Master Thesis

In order to obtain the

Professional Master 2
In
MDFS option: Forensic Science

Presented and defended by:

Louaye Lamaa

On Monday July 22, 2019

Forensic Analysis of WhatsApp SQLite Databases on the Unrooted Android Phones

---

Supervisor:
Dr. Hasan Kazan

Reviewers:
Colonel Albert Khoury
Major Hany Kallassy

Lebanese University - Faculty of Sciences

Acknowledgements

This thesis would not have been achievable without the support and assistance from many people. I would like to thank all of them for being part of this journey and making this thesis possible.

I would like first to express my deepest gratitude to my supervisor Dr. Hasan Kazan for his guidance, patience, and support of my study.

I would like to thank the members of the committee for offering their time to read my thesis and for being able to attend my presentation. I honestly appreciate it.

Finally, I would like to recognize the biggest support that came from my family. I am deeply thankful for their love, sacrifices, and encouragement.

Abstract

WhatsApp is the most popular instant messaging mobile application all over the world. Originally designed for simple and fast communication, its privacy features, such as end-to-end encryption, eased private and unobserved communication for criminals aiming to commit illegal acts.

In this paper, we present the forensic analysis of the artifacts left by the encrypted WhatsApp SQLite databases on the unrooted Android devices.

In order to provide a complete interpretation of the artifacts, we perform a set of controlled experiments to generate them. Once generated, we identify their storage location and databases structure on the device. Since the data is stored in an encrypted SQLite database, we first discuss its decryption. Then, we show how to analyze the artifacts and how they can be correlated to cover all the possible evidence.

The results show how to reconstruct the list of contacts, the history of exchanged textual and non-textual messages as well as the details of their contents. Furthermore, this paper shows how to determine the properties of both the broadcast and the group communications in which the user has been involved as well as of the feature called status. Finally, we show how to reconstruct the logs of the voice and video calls.

These results show that the recontrcution of the WhatsApp data from the SQLite databases is possible and this data persists on the phone even after the uninstallation of WhatsApp.

Keywords: Mobile forensics, WhatsApp messenger, Instant messaging, Android, Unrooted devices, Data recovery, SQLite databases.

Contents

List of Figures

List of Tables