bank account directly using their UPI ID.
Status messages to everyone	Sharing a status message or image or video clip visible for everyone in the contacts list.
Status messages to a selected contact	Sharing a status message or image or video clip visible only to a selected contact.
Starred message	Mark important messages with a start for easy access later.
Local backup	Automatic backup of WhatsApp chats and shared media files locally on the mobile. It happens at 2 AM every day as it is the default setting given in the application and cannot be changed.
Cloud backup	Based on the mobile device operating system, automatic backup of WhatsApp chats and shared media files take place at google drive or iCloud. In addition, the user can set a backup frequency.

Table-2: WhatsApp application features [3]

6. WhatsApp Privacy & Security Features To End-User

WhatsApp provides several privacy & security features to the end-users. These features mentioned below help a WhatsApp user to protect their data from being visible to unauthorized users and protect their data from being captured and read by any third party.

6.1. End-to-end encryption for text.

- All the chat messages between two users or between a user group or a business account to a user are encrypted. Encryption is done on the source device using the public key of the recipient device. It is transmitted through the internet to Facebook servers, delivering the encrypted message to the recipient device. The message will be decrypted using the recipient device's private key. This process is called end-to-end encryption. End-to-end encryption ensures that no one, including Facebook's servers, can see the message while being transmitted.

6.2. End-to-end encryption for calls.

- End-to-end encryption is applied for the audio and video calls made using the WhatsApp application to users or groups.

6.3. Enable or hide "last seen" status to everyone or only those in the user's contacts or nobody.

- WhatsApp has a facility where we can see the "last seen" online time of contact. It can be set to be visible for everyone using WhatsApp or only for those who are in our WhatsApp contacts.

6.4. Set a profile picture for the user account visible to everyone or only those in the user's contacts or nobody.

- WhatsApp user profile can contain a picture visible to everyone or only those in the user's contacts or hide it from everyone. Any image added to as a profile image will be compressed by WhatsApp and removes all the metadata from the image.

6.5. Show the "about profile" to everyone or only those in the user's contacts or nobody.

- A message can be set in the "about" section of the WhatsApp profile. This message can be made visible for everyone using WhatsApp or only for those who are in our WhatsApp contacts.

6.6. Show the "status-message or media" to everyone or only those in the user's contacts or nobody.

- A text message or an image or a video clip can be set as user status in WhatsApp. This status message can be visible for everyone using WhatsApp or only for our WhatsApp contacts or a particular contact.

6.7. Enable or disable message "read receipts".

- Every text message, document, image, video, audio, contact, location shared to a contact or a group shows the status of that message.
- If the message is sent from the user's device but is not yet delivered to the recipient, it shows a single tick mark for the message.
- If the message is sent from the user's device and is delivered to the recipient, it shows a double tick mark for the message.
- If the recipient reads the message, it shows a blue coloured double tick mark for the message.
- Read receipts help us understand the status of the message.
- Read receipts can be disabled so that the message only appears to be delivered but does not show if the message has been read or not.

6.8. Ability to add a user into WhatsApp group by everyone or only those in the contacts of user or those in the contacts of user except few selected contacts.

- WhatsApp users can set if anyone can add them into their WhatsApp group or only their contacts can add them into a group. If someone cannot be added to a group, there is an option to send an invite link to join the group.

6.9. Block certain contacts from sending text messages or calling the user.

6.10. Enabling a biometric authentication (like a fingerprint) to access the application itself.

6.11. Two-step verification to check the user when WhatsApp is being re-installed on a different device.

7. WhatsApp Data Acquisition Methods

As WhatsApp is a mobile platform application, we must discuss few key points related to data extraction from mobile devices. Today we see either Android or iOS being used in the majority of smartphones. Data extraction methods vary widely based on the mobile platform and the mobile device make and model. An investigator must understand all the aspects like the Operating System version, Security patch level, any further customizations that the OEM might have made, like creating dual apps or dual space or second space, etc., as every manufacturer tends to have their terminology.

Data extraction from mobile devices can be classified broadly as physical data extraction and logical data extraction.

7.1. Physical data extraction:

Physical data extraction is the process of obtaining a bit-by-bit copy of the mobile device storage. Physical data acquisition gives us access to deleted data on the mobile device. Mobile forensic applications use various undisclosed/proprietary methods, which vary widely based on the make, model, operating system version, security patch level, system on chip (SoC) to gain physical access to mobile storage. With ever-increasing security consciousness among the end-users, mobile manufacturers are also implementing various hardware and software-controlled security checks and data encryption at the storage and application levels. This security consciousness is making it difficult and, in some cases, impossible to gain physical access to the data stored in the mobile device.

7.2. Logical data extraction:

Logical data extraction is obtaining data by accessing the file system on the mobile device storage. Logical data extraction does not give a bit-by-bit copy of the mobile device storage. It only gives us access to data on the mobile device's storage and is visible to us. The investigator needs the mobile device to be unlocked to obtain the logical data dump. If the mobile device is locked, logical data acquisition will not be possible. Further, Logical data acquisition does not guarantee access to deleted data.

WhatsApp data acquisition, analysis and report generation process is as shown in Fig.2.

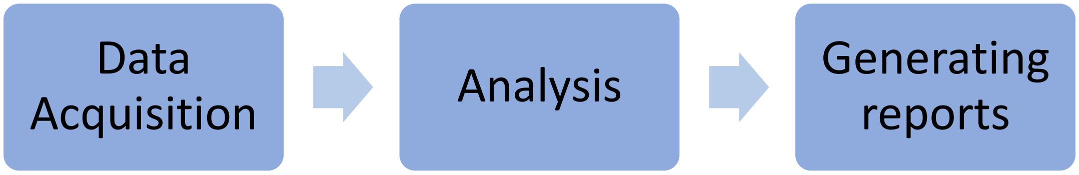


Fig-2: steps in the investigation

8. WhatsApp Artifacts To Be Considered For Investigation

An artifact can be data like a message, image, audio, video, location coordinate, contact, URL link, and invitation link that help us build evidence in a forensic investigation. WhatsApp application data can provide valuable artifacts to an investigator in finding the evidence. An investigator must be prudent while handling the data, not to tamper it while acquiring or analyzing.

8.1. Timestamp: An investigator can look for, timestamp of a message, multimedia file, location coordinate or contact that is shared. It explains the date and time when the data in question is exchanged, when the recipient received the data on their mobile device, and read it. It can be helpful as a piece of evidence in the investigation of crime.

8.2. Starred Messages: An investigator can look for any starred messages. Generally, important messages are marked with a 'star.' From this, an investigator can understand what messages are essential to the WhatsApp user, which helps in understanding the user's interests and priorities based on the contents of the starred messages and helps identify the key contacts that the user is in touch.

8.3. Status of the Messages: An investigator can check the status of the messages sent by WhatsApp user based on the message status marks like,

i. if a message is sent, it is marked with one tick mark; if the message is delivered to the recipient mobile device, it is marked with two tick marks

ii. if the message is read by the recipient, the two tick marks turn to blue colour. Investigator can also check if a message received by the user is a direct message from the sender or a forward message.

iii. If the message is forwarded from another contact, it is marked as "forwarded".

iv. A message can be forwarded at a time to 5 contacts. If a message is forwarded multiple times, such message will be marked as "forwarded many times".

8.4. **Forwarded Messages:** In many cases, these forwarded messages are the main reason for violence, defamation of an institution or a person. Investigator can check for the group where the user is a member and the type of discussion going on; multimedia files shared among the group members, other participants of the group, and the group administrator details. In some cases, a user cannot be added directly to a WhatsApp group. The user has set restrictions on who can add them to a group; in that condition, the WhatsApp group administrator can send an invite link asking the user to join. Investigator can also check if there are any such invite links that the user has received. It helps in understanding who has sent the invite link, what that group is and its description. If the user has joined the group through the received invite link, an investigator can also check for the messages, multimedia messages shared, and other group members' details.

8.5. **Location Sharing:** An investigator can also look at the user's places by checking shared or received location coordinates. This location sharing can be a static coordinate or a live location sharing for a particular duration. The WhatsApp user shares his location to another user or group for guidance to reach him,

8.6. **Contacts:** An investigator can look for the contacts that are shared by the user or contacts shared with the user by someone. It helps the investigator find if these new contacts are connected to the crime.

8.7. **Multimedia:** An investigator can also look for any multimedia content like image, video, audio, or documents shared by the user or shared with the user or shared in a group that the user is participating.

8.8. **Call Logs:** An investigator can look at the user call logs of audio or video like call duration, date, and time of the call made or received by the user from another WhatsApp user or a WhatsApp group.

8.9. **Profile Picture or Display Picture:** An investigator can understand a user's likes and, to some extent, their state of mind by looking at the profile picture of the user account or the group that the user is an administrator.

8.10. **Status of Messages:** An investigator can also look at the status message that the user has set to understand the information the user is sharing publicly with everyone. This also helps an investigator to understand the user's state of mind to some extent.

8.11. **Paired devices:** An investigator can check if the WhatsApp account is used from any other device like a PC or a Mac. It helps an investigator decide if the synced device can be seized for further investigation.

8.12. **WhatsApp Payments:** An investigator can also check if the user has made or received any WhatsApp payments. WhatsApp can be used to pay or receive money from any WhatsApp contacts through UPI payment interface. It helps an investigator understand any monetary transactions between the user and someone else related to the crime.

9. WhatsApp Files - An Investigator's Lookout

All the WhatsApp artifacts can be retrieved and analyzed using various mobile forensic tools to analyze the data found automatically. But, in some cases, an investigator can also look for data stored on the WhatsApp database files. An investigator can copy the database files from the mobile device to their PC and manually analyze the data. The challenge is that all the data on these databases is encrypted.

