The Partial Digital Evidence Disclosure in Respect to the Instant Messaging Embedded in Viber Application Regarding an Android Smart Phone

Hai-Cheng Chu1, Szu-Wei Yang2, Shiuh-Jeng Wang3, and Jong Hyuk Park4,*

1 Department of International Business, National Taichung University of Education, 140 Min-Shen Road, Taichung 40306 Taiwan ROC
2 Department of Education, National Taichung University of Education, 140 Min-Shen Road, Taichung 40306 Taiwan ROC
3 Department of Information Management, Central Police University, 56 Shujen Road, Kueishan Hsiang, Taoyuan 33304 Taiwan ROC
4 Department of Computer Science and Engineering, Seoul National University of Science and Technology, 172 Gongneung-dong 2, Nowon-gu 139743, Korea
hcchu@mail.ntcu.edu.tw, sjwang@mail.ntcu.edu.tw, swyang@mail.cpu.edu.tw, parkjonghyukl@hotmail.com

Abstract. As Android Operating System (OS) for smart phones become pervasive, more and more end users are taking advantage of the contemporary Instant Messaging (IM) tools with high availability and agile mobility. Unfortunately, the cyber criminals or hacktivists are abusing this state-of-the-art mobile communication gadget to fulfill illegal conspiracies. The content with regard to the IM is a critical success factor in cracking some complicated cyber crime cases in a timely manner. The paper significantly contributes to the research arena of Digital Forensics (DF) practitioners and researchers respecting partial digital evidence disclosure in a generic Viber session in Android mobile OS due to the commonness of IM under contemporary ubiquitous on-demand computing infrastructures. Being accumulated with sophisticated researches both in Android smart phones and the Viber Application Program (AP), this paper is capable of utilizing some specific search string in regard to the image of the Random Access Memory (RAM) in order to disclose the digital breadcrumb in terms of the received IM and the cellular phone number in previous Viber sessions as probative evidenced in a court of law.

Keywords: Viber application program, Android smart phone, instant messaging, digital evidence, non-volatile memory.

1 Introduction

Nowadays, with the rapid progress of unparallel disruption technology, IM has become one of the contemporary communication channels in today’s ubiquitous
mobile computing communities. New models of smart phones with rapid phase of updated firmware and OS overwhelming with affordable competitive prices stimulate the massive applications for communications from business arenas to entertainment perspectives. Regrettably and unarguably, the smart phones have been participated in certain cyber crimes incidents or cyber terrorist conspiracies. Demonstrably, the acquisition of probative digital evidences is an imminent and indispensible task for law enforcement agencies in order to hinder the metamorphic cyber crimes on a daily basis. The RAM of the mobile computing devices contains some kind of volatile data and the acquisition of it could be precious in some cases. Due to the volatility in its nature, some acquisition procedures are irreversible if it is not being properly handled especially under Windows OS platforms. Phenomenally, Android has been another big giant mobile OS for voluminous end users and the DF of Android is still in its infancy especially compared to the one under Windows. Consequently, in this paper, we target on the digital evidence collection and analysis in regard to Viber, which is a newly emerged IM AP with mushrooming growing population of users. The research tries to disclose the digital evidences concerning a generic Viber session under Android OS. Astonishingly, even after an Android smart phone has been rebooted, with the imperceptible and negligible digital trails, we are able to identify the received IM with the corresponding participant in the previous IM session. The methodology in this research could be a paradigm for law enforcement agencies or DF specialists to ponder in furtherance of the crackdown of cyber criminal conspiracies.

2 Literature Review

Substantively and unarguably, the research of Android smart phones DF is still in its infancy. Due to the diversities of smart phones from varied global manufacturers as well as the corresponding OSs, the DF of Android smart phones is more complicated than that of Windows. However, there are still some rules of thumbs methodologies that could be the generic guidelines for the associate law enforcement agencies or DF researchers [1, 2]. For Windows-based smart phones, the RAM contains some kind of volatile memory where digital evidences reside and could be vanishing forever once the power of memory is gone. Hence, the memory of structure between Windows and Android plays an important role respecting the disclosure of digital trails. The format of Android file system is Yet Another Flash File System 2 (YAFFS2) with YAFFS was developed in 2002, which was the first file system designed for NAND (Not-AND) flash memory devices. In addition, YAFFS2 was designed in 2004 in response to the availability of larger sized NAND flash devices. Phenomenally, the memory of a smart phone could be unknowingly precious and critical. The digital evidences could encompass from the call logs, IM text, and the contact list. Besides, the web surfing history, images viewed on the smart phone, identification and passwords of some web sites could be unintentionally hidden and not being disclosed.