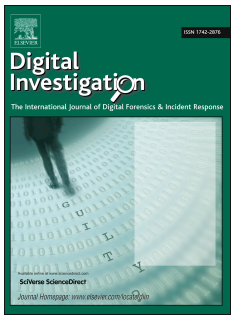
Accepted Manuscript



Forensic analysis of Telegram Messenger on Android smartphones

Cosimo Anglano, Massimo Canonico, Marco Guazzone

PII: S1742-2876(17)30176-7

DOI: 10.1016/j.diin.2017.09.002

Reference: DIIN 708

To appear in: *Digital Investigation*

Received Date: 29 May 2017

Revised Date: 11 September 2017

Accepted Date: 12 September 2017

Please cite this article as: Anglano C, Canonico M, Guazzone M, Forensic analysis of Telegram Messenger on Android smartphones, *Digital Investigation* (2017), doi: 10.1016/j.diin.2017.09.002.

Forensic Analysis of Telegram Messenger on Android Smartphones

Cosimo Anglano[a,*], Massimo Canonico[a], Marco Guazzone[a]

[a] *DiSIT - Computer Science Institute, Università del Piemonte Orientale, Alessandria (Italy)*

Abstract

In this paper we present a methodology for the forensic analysis of the artifacts generated on Android smartphones by *Telegram Messenger*, the official client for the Telegram instant messaging platform, which provides various forms of secure individual and group communication, by means of which both textual and non-textual messages can be exchanged among users, as well as voice calls.

Our methodology is based on the design of a set of experiments suitable to elicit the generation of artifacts and their retention on the device storage, and on the use of virtualized smartphones to ensure the generality of the results and the full repeatability of the experiments, so that our findings can be reproduced and validated by a third-party.

In this paper we show that, by using the proposed methodology, we are able (a) to identify all the artifacts generated by Telegram Messenger, (b) to decode and interpret each one of them, and (c) to correlate them in order to infer various types of information that cannot be obtained by considering each one of them in isolation.

As a result, in this paper we show how to reconstruct the list of contacts, the chronology and contents of the messages that have been exchanged by users, as well as the contents of files that have been sent or received. Furthermore, we show how to determine significant properties of the various chats,

*Corresponding author. Address: viale T. Michel 11, 15121 Alessandria (Italy). Phone: +39 0131 360188.

Email addresses: cosimo.anglano@uniupo.it (Cosimo Anglano), massimo.canonico@uniupo.it (Massimo Canonico), marco.guazzone@uniupo.it (Marco Guazzone)