The following table lists all the database files related to WhatsApp in Android mobile devices and their location on the device:

Description	Path
WhatsApp file history, recent device transfer history	/data/com.WhatsApp/databases/main.db
WhatsApp calls log, call log participant, chat list, chat group participants, message settings, message lables, deleted messages	/data/com.WhatsApp/databases/msgstore.db

lables, chat messages, chat group invite links.	
WhatsApp profiles, block list, contacts, group descriptions	/data/com.WhatsApp/databases/wa.db
WhatsApp web and PC sessions	/data/com.WhatsApp/databases/web_sessions.db
WhatsApp Payments	/data/com.WhatsApp/databases/payments.db
Shared media files	/data/com.WhatsApp/databases/media.db

Table-3: Location of WhatsApp database files in Android device

The following table lists the location of WhatsApp media storage on an Android mobile device:

Media Type	Received content location	Sent content location
Images	/internal storage/WhatsApp/Media/ WhatsApp Images	/internal storage/WhatsApp/Media/ WhatsApp Images/sent
Videos	/internal storage/WhatsApp/Media/ WhatsApp Video	/internal storage/WhatsApp/Media/ WhatsApp Video/sent
Animated Gifs	/internal storage/WhatsApp/Media/ WhatsApp Animated Gifs	/internal storage/WhatsApp/Media/ WhatsApp Animated Gifs/sent
Documents	/internal storage/WhatsApp/Media/ Documents	/internal storage/WhatsApp/Media/ Documents/sent
Voice notes	/internal storage/WhatsApp/Media /Voice notes	/internal storage/WhatsApp/Media/ Voice notes/sent
Stickers	/internal storage/WhatsApp/Media/ Stickers	/internal storage/WhatsApp/Media/ Stickers/sent
Profile photos	/internal storage/WhatsApp/Media/ profile photos	NA

Table-4: Location of WhatsApp media files in Android device

In the older versions of Android, few manufacturers have given an option to store WhatsApp application data on external storage like a memory card. The following table lists the location of WhatsApp files stored in external storage:

Media Type	Description	Path
.Shared	Files that have been sent to other user	/mnt/sdcard/WhatsApp/.Share/
.trash	Contains deleted files	/mnt/sdcard/WhatsApp/.trash/
Backups	Previous backups	/mnt/sdcard/WhatsApp/.Backups/
Databases	Contains encrypted backup copies	/mnt/sdcard/WhatsApp/Databases/
Media	Contains media files	/mnt/sdcard/WhatsApp/Media/

Table-5: Location of WhatsApp files on external storage in Android device

Similarly, WhatsApp database files are also found on Apple iOS devices. Apple iOS's filesystem is different from that of the Android filesystem and the way data is stored also defers in iOS devices. The table below lists all the database files related to WhatsApp in iOS devices and their location.

Description	Path
WhatsApp version	/var/mobile/Applications/group.net.WhatsApp.WhatsApp.private/consumer_version
Status messages	/var/mobile/Applications/net.WhatsApp.WhatsApp/Documents/StatusMessages.plist
Blocked contacts	/var/mobile/Applications/net.WhatsApp.WhatsApp/Documents/blockedcontacts.dat
Contacts	/var/mobile/Applications/group.net.WhatsApp.WhatsApp.shared/ContactsV2.sqlite
Call logs	/var/mobile/Applications/group.net.WhatsApp.WhatsApp.shared/CallHistory.sqlite

Chat	/var/mobile/Applications/group.net.WhatsApp.WhatsApp.shared/ChatStorage.sqlite
Payments	/var/mobile/Applications/group.net.WhatsApp.WhatsApp.shared/Payments/payments.sqlite
Media	/var/mobile/Applications/group.net.WhatsApp.WhatsApp.shared/Message/Media/{mobile_number@s.WhatsApp.net/x}

Table-6: Location of WhatsApp database files in iOS device

10. Forensic Extraction Of WhatsApp Artifacts

The first rule of digital forensics is to avoid tampering with data and change of last access dates. Specific measures are to be taken by the investigator while handling the evidence to maintain its integrity. Scientific methods are used for the extraction of data and they are as follows.

10.1. WhatsApp data extraction methods in Android mobile device:

i. Mobile forensic application:

Mobile forensic applications can extract data from the mobile device storage, analyze the extracted data, and create a report of all the information found in the analysis. Mobile forensic applications use various protocols to communicate with the storage and operating system and extract data stored. As the mobile device ecosystem is diverse, with multiple operating systems, data storage mechanisms, and customizations applied by manufacturers to differentiate their devices from the competitors, mobile forensic applications must rely on custom-developed proprietary protocols to extract data. For example, an investigator can extract data from Android-based mobile devices by directly connecting it to a mobile forensic application like GMD Hancom (MD-Live, MD-Next, MD-Red), MOBILedit Forensic Express, UFED 4PC, MSAB-XRY, Magnet Axiom Complete, Oxygen Forensics, etc.

ii. Accessing the original WhatsApp database:

WhatsApp databases can be accessed directly from an Android mobile device. Database files can be copied from mobile devices to the investigator's system, but the challenge is all the data on these databases is encrypted. So, accessing the chat details directly from a database is not possible. Whereas, All the media files can be accessed without any restrictions.

iii. Downgrading WhatsApp:

The recent versions of WhatsApp have set restrictions to its database files, making it impossible or difficult to access or copy the database files to an investigator's system. Downgrading the application to an older version gives us access to WhatsApp database files which lets us copy the files to the investigator's system for further analysis. App downgrading does not delete the user data. App downgrading is only possible while extracting WhatsApp data through a mobile forensic application. App downgrading is done automatically by the mobile forensic application and does not involve any manual intervention by the investigator.

iv. WhatsApp Backup on Android Device:

WhatsApp application takes a backup of the entire chat and all the shared media every day at 2 AM as pre-defined in the application settings. These backup files are encrypted as a ".crypt12" file and stored in the mobile device storage. These backup files can be extracted and analyzed using a mobile forensic application if available on a mobile device. The encrypted ".crypt12" files will be available at "/data/com.WhatsApp/ databases/msgstore.db.crypt12"

v. WhatsApp Backup on Cloud:

WhatsApp also has an option to sync the backup files to the cloud through Google Drive. However, these cloud backup files can only be restored to an Android mobile while re-installing the application. If the restore backup option is not selected while re-installing the WhatsApp application, the backup files on cloud storage will be deleted automatically. The backup files on cloud storage cannot be accessed directly, but investigators can use applications like Elcomsoft Explorer for WhatsApp to download the cloud backup files for analysis.

10.2. WhatsApp data extraction methods in an iOS mobile device:

i. Mobile forensic application:

Apple iOS devices have a completely different approach towards mobile device storage and its organization. iOS devices do not permit a user to access or view the files on the mobile storage natively. As there is no direct access to storage, accessing the WhatsApp database files using a file manager is impossible in iOS devices. Furthermore, iOS device storage is not accessible even if the mobile device is connected to a PC. Therefore, to extract WhatsApp data and analyze the data, an investigator must directly connect the iOS device to a mobile forensic application.

ii. WhatsApp Backup using iTunes:

iTunes can be used to sync or take backup of the iOS device to a PC. iTunes backup also follows a proprietary format and does not expose application files and folders to the user. The investigator can use a mobile forensic application like Elcomsoft Phone Viewer and MOBILedit Forensic Express to analyze these iTunes backup files.

iii. WhatsApp Backup on iCloud:

WhatsApp also has an option to sync the backup files to iCloud. However, these iCloud backup files are not accessible to the user. They are only helpful in restoring WhatsApp chats and media when the application is re-installed on a user's mobile device. To analyze this iCloud backup, the investigator can use a mobile forensic application like Elcomsoft Phone Viewer and MOBILedit Forensic Express.

11. Manual Data Verification From WhatsApp Databases

WhatsApp database files present in the "/data/com.WhatsApp/databases" location of an android device can be examined manually using DB browser for SQLite application. For this, the database files must be copied manually from the mobile device to the investigator's PC using the Android Debug Bridge (ADB) commands or any other proprietary communication protocol specific to that make and model of the Android device. This process will be helpful in some instances if a forensic tool does not clearly show few details like linked PC or Mac or payment information. For the manual verification process, an investigator must have a sound knowledge of database architecture, without which an investigator may not understand how to get data stored in the database.

11.1. Data found in "msgstore.db" database:

msgstore.db contains WhatsApp call log, chat list, chat group participants, message settings, message labels, deleted message labels, chat messages, chat group invite links.

- In the "**available_message_view**" table of the "**msgstore.db**" database, we get details about the message sender, like their WhatsApp profile information.

