WHITE PAPER

Research on how end-to-end encrypted WhatsApp data can be recovered and decrypted by MD-RED.

Contents

Background

This white paper provides a technical explanation of WhatsApp's encryption system, major features of WhatsApp that needs advanced research and how those data can be recovered/decrypted and viewed.

Summary

MD-RED will support forensic investigators to analyze various features of the latest WhatsApp installed in any version of Android and iOS. And through our regular product updates, phone models over 80 manufacturers are supported and deleted and encrypted data such as Message/Multimedia/Contacts/File and etc. can be recovered and decrypted by MD-RED.

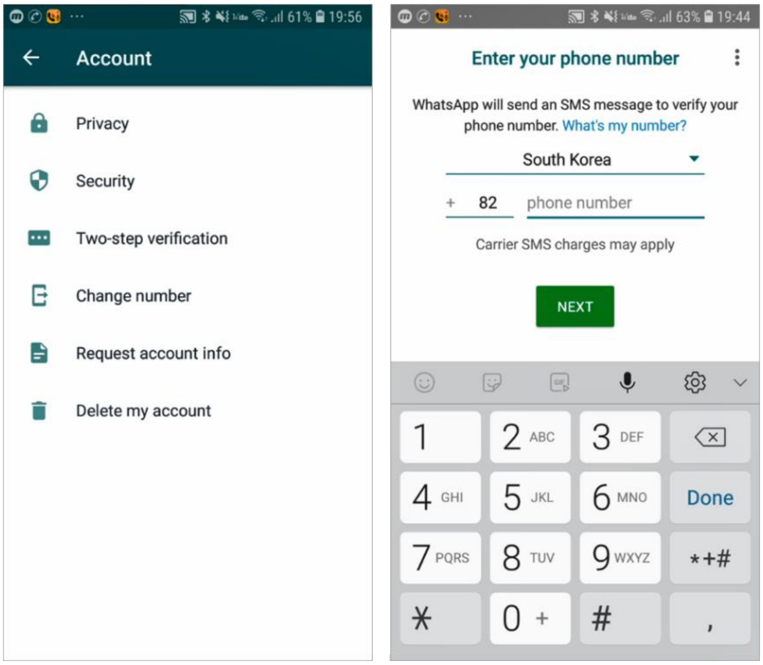
WhatsApp Overview

Major Features

❖ Supports various platforms

I. Supported OS: Android, iOS, KaiOS, Windows, MacOS, Blackberry

II. Supports KaiOS version from v2.5.(Nov. 2017)



Enter your phone number

WhatsApp will send an SMS message to verify your phone number. What's my number?

South Korea

+ 82 phone number

Carrier SMS charges may apply

Figure 1. Account

❖ Accounts

I. Allows one accounts for one mobile phone number.

II. If mobile phone number is changed, user needs to request for an account information modification.

III. It takes certain period of time after the requests for account deletion is submitted.

IV. Provides various messaging functions: Chat, Camera, Voice/Video Call, Document/Photo/Audio/Location/Contact transmission.

❖ End-to-end Encryption

WhatsApp's End-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp. For added protection, every message being sent has its own unique lock and key. All of this happens automatically: no need to turn on settings or set up special secret chats to secure the messages. Payments on WhatsApp, which are available in select countries, enable transfers between accounts at financial institutions. Card and bank numbers are stored encrypted and in a highly-secured network. However, because financial institutions can't process transactions without receiving information related to these payments, these payments aren't End-to-end encrypted.

Data analysis result of major features by MD-RED

❖ MD-Series Support Status

I. Tested environment

MD-Series	MD-NEXT 1.89.3 (Jun. 2020), MD-RED 3.6.6 (Jun. 2020), MD-CLOUD 1.3.0 (Jul. 2020)
WhatsApp Version	Android 2.20.157 (May 2020), iOS 2.20.51 (May 2020)
Tested Device	Android: Samsung SM-A510L (A5 2016), Android 8.0 iOS: Apple A1778 (iPhone 7), iOS 12.4.1

II. Supported status by platform

Platform	Data Extraction(MD-NEXT)	Data Analysis(MD-RED)
Android	Supported method – Physical, FFS, Android Live	Supports App data and decryption of encr ypted App local backup data
iOS	Supported method - FFS, iOS Backup	Supports App data

- Acquisition method varies depending on the device model, OS version, and installed WhatsApp version.
- When proceeding with Android Live method and the installed WhatsApp version is 2.19.275 (Sep. 2019) or higher, app needed to be downgraded before the extraction.
- If app downgrade and extraction is completed, reinstall WhatsApp as its' original version.
- Local Backup

- Backup methods for backup data on the device.

- Android version supports local backup, and the backup data is saved as an encrypted file.

- Encryption method depends on WhatsApp version.

- Android 2.20.157 uses crypt12 method.

- For more details, refer to 'III. Detailed information by its' features > 2. Backup setting'

IV. Deleted message status by deletion method

The results below are based on our test results, and the deletion and recovery results may vary depending on the test environment.

Platform	DELETE FOR ME	DELETE from EVERYONE	DELETE GROUP
Android	○	△	○
iOS	X	△	△

- ○: Message data remains in deleted messages.
- △: Remains Message type, Time, Receiver/Sender information, but no text contents.
- X : Deleted message does not remain.