CRIMSON PUBLISHERS
Wings to the Research

Forensic Science & Addiction Research

ISSN 2578-0042

Mini Review

The Evolution of Instant Messaging Applications from a Forensic Perspective

J Gregorio*, B Alarcos and A Gardel

University of Alcalá, Spain

***Corresponding author:** J Gregorio, University Institute of Research in Police Sciences, University of Alcalá, Spain, Tel: +34 918856585; Email: jesus.gregorio@edu.uah.es

Submission: March 19, 2018; **Published:** March 27, 2018

Introduction

The facilities offered by the evolution of new information technologies leads that people desire (and many times, desperately need) to be increasingly interconnected to the Internet, exchanging information with other people anywhere and anytime. Currently, most people make extensive use of mobile devices with hardware and software capabilities similar to those of a computer, which added to the greater coverage of telephone operators and better speed in data networks, provide the user with permanent connection availability. At the same time, the software companies have developed a huge number of applications in different fields such as communication, appointments, finances, news, social networks, geo-location, that are used to transfer and share information which will be important from the forensic perspective. We focus our attention on the so called Instant Messaging (IM) applications such as whatsApp, Signal, Telegram, etc.

More and more, these IM applications use cloud-based services, offering their users total availability to their communications regardless of the device used. Nowadays, users access their data from anywhere since the information (sometimes a copy) is stored on remote servers. In this way, IM applications provide the user with different ways of connecting to their communications, either from an application installed on a Smartphone (mobile-client), from an application installed on a computer (desktop-client) or even from a web browser (web-client).

From a forensic perspective, the evolution of messaging application models has led to an evolution in the methods for obtaining the information subject to forensic analysis of messaging applications. The studies carried out on different models of IM applications (mobile-client, desktop-client, and web-client) show that the forensic methodology for the acquisition and analysis of artifacts requires several changes in order to obtain more details of information related to a user's communications.

Current Forensic Analysis of IM Applications Data

The result of forensic analysis of the artifacts generated by an IM application will depend to a large extent on the amount of information analyzed and therefore on the method of acquisition.

We can enumerate up to 4 different forensic methods to acquire the digital evidences for later processing of the information

a. Logic: This method obtains a copy of the information as it would have been shown in the original device. In the case of IM applications, the logical acquisition will get the information related to the conversations (personal chat, group chat, etc.) or contacts. The logical acquisition can be done using backup copy software ("Smart Switch", "iTunes", etc.) or forensic software ("Cellebrite", "MOBILedit", etc.).

b. File system: Through this method, a copy of the file system containing the digital evidence is obtained.

c. Physical: This acquisition method provides a complete bit-image copy of the mass storage system of the digital evidence. These latter two methods, in addition to providing access to data files or databases containing IM application conversations, allow for more detailed forensic analysis and data retrieval of the different records generated by these types of applications. There are different software/hardware tools (bootloaders, rooted, jailbreak, security failures, flash boxes, commercial forensic tools, etc.) as well as other more invasive techniques (JTAG and Chip-off) that are used for this type of acquisition.

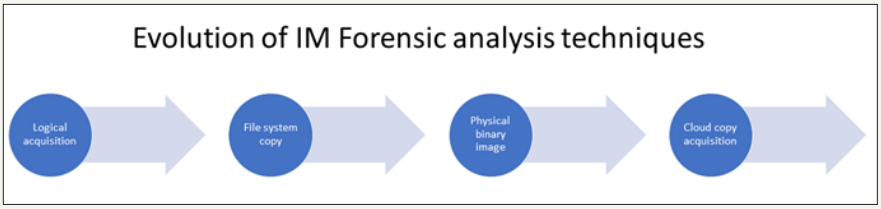

Figure 1: Evolution of IM forensic analysis techniques.

d. Cloud: This method of acquisition retrieves a copy of the user information contained in the cloud using the user's credentials (Figure 1).

The first three acquisition methods (logic, file system and physical) are well known and profusely used in the forensic community to obtain information from the different mobile-client IM applications. There are several commercial forensic tools ("Cellebrite", "MSAB", "Oxygen Forensics", etc.), which provide comprehensive solutions for both the acquisition of the information contained in the evidence and automated forensic analysis of the information.

Desktop-client and web-client models of IM application have special features that make forensic data acquisition and analysis completely different from that performed on a mobile-client model. For example, encryption capabilities are not usually included in the mobile applications due to the lower computing power. On the other hand, the location of user data mobile devices represents important information.

Studies on different desktop-client and web-client based IM applications, using different specialized commercial tools ("EnCase", "X-Ways", "Internet Evidence Finder", "Belkasoft", etc.) and free tools ("NirSoft", "MiTeC", etc), conclude that from the static analysis of the artifacts generated by these versions on a digital device, little information is obtained, and records of the user's conversations are rarely obtained. Therefore, it is necessary to extend the acquisition methods and proceed to obtain the user information stored in the cloud.

In many cases, the forensic specialist can obtain desktop-client or web-client conversations by emulating the original digital device, using commercial forensic software ("Perlustro", "Forensics Explorer", etc.) which combine the classic methods of information acquisition (copy, image or forensic cloning) with virtualization tools. Currently, different commercial forensic tools ("UFED Cloud Analyzer" by Cellebrite, "Cloud Data Extraction" by Oxygen Forensics, etc.) are aware of the limitations of static forensic analysis of artifacts in these clients, so they are developing solutions for retrieving the information hosted in the cloud through access via user tokens or credentials.

Conclusion

Nowadays, at forensic level, the study of the mobile-client version is quite addressed by multiple forensic tools. Concerning the desktop-client and web-client versions, their special characteristics (encryption, location, volatility of information, etc.) make it difficult to carry out a static analysis of artifacts contained inside the founded digital devices, and there are often few records related with the application, its usage or user personal data. This means that the forensic technician requires other methods of obtaining information from the IM applications, either emulating the original digital device environment or using specialized commercial forensic tools that logically acquire the information stored in the cloud through the user's credentials.