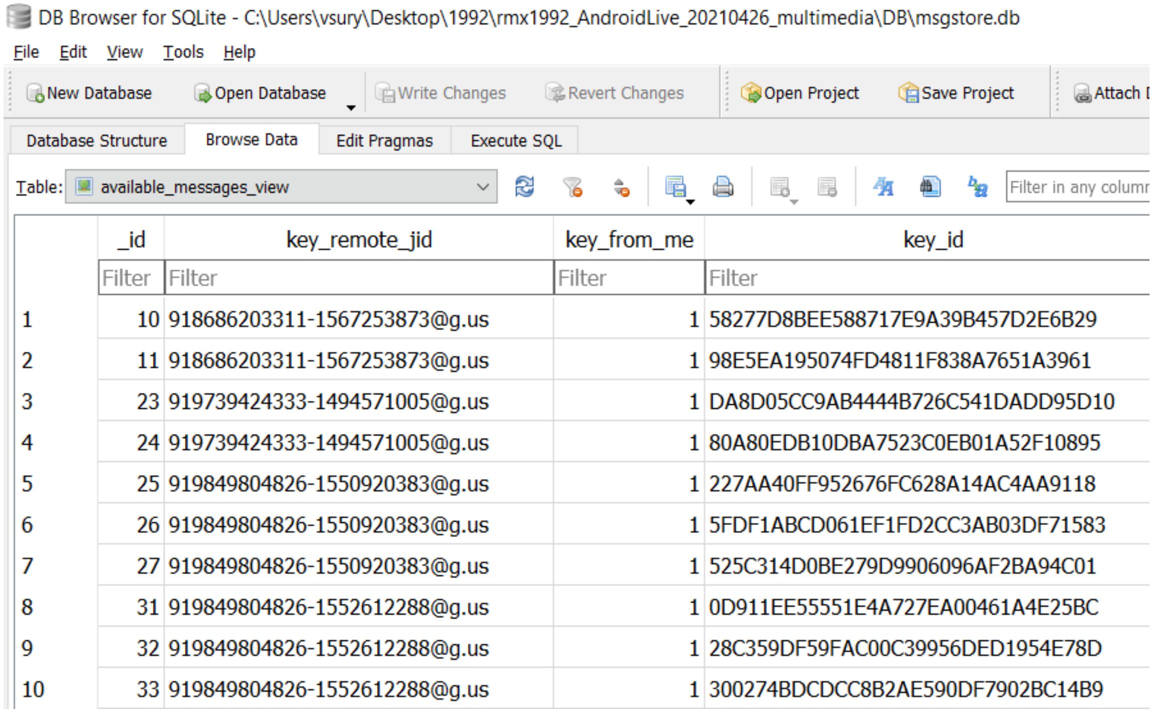


Table: available_messages_view

	_id	key_remote_jid	key_from_me	key_id
	Filter	Filter	Filter	Filter
1	10	918686203311-1567253873@g.us	1	58277D8BEE588717E9A39B457D2E6B29
2	11	918686203311-1567253873@g.us	1	98E5EA195074FD4811F838A7651A3961
3	23	919739424333-1494571005@g.us	1	DA8D05CC9AB4444B726C541DADD95D10
4	24	919739424333-1494571005@g.us	1	80A80EDB10DBA7523C0EB01A52F10895
5	25	919849804826-1550920383@g.us	1	227AA40FF952676FC628A14AC4AA9118
6	26	919849804826-1550920383@g.us	1	5FDF1ABCD061EF1FD2CC3AB03DF71583
7	27	919849804826-1550920383@g.us	1	525C314D0BE279D9906096AF2BA94C01
8	31	919849804826-1552612288@g.us	1	0D911EE55551E4A727EA00461A4E25BC
9	32	919849804826-1552612288@g.us	1	28C359DF59FAC00C39956DED1954E78D
10	33	919849804826-1552612288@g.us	1	300274BDCDCC8B2AE590DF7902BC14B9

Fig-3: WhatsApp IDs of Senders

- We get the chat message content from a contact in the "**legacy_available_message_view**" table of the "**msgstore.db**" database.

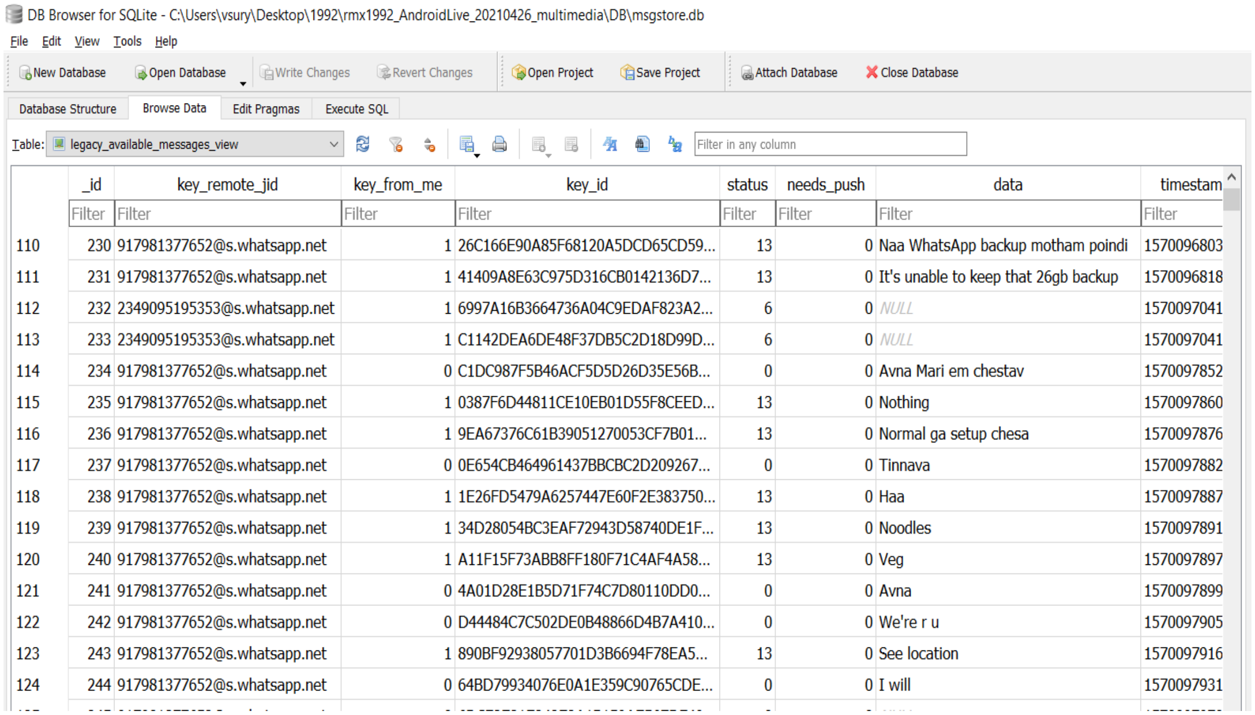


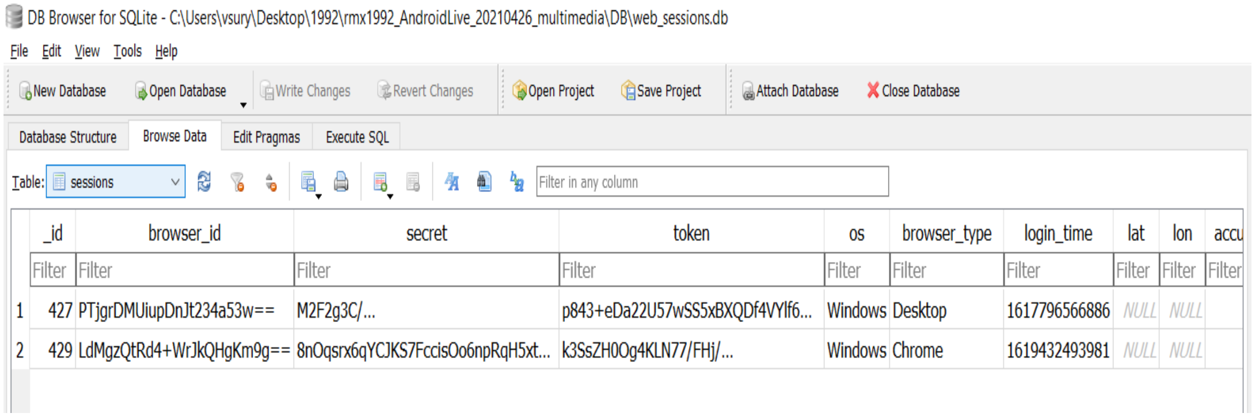
Table: legacy_available_messages_view

	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	timestam
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
110	230	917981377652@s.whatsapp.net	1	26C166E90A85F68120A5DCD65CD59...	13	0	Naa WhatsApp backup motham poindi	1570096803
111	231	917981377652@s.whatsapp.net	1	41409A8E63C975D316CB0142136D7...	13	0	It's unable to keep that 26gb backup	1570096818
112	232	2349095195353@s.whatsapp.net	1	6997A16B3664736A04C9EDAF823A2...	6	0	NULL	1570097041
113	233	2349095195353@s.whatsapp.net	1	C1142DEA6DE48F37DB5C2D18D99D...	6	0	NULL	1570097041
114	234	917981377652@s.whatsapp.net	0	C1DC987F5B46ACF5D5D26D35E56B...	0	0	Avna Mari em chestav	1570097852
115	235	917981377652@s.whatsapp.net	1	0387F6D44811CE10EB01D55F8CEED...	13	0	Nothing	1570097860
116	236	917981377652@s.whatsapp.net	1	9EA67376C61B39051270053CF7B01...	13	0	Normal ga setup chesa	1570097876
117	237	917981377652@s.whatsapp.net	0	0E654CB464961437BBCBC2D209267...	0	0	Tinnava	1570097882
118	238	917981377652@s.whatsapp.net	1	1E26FD5479A6257447E60F2E383750...	13	0	Haa	1570097887
119	239	917981377652@s.whatsapp.net	1	34D28054BC3EAF72943D58740DE1F...	13	0	Noodles	1570097891
120	240	917981377652@s.whatsapp.net	1	A11F15F73ABB8FF180F71C4AF4A58...	13	0	Veg	1570097897
121	241	917981377652@s.whatsapp.net	0	4A01D28E1B5D71F74C7D80110DD0...	0	0	Avna	1570097899
122	242	917981377652@s.whatsapp.net	0	D44484C7C502DE0B48866D4B7A410...	0	0	We're r u	1570097905
123	243	917981377652@s.whatsapp.net	1	890BF92938057701D3B6694F78EA5...	13	0	See location	1570097916
124	244	917981377652@s.whatsapp.net	0	64BD79934076E0A1E359C90765CDE...	0	0	I will	1570097931

Fig-4: WhatsApp chat message contents

11.2. Data found in “web_sessions.db” database:

- "**web_sessions.db**" database gives information about the WhatsApp web and WhatsApp desktop client sessions where the WhatsApp application has been synced.



