

Digital Forensic Analysis on Window8 Style UI Instant Messenger Applications

Chanjin Lee and Mokdong Chung

Dept. of Computer Engineering, Pukyong National University, Korea
{leecj011,mdchung}@pknu.ac.kr

Abstract. The existing digital forensic research on Windows 8 Style UI applications is conducted on native applications and there is a lack of study on other 3rd party applications. Therefore, we analyze 3rd party instant messengers of Style UI and we propose a digital forensic methodology. In this paper, we identify artifacts of Viber and Line, which are popular instant messengers, and analyze them in various ways. The proposed approach is expected to help criminal investigation by efficiently and rapidly providing information about an ongoing case in court.

Keywords: Digital Forensic, Style UI, Instant Messenger, Viber, Line.

1 Introduction

Digital data, which is created and recorded on digital media, increases at an exponential rate and it often serves as evidence material in court. Digital forensics is defined as a concept of technology and procedure of collecting, examining, analyzing and preserving digital data in order to present in court [1].

Windows 8 supports PC and mobile devices that are based on SOC (System on chip). Therefore, it is possible to interwork smartphones and tablet devices, and we can use applications without a separate player in PC. Since smartphones are equipped with various sensors and communication capabilities, the data for operating PC's applications remains by synchronizing with smartphones. Especially because these traces leave the information such as application type, run time, timestamp, etc. they can be clues or evidences to understand criminal behavior patterns in the perspective of digital forensics [2].

In this paper, we check instant messengers based on Style UI, where we can find the artifacts like contacts, chat, location information, etc. and we suggest the methodology of digital forensic analysis.

Section 2 reviews related work. In Section 3, we analyze Style UI instant messengers in terms of digital forensics. Section 4 draws conclusions and discusses the directions of our future research.

2 Related Work

2.1 Research on Windows 8 Style UI Forensics

Style UI, former called Metro UI, is a user interface that is appropriate for mobile devices. The artifacts are created automatically by using operating systems and

applications. Analysis of artifacts and traces can be classified as digital forensic analysis. Therefore, when analyzing the Style UI applications, it is possible to know the user's habits, preferences, etc. and we can find the user's various private information, from mail and SNS (Social Network Service) applications, as an investigation clue. Table 1 shows the Style UI artifacts of basic applications in previous researches [3, 4]. You must have administrator permissions in order to access the contents of the listed paths in Table 1.

Table 1. Windows 8 Style UI artifacts

Artifacts	Path
App EXE	%SystemDrive%\Program Files\WindowsApps
App Short cut	%UserProfile%\AppData\Local\Microsoft\Windows\Application Shortcuts
App Package List & Setting status	%UserProfile%\AppData\Local\Packages
App internet user trace data	%UserProfile%\AppData\Local\Packages\[AppName]\AC\[Sub folders]
App storage	%SystemDrive%\ProgramData\Microsoft\Windows\AppRepository
Notification setting	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifications\Applications

2.2 Instant Messenger Forensics

As smartphones are wide spread, the number of users who use the messenger applications instead of SMS services increases rapidly. Recent instant messenger applications do not only provide the feature of sending instant messages but also multimedia transaction, file sharing etc. Therefore, it is likely to obtain useful information on a criminal investigation by analyzing the messenger.

There are further researches on smartphone instant messengers. Information was extracted and analyzed, on both Android and iOS, out of twelve messenger applications, such as Facebook Messenger, WeChat and KakaoTalk [5]. Viber and WhatsApp were analyzed on Android in more detail, as well as People, the basic application of Windows 8 [3, 6].

In the existing research, many types of messenger applications were studied, but there is a lack of study on Style UI messenger applications.

3 Forensic Analysis on Instant Messenger of Style UI

We analyze Viber and Line, which are instant messenger applications for Style UI. Viber and Line are widespread applications in the world and they provide many functions such as chat, free calls and sending images, where we can find a lot of information for criminal investigation.

Especially Viber and Line are synchronized to the account applications at first launch. Therefore, we can identify some artifacts like contacts, phone numbers, and names. They have many functions to contact other people, where we can find