C15 WAEventsLogParser: Recovering Hidden (and Relevant) Evidence From WhatsApp Events Log File in Android™ Devices

Mateus D.C. Polastro, MSc, Brazilian Federal Police, Campo Grande, Mato Grosso do Sul 79110-503, BRAZIL*

Learning Overview: After attending this presentation, attendees will be aware of the most relevant evidence stored in the WhatsApp events log file and will understand how investigators can use them for forensic purposes.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by presenting and exploring a new source of evidence of activities on WhatsApp for Android™, the event log file. It will also present the software developed to interpret these events and will show how new events can be discovered and configured.

Mobile messaging apps are very popular around the world and WhatsApp is the most used when considering the number of active users.[1] WhatsApp ended the year 2017 with 1.5 billion users, and many countries, such as Germany, Brazil, and Mexico, have more than 50% of their population using the app.[2,3]

WhatsApp allows the user to send text messages, voice notes, files, localization, contacts, and voice and video calls for free since the user has access to the internet. In addition, the app has a strong end-to-end encryption enabled by default, based on Signal Protocol, which prevents third parties from having access to information exchanged between the users.[4] Thus, investigators can only access the data exchanged by WhatsApp users through the mobile phone seizure and later extraction and decoding of the app data. Nevertheless, it is common for criminals to erase suspicious contacts and messages to eliminate traces of criminal activity.

Several forensic tools support the extraction and decoding of WhatsApp data and, in some cases, can retrieve deleted messages from the SQLite database. However, some events related to the use of the WhatsApp, such as the deletion date of a chat, are not stored in the app's SQLite database and available mobile forensic tools cannot retrieve it. Moreover, sometimes only the evidence that a user talked to a certain contact or even had him on his contact list may already be enough to advance the criminal investigation. The event log files generated by WhatsApp store this type of information but are still unexplored by traditional mobile forensic tools.

WhatsApp log files store two types of information that mobile forensic tools do not explore. The first is data deleted by the user that the tools can no longer recover. The second is the information that WhatsApp does not save in its databases but stores in the events log file. Thus, this study developed a software tool to extract relevant information from the WhatsApp event log files to assist investigators in elucidating crimes.

The WhatsApp for Android™ saves very verbose event log files in the folder "/data/data/com.whatsapp/files/log." These files store a detailed timeline of events related to the app, such as app activation date, connections to networks, contact synchronization, sent and received messages, deleted conversations, blocked contacts, exchange of encryption keys, user status, battery status, available memory on the device, and sound notifications, among many other types of events. These event log files can only be accessed with root permission on Android™ or by getting a physical image of the device memory. This fact, although it may seem like a problem, is an advantage, as it does not allow the ordinary user to delete them.

To find relevant data from these event log files for forensic use, experiments were conducted using an Android™ mobile device with root access and the WhatsApp version 2.18.191 installed, simulating various activities with the app and getting the corresponding events saved to the log file. Every event stored in the log file holds the date and time of occurrence, followed by information about the event. The content of the exchanged messages, for instance, is not stored, but the identification of the WhatsApp users involved in this activity is available, similar to many other cases.

The developed software, WAEventsLogParser, is free and can generate a detailed or grouped report containing the events found. Several events identified in this study are already configured in WAEventsLogParser and users can easily add more.

Aspects related to the use, distribution, and features of the software, as well as future development and strategies to identify the events, will be discussed in this presentation.

Reference(s):

1. *Most Popular Global Mobile Messenger Apps as of July 2018, Based on Number of Monthly Active Users (in Millions).* Statista, The Statistics Portal, July 2018, https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.
2. *Number of Monthly Active Whatsapp Users Worldwide From April 2013 to December 2017 (in Millions).* Statista, The Statistics Portal, January 2018, https://www.statista.com/statistics/260819/number-of-monthly-active-WhatsApp-users/.
3. *Share of Population in Selected Countries Who Are Active WhatsApp Users as of 3rd Quarter 2017.* Statista, The Statistics Portal, January 2018, https://www.statista.com/statistics/291540/mobile-internet-user-WhatsApp.
4. WhatsApp. *WhatsApp Encryption Overview*. Technical White Paper, December 19, 2017.

WhatsApp, Events Log File, Mobile Forensics