DB Browser for SQLite - C:\Users\vsury\Desktop\1992\rmx1992_AndroidLive_20210426_multimedia\DB\web_sessions.db

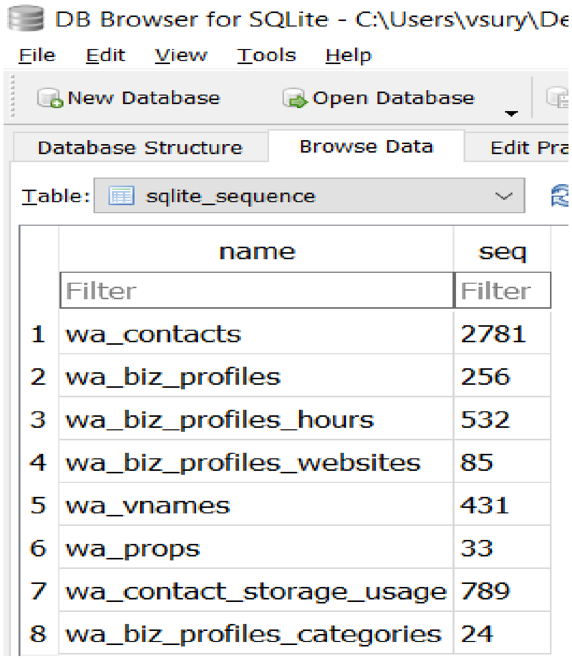
Table: sessions

	_id	browser_id	secret	token	os	browser_type	login_time	lat	lon	accu
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	427	PTjgrDMUiupDnJt234a53w==	M2F2g3C/...	p843+eDa22U57wSS5xBXQDf4VYlf6...	Windows	Desktop	1617796566886	NULL	NULL	
2	429	LdMgzQtRd4+WrJkQHgKm9g==	8nOqsrx6qYCJKS7FccisOo6npRqH5xt...	k3SsZH0Og4KLN77/FHj/...	Windows	Chrome	1619432493981	NULL	NULL	

Fig-5: WhatsApp desktop and web client sessions information

11.3. Data found in "wa.db" database:

- wa.db database gives us information about the number of WhatsApp business profiles, contacts, websites, and categories.



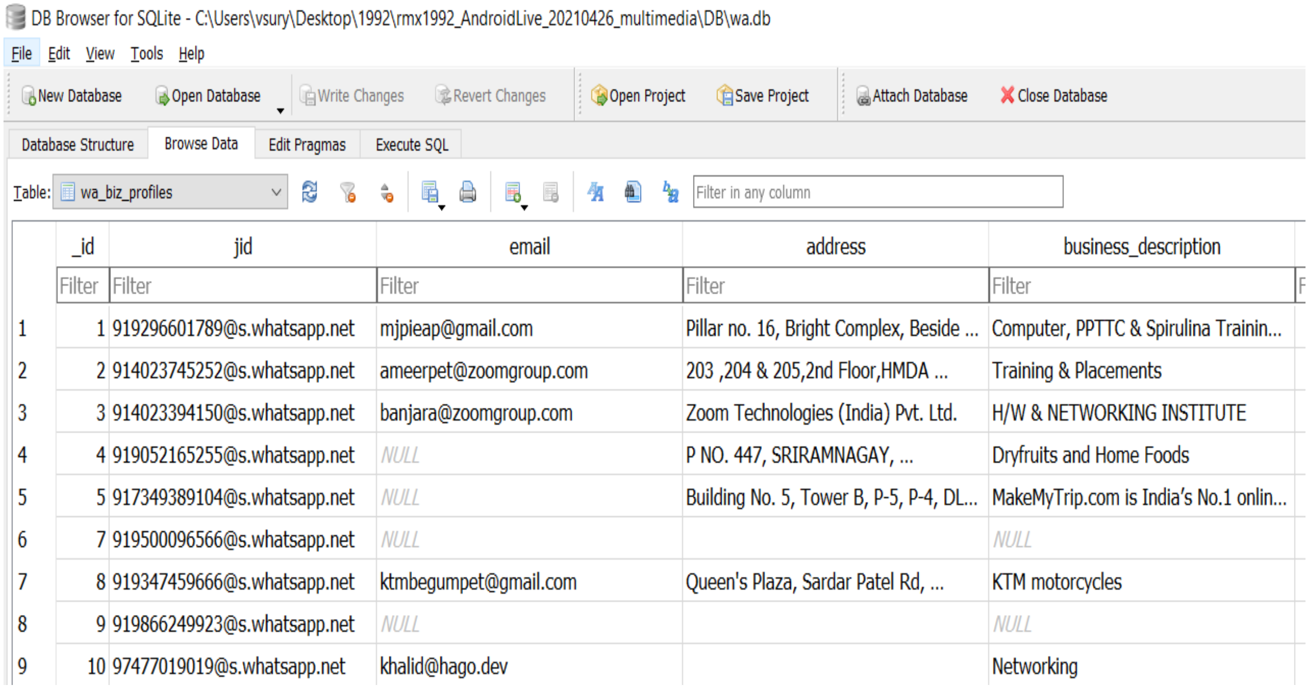
DB Browser for SQLite - C:\Users\vsury\De

Table: sqlite_sequence

	name	seq
	Filter	Filter
1	wa_contacts	2781
2	wa_biz_profiles	256
3	wa_biz_profiles_hours	532
4	wa_biz_profiles_websites	85
5	wa_vnames	431
6	wa_props	33
7	wa_contact_storage_usage	789
8	wa_biz_profiles_categories	24

Fig-6: WhatsApp business profile's details

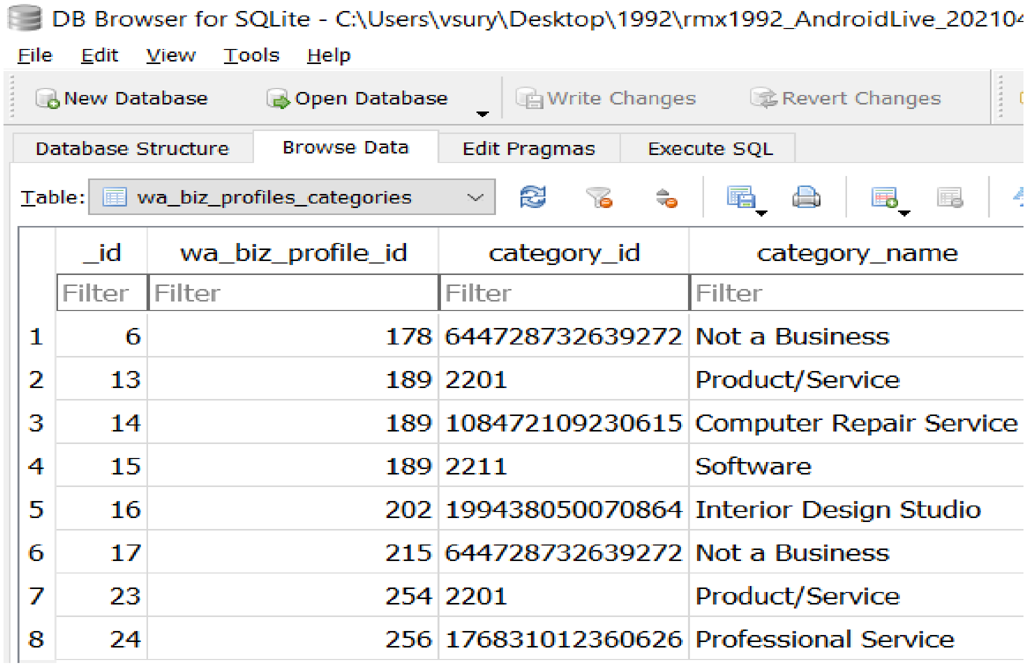
- In the "**wa_biz_profiles**" table of "**wa.db**" database, we can see WhatsApp business profile details like their WhatsApp profile information, email address, business address, and business description.



	_id	jid	email	address	business_description
1	1	919296601789@s.whatsapp.net	mjpieap@gmail.com	Pillar no. 16, Bright Complex, Beside ...	Computer, PPTTC & Spirulina Trainin...
2	2	914023745252@s.whatsapp.net	ameerpet@zoomgroup.com	203 ,204 & 205,2nd Floor,HMDA ...	Training & Placements
3	3	914023394150@s.whatsapp.net	banjara@zoomgroup.com	Zoom Technologies (India) Pvt. Ltd.	H/W & NETWORKING INSTITUTE
4	4	919052165255@s.whatsapp.net	NULL	P NO. 447, SRIRAMNAGAY, ...	Dryfruits and Home Foods
5	5	917349389104@s.whatsapp.net	NULL	Building No. 5, Tower B, P-5, P-4, DL...	MakeMyTrip.com is India’s No.1 onlin...
6	7	919500096566@s.whatsapp.net	NULL		NULL
7	8	919347459666@s.whatsapp.net	ktmbegumpet@gmail.com	Queen's Plaza, Sardar Patel Rd, ...	KTM motorcycles
8	9	919866249923@s.whatsapp.net	NULL		NULL
9	10	97477019019@s.whatsapp.net	khalid@hago.dev		Networking

Fig-7: WhatsApp business profile's addresses

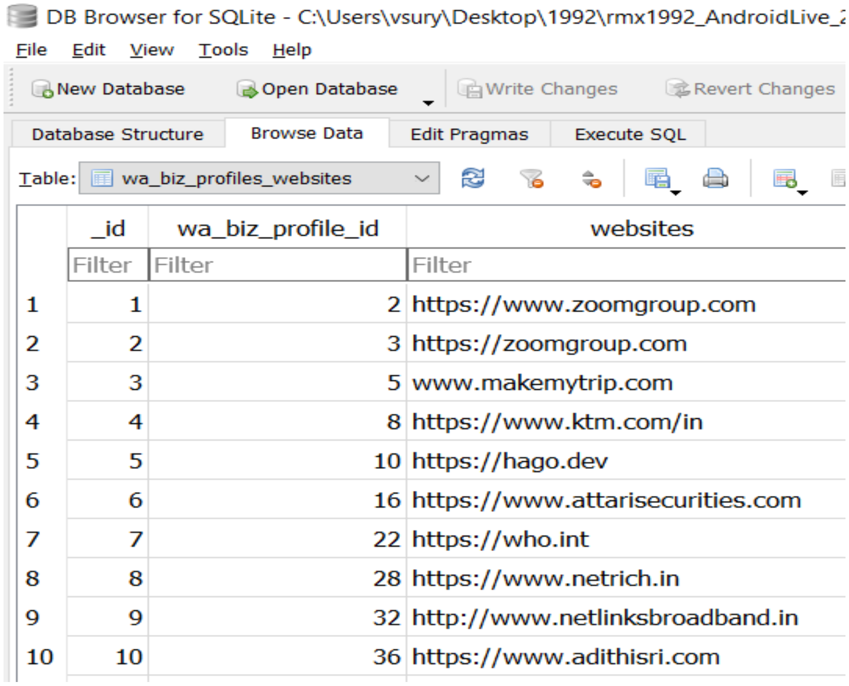
We can see WhatsApp business profile categories in the "**wa_biz_profiles_categories**" table of "**wa.db**" database. The "**_id**" tag is a reference of "_id" tag in the "**wa_biz_profiles**" table of "**wa.db**" database.


