Digital Investigation 17 (2016) 40–52

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Forensic analysis of Kik messenger on iOS devices

Kenneth M. Ovens*, Gordon Morison

School of Engineering & Built Environment, Glasgow Caledonian University, Cowcaddens Road, Glasgow, G4 0BA, Scotland, United Kingdom

ARTICLE INFO

Article history:
Received 4 November 2015
Received in revised form 30 March 2016
Accepted 1 April 2016
Available online 30 April 2016

Keywords:
Kik
Instant messaging
iOS
Mobile device forensics
Apple

ABSTRACT

Instant messaging applications continue to grow in popularity as a means of communicating and sharing multimedia files. The information contained within these applications can prove invaluable to law enforcement in the investigation of crimes.

Kik messenger is a recently introduced instant messaging application that has become very popular in a short period of time, especially among young users. The novelty of Kik means that there has been little forensic examination conducted on this application.

This study addresses this issue by investigating Kik messenger on Apple iOS devices. The goal was to locate and document artefacts created or modified by Kik messenger on devices installed with the latest version of iOS, as well as in iTunes backup files. Once achieved, the secondary goal was to analyse the artefacts to decode and interpret their meaning and by doing so, be able to answer the typical questions faced by forensic investigators.

A detailed description of artefacts created or modified by Kik messenger is provided. Results from experiments showed that deleted images are not only recoverable from the device, but can also be located and downloaded from Kik servers. A process to link data from multiple database tables producing accurate chat histories is explained. These outcomes can be used by law enforcement to investigate crimes and by software developers to create tools to recover evidence.

Introduction

Instant messaging is not new; in fact, it has been claimed to be older than the Internet itself (Van Vleck, 2012). The popularity of messaging applications grew in the 1990's when graphical user interfaces replaced text-based interfaces. At that time, the popular applications included AOL Instant Messenger, ICQ and Yahoo! Messenger.

What is relatively novel is the popularity they have gained on the mobile platform. Just as smartphones and tablets overtake laptops and personal computers as the most popular method of accessing the Internet, instant messaging applications are significantly gaining ground on traditional phone calls and text messaging as the favoured means of communication, especially for the younger generation (Ofcom, 2015).

There are now billions of instant messaging user accounts; currently the most popular applications include WhatsApp, Facebook Messenger, Skype, and Viber. A more recent addition to instant messaging, and one that is especially popular among younger users, is the application, Kik. Launched in 2010, Kik's user base has currently grown to over 200 million, including 40% of American youth, according to the developer's website (Kik, 2015b).

As Kik has grown in popularity, crimes that have in some way involved the application, have also increased, particularly crimes that involve bullying and child abuse (Alvarez, 2013; Federal Bureau of Investigation, 2015; Zauzmer,

* Corresponding author.
E-mail address: kenneth.ovens@gcu.ac.uk (K.M. Ovens).

http://dx.doi.org/10.1016/j.diin.2016.04.001
1742-2876/

2014). These types of crimes are not unique to Kik, but weak user identification, no age verification, as well as user's perceived anonymity, may be combining to create user behaviours that are of concern to law enforcement (Godfrey, 2013; Larson, 2015).

During registration of a new account, the user is prompted to submit a first and last name, a unique username, email address, password, and a date of birth. However, there is no requirement to link a mobile phone number and failure to verify the email address does not prohibit the user sending messages. In comparison to registering a new account with Facebook, where it is a requirement to use your real name, if email addresses are not verified, the accounts cannot continue to be used. New account registrations for WhatsApp and Viber require phone numbers to be linked and verified. While it is not too difficult for a determined person to bypass these verification steps, there is little effort required to bypass Kik's verification procedures and age restrictions. Kik states that users are required to be at least thirteen years old, as this also is not verified, it is very easy for younger users to enter a fake date of birth and begin communicating immediately (Kik, 2015c).

What will be of further concern to law enforcement, is that Kik do not store and cannot retrieve any sent or received messages (Kik, 2015a). It is therefore crucial that forensic examiners are able to obtain as much information as possible from recovered mobile devices to aid investigations. While there has been a growing body of research concerning the more established instant messaging applications, to date, there is a distinct lack of detailed forensic investigation focused on Kik messenger.

The situation prompts this study into the identification, recovery, and analysis of artefacts relating to the usage of Kik messenger. This study provides the first detailed forensic analysis of Kik on Apple iOS devices. Other platforms on which Kik can be installed (Android, Windows, Amazon) are outside the scope of this study and are left for future work. Preconditions to accessing these artefacts are that the iOS device is not password locked and the investigator has access to unencrypted backup files.

The following proposed questions, common to forensic examinations, are the focus of this study:

1. Who has the user been communicating with and when?
2. What was the content of the communications?
3. What attachments were exchanged and where can they be found?

The study was conducted using tools that are freely available to practitioners. The results were used to develop open-source software that can be used to extract and present Kik artefacts, and can likewise be used by other software developers to create more forensic tools that can accurately retrieve relevant data. It also contributes to the documentation and analysis of artefacts created by Kik messenger, benefiting law enforcement in their investigations.

The rest of this paper is structured as follows: Section Related work presents an overview of research conducted into instant messaging applications and discusses methods used to acquire data from iOS devices. Section Methodology describes the experiments undertaken to address the typical questions that would arise in a forensic investigation. Section Forensic analysis of Kik messenger reports the results and analysis of the experiments. Finally, Section Conclusions and future work draws conclusions from the study and proposes avenues for future research.

Related work

A brief summary of the research methods, limitations, and conclusions for each study has been provided.

Early instant messaging research on mobile devices focused on the popular applications of the time. Husain and Sridhar (2010) examined artefacts from three applications: AIM, Yahoo! and Google Talk. With a limited data set (two messages for each application), the authors located artefacts that could have been of evidentiary value. This was achieved by searching the backup files of an iPhone 3G which had a firmware version (later named iOS) of 2.2.1. The backup files were produced by Apple's mobile device management application, iTunes.

A more comprehensive examination of the iTunes backup data was performed by Bader and Baggili (2010), to establish what data of forensic value could be recovered. The researchers manually searched through the backup files of an iPhone 3GS installed with firmware version 3.1.2, and located various types of data using command-line tools such as *'grep'* and *'find'*. The iTunes backup files were then matched against the original files located on the iPhone. This research is useful and can be applied to studies of any application that is backed up by iTunes.

Al Mutawa et al. (2012) researched social networking applications that also offer instant messaging features, namely Facebook, MySpace, and Twitter. The devices examined were iPhone 4 (iOS 4.3.3), Android, and BlackBerry mobile phones. The methods employed for the study involved installing the social networking applications on the devices, performing common user activities, then obtaining a logical image of each device before conducting a manual analysis. For the iOS device, the researchers used the iTunes application to obtain a backup of the user files. From this, they were able to extract artefacts relating to the social networking applications.

Tso et al. (2012) also focused on examining social networking applications and chose the most popular applications at that time, Facebook Chat, Viber, Skype, WhatsApp, and Windows Live Messenger. One of the reasons stated as justification for the study was that the applications provide instant and convenient information transmission used by criminals. The researchers examined an iPhone 4 with iOS 4.3.5 installed. Again, the iTunes backup application was leveraged to acquire the relevant artefacts.

Sgaras et al. (2015) also highlighted the growing concern of instant messaging applications being used by criminals to communicate with victims or to evade detection. The researchers suggested that published studies focused mainly on Android devices, whereas iOS devices had not been extensively examined. Commercial tools, namely Cellebrites UFED (Universal Forensic Extraction Device), were used to extract and classify data from