DB Browser for SQLite - C:\Users\vsury\Desktop\1992\rmx1992_AndroidLive_20210
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: wa_biz_profiles_categories

	_id	wa_biz_profile_id	category_id	category_name
1	6	178	644728732639272	Not a Business
2	13	189	2201	Product/Service
3	14	189	108472109230615	Computer Repair Service
4	15	189	2211	Software
5	16	202	199438050070864	Interior Design Studio
6	17	215	644728732639272	Not a Business
7	23	254	2201	Product/Service
8	24	256	176831012360626	Professional Service

Fig-8: WhatsApp business profile's categories information

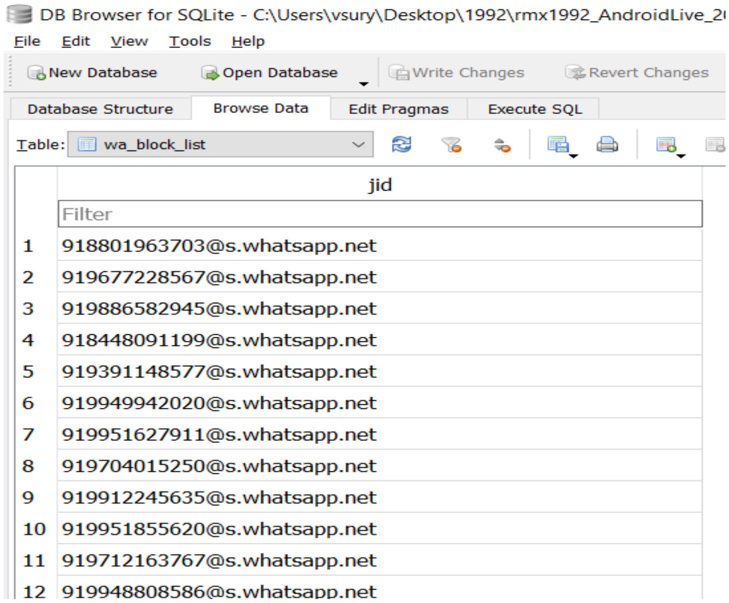
- We can see WhatsApp business profile's website addresses in the "**wa_biz_profiles_websites**" table of "**wa.db**" database. The "**_id**" tag is a reference of "_id" tag in the "**wa_biz_profiles**" table of "**wa.db**" database.


DB Browser for SQLite - C:\Users\vsury\Desktop\1992\rmx1992_AndroidLive_2
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Table: wa_biz_profiles_websites

	_id	wa_biz_profile_id	websites
	Filter	Filter	Filter
1	1	2	https://www.zoomgroup.com
2	2	3	https://zoomgroup.com
3	3	5	www.makemytrip.com
4	4	8	https://www.ktm.com/in
5	5	10	https://hago.dev
6	6	16	https://www.attarisecurities.com
7	7	22	https://who.int
8	8	28	https://www.netrich.in
9	9	32	http://www.netlinksbroadband.in
10	10	36	https://www.adithisri.com

Fig-9: WhatsApp business profile's website URLs

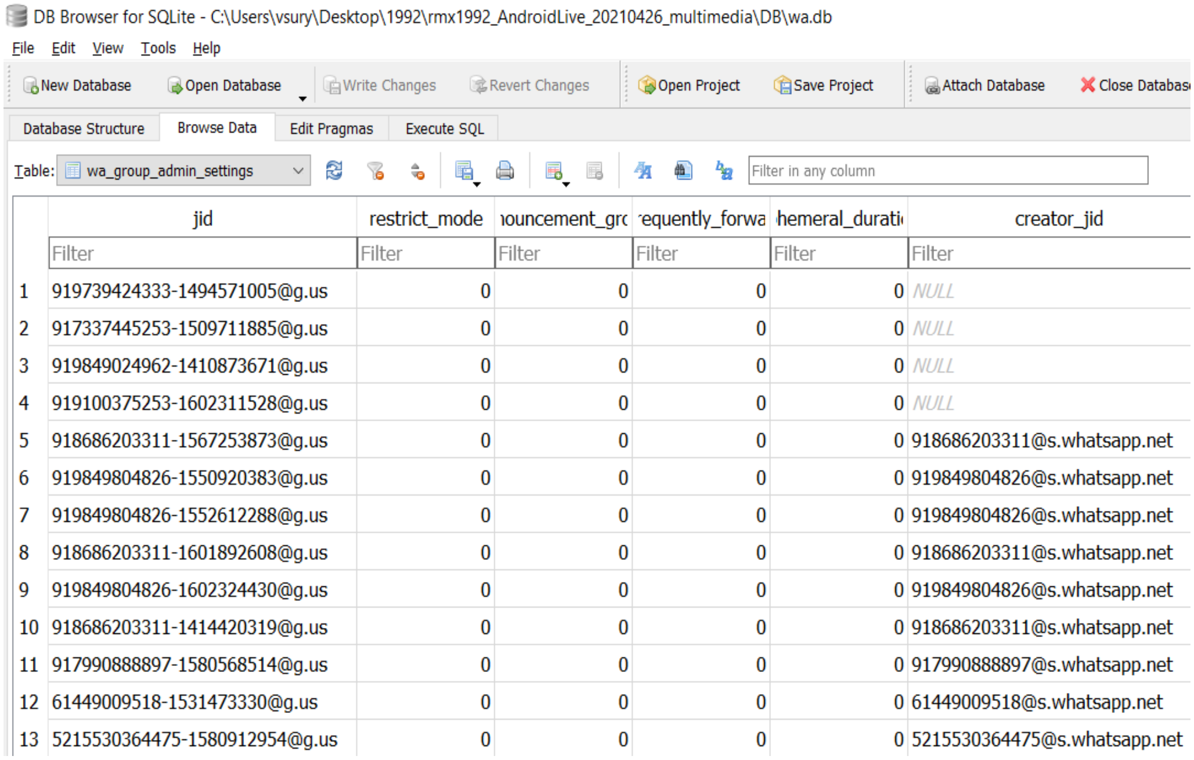
- We can see a blocked contacts list for a WhatsApp profile in the "**wa_block_list**" table of "**wa.db**" database.



	jid
	Filter
1	918801963703@s.whatsapp.net
2	919677228567@s.whatsapp.net
3	919886582945@s.whatsapp.net
4	918448091199@s.whatsapp.net
5	919391148577@s.whatsapp.net
6	919949942020@s.whatsapp.net
7	919951627911@s.whatsapp.net
8	919704015250@s.whatsapp.net
9	919912245635@s.whatsapp.net
10	919951855620@s.whatsapp.net
11	919712163767@s.whatsapp.net
12	919948808586@s.whatsapp.net

Fig-10: WhatsApp blocked contacts information

- In the "**wa_group_admin_settings**" table of "**wa.db**" database, we can see WhatsApp group administrator profile details in "**creator_id**" field.



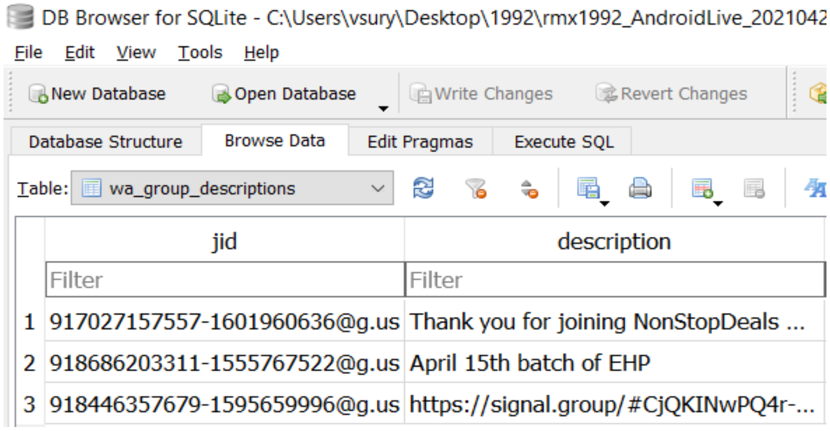
DB Browser for SQLite - C:\Users\vsury\Desktop\1992\rmx1992_AndroidLive_20210426_multimedia\DB\wa.db

Table: wa_group_admin_settings

	jid	restrict_mode	ıouncement_grc	·equently_forwa	·hemeral_durati	creator_jid
	Filter	Filter	Filter	Filter	Filter	Filter
1	919739424333-1494571005@g.us	0	0	0	0	NULL
2	917337445253-1509711885@g.us	0	0	0	0	NULL
3	919849024962-1410873671@g.us	0	0	0	0	NULL
4	919100375253-1602311528@g.us	0	0	0	0	NULL
5	918686203311-1567253873@g.us	0	0	0	0	918686203311@s.whatsapp.net
6	919849804826-1550920383@g.us	0	0	0	0	919849804826@s.whatsapp.net
7	919849804826-1552612288@g.us	0	0	0	0	919849804826@s.whatsapp.net
8	918686203311-1601892608@g.us	0	0	0	0	918686203311@s.whatsapp.net
9	919849804826-1602324430@g.us	0	0	0	0	919849804826@s.whatsapp.net
10	918686203311-1414420319@g.us	0	0	0	0	918686203311@s.whatsapp.net
11	917990888897-1580568514@g.us	0	0	0	0	917990888897@s.whatsapp.net
12	61449009518-1531473330@g.us	0	0	0	0	61449009518@s.whatsapp.net
13	5215530364475-1580912954@g.us	0	0	0	0	5215530364475@s.whatsapp.net

Fig-11: WhatsApp group administrator's information

- We can see WhatsApp group descriptions in the "**wa_group_descriptions**" table of "**wa.db**" database.



DB Browser for SQLite - C:\Users\vsury\Desktop\1992\rmx1992_AndroidLive_2021042

Table: wa_group_descriptions

	jid	description
	Filter	Filter
1	917027157557-1601960636@g.us	Thank you for joining NonStopDeals ...
2	918686203311-1555767522@g.us	April 15th batch of EHP
3	918446357679-1595659996@g.us	https://signal.group/#CjQKINwPQ4r-...

Fig-12: WhatsApp group's descriptions

- In the "**wa_props**" table of "**wa.db**" database, we can see WhatsApp media storage size information along with the number of media files.

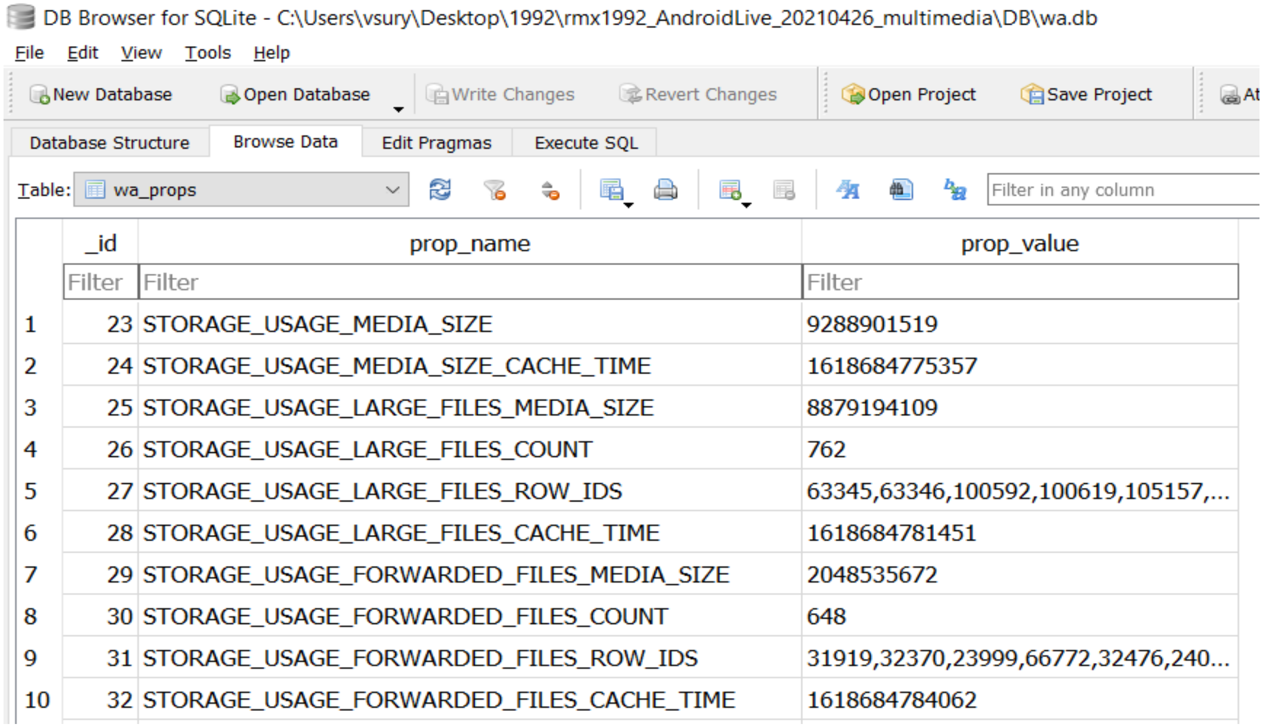


Table: wa_props

	_id	prop_name	prop_value
	Filter	Filter	Filter
1	23	STORAGE_USAGE_MEDIA_SIZE	9288901519
2	24	STORAGE_USAGE_MEDIA_SIZE_CACHE_TIME	1618684775357
3	25	STORAGE_USAGE_LARGE_FILES_MEDIA_SIZE	8879194109
4	26	STORAGE_USAGE_LARGE_FILES_COUNT	762
5	27	STORAGE_USAGE_LARGE_FILES_ROW_IDS	63345,63346,100592,100619,105157,...
6	28	STORAGE_USAGE_LARGE_FILES_CACHE_TIME	1618684781451
7	29	STORAGE_USAGE_FORWARDED_FILES_MEDIA_SIZE	2048535672
8	30	STORAGE_USAGE_FORWARDED_FILES_COUNT	648
9	31	STORAGE_USAGE_FORWARDED_FILES_ROW_IDS	31919,32370,23999,66772,32476,240...
10	32	STORAGE_USAGE_FORWARDED_FILES_CACHE_TIME	1618684784062

Fig-13: WhatsApp storage information

11.4. Data found in "contents.db" database:

- "**contents.db**" database gives information about the mobile device like a model, make, Android ID, device serial number, IMEI number, IMSI number and time zone on which WhatsApp is installed.

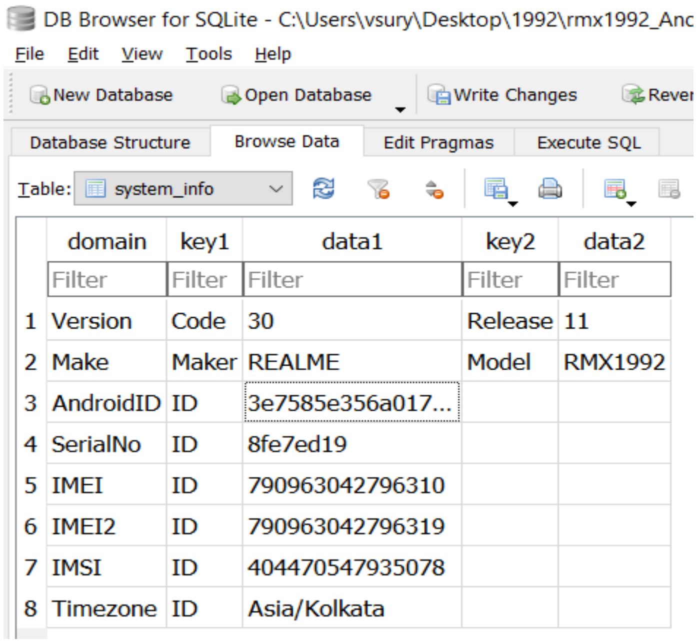


Table: system_info

	domain	key1	data1	key2	data2
	Filter	Filter	Filter	Filter	Filter
1	Version	Code	30	Release	11
2	Make	Maker	REALME	Model	RMX1992
3	AndroidID	ID	3e7585e356a017...		
4	SerialNo	ID	8fe7ed19		
5	IMEI	ID	790963042796310		
6	IMEI2	ID	790963042796319		
7	IMSI	ID	404470547935078		
8	Timezone	ID	Asia/Kolkata		

Fig-14: Mobile device information where WhatsApp is installed

11.5. Data found in "media.db" database:

- "**media.db**" gives us information about shared media files like images, audio, video, documents along with the path of the file on the device storage and the file type information.

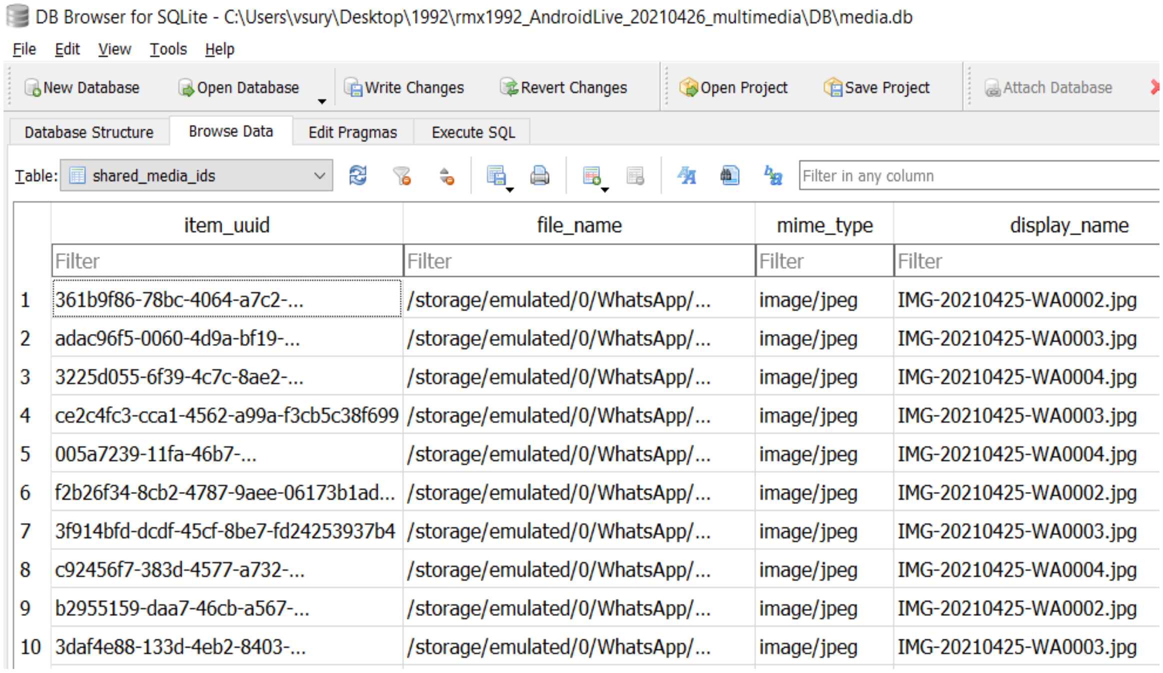


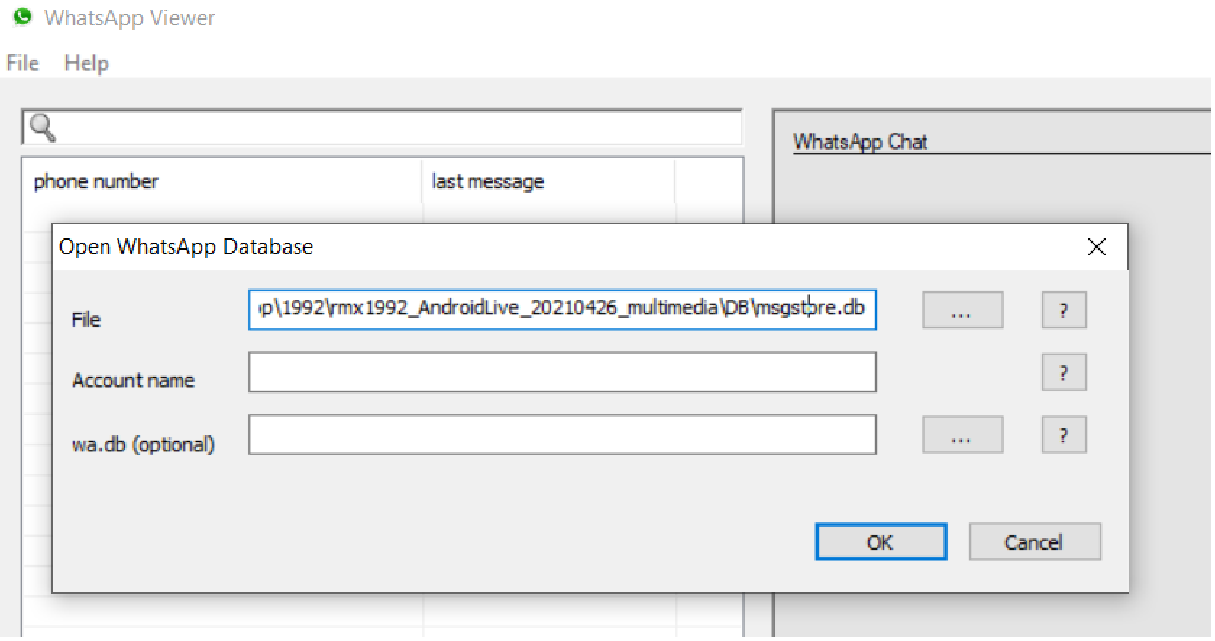
Table: shared_media_ids

	item_uuid	file_name	mime_type	display_name
	Filter	Filter	Filter	Filter
1	361b9f86-78bc-4064-a7c2-...	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0002.jpg
2	adac96f5-0060-4d9a-bf19-...	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0003.jpg
3	3225d055-6f39-4c7c-8ae2-...	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0004.jpg
4	ce2c4fc3-cca1-4562-a99a-f3cb5c38f699	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0003.jpg
5	005a7239-11fa-46b7-...	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0004.jpg
6	f2b26f34-8cb2-4787-9aee-06173b1ad...	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0002.jpg
7	3f914bfd-dcdf-45cf-8be7-fd24253937b4	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0003.jpg
8	c92456f7-383d-4577-a732-...	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0004.jpg
9	b2955159-daa7-46cb-a567-...	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0002.jpg
10	3daf4e88-133d-4eb2-8403-...	/storage/emulated/0/WhatsApp/...	image/jpeg	IMG-20210425-WA0003.jpg

Fig-15: Information of sharing media files using WhatsApp

12. Manually View WhatsApp Messages In Conversation View

Investigator can use a third-party tool like "**WhatsApp Viewer**" to view the messages stored in "**/data/com.WhatsApp/databases/msgstore.db**" in a conversation view. The investigator must open the "**msgstore.db**" database file using the application to view the chat conversation.



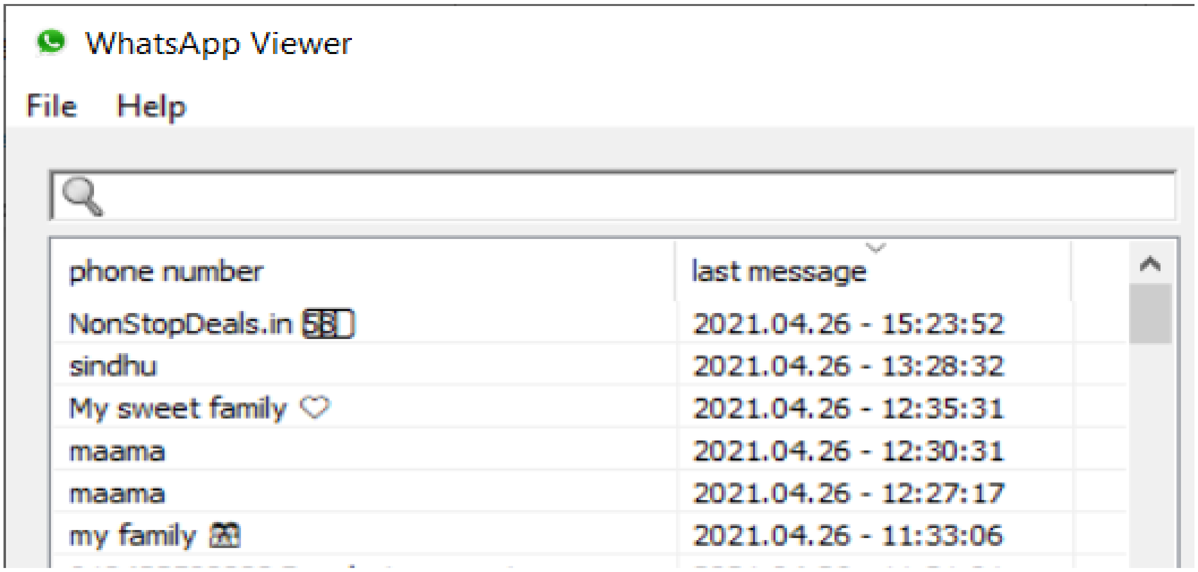
File: p\1992\rmx1992_AndroidLive_20210426_multimedia\DB\msgstore.db

Account name:

wa.db (optional):

Fig-16: WhatsApp database file selection in WhatsApp Viewer application

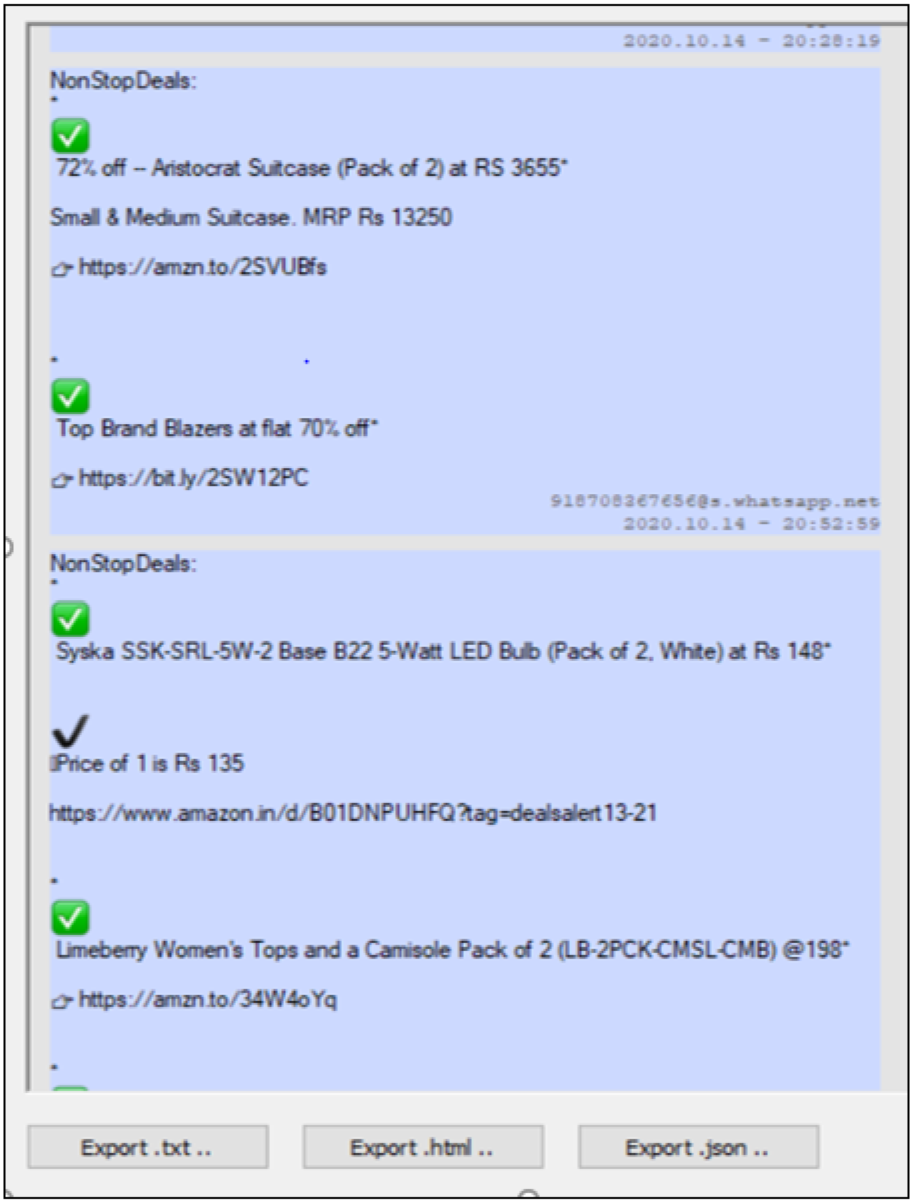
- The application analyses the chats in the database file and displays information about the contact or the group and the date and time of the last message from that contact or group as shown in the below image.



phone number	last message
NonStopDeals.in 58	2021.04.26 - 15:23:52
sindhu	2021.04.26 - 13:28:32
My sweet family ♡	2021.04.26 - 12:35:31
maama	2021.04.26 - 12:30:31
maama	2021.04.26 - 12:27:17
my family	2021.04.26 - 11:33:06

Fig-17: WhatsApp contact's/group's last message data & time information in WhatsApp Viewer application

- Selecting any of the contact or group displays the full chat in a conversation view along with the date and time of the message and sender information as shown in the below image. The chat conversation can also be exported into a text file or html file or json file.



2020.10.14 - 20:28:19

NonStopDeals:

✓ 72% off – Aristocrat Suitcase (Pack of 2) at RS 3655*

Small & Medium Suitcase. MRP Rs 13250

☞ https://amzn.to/2SVUBfs

✓ Top Brand Blazers at flat 70% off*

☞ https://bit.ly/2SW12PC

918708367656@s.whatsapp.net
2020.10.14 - 20:52:59

NonStopDeals:

✓ Syska SSK-SRL-5W-2 Base B22 5-Watt LED Bulb (Pack of 2, White) at Rs 148*

✓ Price of 1 is Rs 135

https://www.amazon.in/d/B01DNPUHFQ?tag=dealsalert13-21

✓ Limeberry Women's Tops and a Camisole Pack of 2 (LB-2PCK-CMSL-CMB) @198*

☞ https://amzn.to/34W4oYq

Fig-18: WhatsApp message conversation view in WhatsApp Viewer application

13. WhatsApp Client Verification On A User's PC

WhatsApp can be accessed using a desktop client on a user's PC or by syncing WhatsApp with a web browser installed on the user's PC. It gives the user an option to send, receive messages or multimedia, make, and receive calls using their PC. An investigator can check if the user has connected to WhatsApp through their PC by looking at the log file or the SQLite database file of the specific web browser. The table below shows the log file or database file for the Windows desktop client, Google Chrome web browser and Mozilla Firefox browser.

Application	Path on PC
Windows desktop	C:\Users\{username}\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\Roaming\WhatsApp\IndexedDB\file__0.indexeddb.leveldb/{**

client	****}.log
Google Chrome	C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_web.WhatsApp.com_0.indexeddb.leveldb\{******}.log
Mozilla Firefox	C:\Users\{username}\AppData\Roaming\Mozilla\Firefox\Profiles\xqimcopc.default\storage\default\https+++web.WhatsApp.com\idb\{##########}wcaw.sqlite

Table-7: Location of WhatsApp log and database files on PC

An investigator can find the messages or media shared with or received from WhatsApp web or desktop clients. However, this log file and database file do not show the contents of the chat or the actual file that has been shared. The desktop or web client of WhatsApp would relay information to the user's mobile device, sending or receiving the chat message or the media file being shared. The below table shows the various status messages like a message sent, received, media shared, etc. The timestamps shown for all the status messages in the log file is in YYYY-MM-DD HH:MM:SS.MS format according to Pacific Time (PT) zone, which is 12 hours 30 minutes behind Indian Standard Time (IST). So, if a message is marked to be sent at 13:40:02:45 IST is shown as 01:10:02:45 in the log file. An investigator has to consider this time zone difference while analyzing the status message's timestamps.

Log status	Note
Windows desktop clientaction,presence,[available/unavailable]	User's online or offline status
action,chatstate,[composing/paused/recording]	It shows if a user is typing the message or it is paused. This status is recorded every 10 seconds after the user starts typing a message in chat.
action,message,[image/video/chat/vcard/document/ptt]	This status message shows when a message or media file has been sent from the user. It does not portray us the recipient information.
action,msgs,delete	This status message shows when the user has deleted a message.
action,battery,{**},true/false	This status shows the battery status on the user's mobile device. ** is the percentage of battery.
action,chat,read	This status message shows that the user has read the message.
action,status,read	This status message shows the user has viewed a status upload of a contact.
Media:sendToChat chat {************}@c.us	This status message shows that the user has sent a media file to a contact. {************} is the recipient's contact number, including the country code.
Media:sendToChat chat {************}@g.us	This status message shows that the user has sent a media file to a contact. {************} is the WhatsApp group ID.
action,msg,relay,[chat,image,video],{###########}@c.us,{************}@c.us	This status message shows that the user has received a chat message or a media file from a contact. {###########}@c.us is the user's WhatsApp ID, {************}@c.us is the sender's WhatsApp ID.
action,msg,relay,image,status@broadcast,{###########}@c.us,false_status@broadcast_4790FEFF50776B69E817BF1AB725DE46,{************}	This status message shows that the user has received a status upload message or media from a contact. For example, {###########}@c.us is the user's WhatsApp ID, {************}@c.us is the sender's WhatsApp ID.

@c.us	

Table-8: WhatsApp desktop and web client status messages from the log file.

14. Investigator's Challenges

Investigators face various challenges while extracting WhatsApp data from either Android or iOS mobile devices. In some instances, the mobile device is locked and there is no password to unlock the device. In such cases, data extraction is not possible. A significant challenge is various make and model of the devices, updated security patch levels, encrypted communication of WhatsApp, encrypted database files of WhatsApp. Features like delete to everyone and disappearing message features make it even more challenging to retrieve the data. Suppose the suspect user has changed the mobile device after the crime and has not restored the WhatsApp backup while installing the application. In that case, all the evidence will be lost as the backup file will be deleted from the cloud storage also. When multimedia files like images or videos are shared using WhatsApp, all the metadata related to the image or video, including the name of the image or video, will be stripped out of the file and the resolution of the image or video will be shrunk. All metadata, including the name of the image set as a profile picture of the contact, will be stripped. Data deleted from mobile devices like chat messages, images, videos, audio files, documents once deleted may be difficult to retrieve if physical data extraction is impossible. Accessing the contents of ".crypt12" files either on the user's mobile device or PC is impossible because those files are encrypted. The key to decrypt them stored in the user's mobile will not be directly accessible unless the mobile device is rooted.

15. Mobile Data Extraction Software

Mobile forensic software can acquire data from a mobile device using specialized debugging protocols explicitly developed for the Operating System or by extracting a physical dump of the mobile device storage. Mobile forensic software can also analyze the extracted data from a mobile phone and gives us a detailed view of all the data found.

The list of software that can be used for mobile forensic data extraction and analysis:

i. Hancom MD-Series (http://hancomwith.com)

ii. MOBILedit Forensic Express (https://www.mobiledit.com/forensic-express)

iii. ADF Digital Evidence Investigator pro (https://www.adfsolutions.com/dei-pro)

iv. Cellebrite UFED (https://www.cellebrite.com/en/ufed)

v. MSAB XRY (https://www.msab.com/products/xry)

vi. Oxygen Forensic (https://www.oxygen-forensic.com/en/products/oxygen-forensic-extractor)

vii. Elcomsoft Explorer for WhatsApp (https://www.elcomsoft.com/exwa.html)

viii. DB Browser for SQLite (https://sqlitebrowser.org/dl/)

16. Conclusion

Mobile forensics is an evolving discipline in cyber forensics. For example, mobile forensic software can acquire WhatsApp artifacts such as WhatsApp call logs, text messages, shared images, video, audio, contacts, location information and analyze them.

As mobile operating systems evolve with improving security acquiring physical dump from a mobile device is becoming a challenge. WhatsApp keeps adding new security features to the application regularly, such as end-to-end encryption of all data exchanged, encrypted databases on the mobile device, etc. Therefore, not accessing the database files on a mobile device needs constant research work to overcome these restrictions in data acquisition.

WhatsApp continues to be a dominant internet-based messenger application across Android and iOS platforms despite many competing applications like Signal, Telegram, etc., providing similar features. Every message or multimedia file retrieved from WhatsApp conversations can help solve a case in one way or another. WhatsApp chat messages, call logs, and multimedia can be very helpful as a piece of evidence in proving the crime in many investigations.

17. References

[1] https://www.WhatsApp.com

[2] https://www.WhatsApp.com/security/WhatsApp-Security-Whitepaper.pdf

[3] https://www.WhatsApp.com/features/

[4] https://faq.WhatsApp.com/general/

[5] https://backlinko.com/WhatsApp-users

[6] https://twitter.com/wcathcart/status/1334942254016786434?ref_src=twsrc%5Etfw

[7] https://www.statista.com/statistics/260819/number-of-monthly-active-WhatsApp-users/

[8] https://en.wikipedia.org/wiki/Timeline_of_WhatsApp#:~:text=WhatsApp%20introduces%20its%20document%2Dsharing,PDF%20files%20with%20their%20contacts.&text=WhatsApp%20and%20Open%20Whisper%20Systems,now%20verify%20each%20other's%20keys

[9] https://www.indiatoday.in/technology/news/story/WhatsApp-users-in-india-spent-21-3-hours-per-month-on-an-average-in-2020-report-1759371-2021-01 15#:~:text=WhatsApp%20led%20the%20way%20when,hours%20per%20month%20in%202019

[10] https://techcrunch.com/2020/10/29/WhatsApp-is-now-delivering-roughly-100-billion-messages-a-day/

AUTHOR'S PROFILE:

Mr. Nagendar Rao Koppolu joined Police Service as Sub-Inspector in the year 1998. He served in Law Enforcement, Bureau of Immigration (IB), Central Bureau of Investigation (CBI) (Anti-Corruption Wing), State Intelligence Department, and State Information Technology Cell. He pursued M.Tech (CSE), M.Sc.(IT), and Criminal Justice Data Analysis (IIT Kanpur). He is a certified Cyber Security Professional and ISO 27001 ISMS Lead Auditor. He co-authored two books on cybercrime. Presently, he is Inspector (in-charge) of State Cyber Vertical, Telangana.