A novel approach to the f~~F~~orensic a~~A~~cquisition and analysis of ~~Android~~ social media applications on Android

Muhammad Faheem
School of Computer Science
University College Dublin
Dublin, Ireland
muhammad.faheem@ucdconnect.ie

Darren Hayes
Seidenberg School of CSIS~~Department of Computer Science~~
Pace University, NY, USA
d~~arren.~~hayes@pace.edu

Tahar Kechadi, Nhien-An Le-Khac
School of Computer Science
University College Dublin
Dublin, Ireland
{tahar.kechadi,an.lekhac}@ucd.ie

***Abstract*— ~~The s~~Social networks ha~~s~~ves witnessed unprecedented growth in the recent years, ~~and~~ while millions of registered users are accessing it using Smartphones. ~~The s~~Social network applications (apps) on mobile devices ~~introduce~~ not only provide convenient access~~e~~ but ~~also various issues~~can also provide a wealth of information related to criminal and their illegal activities. Despite being primarily used to communicate and socialize with contacts, the multifarious and often anonymous nature of social networking websites ~~increases susceptibility to cybercrimes~~makes them attractive to criminal actors. ~~So far~~To date, a forensic acquisition and a corresponding analysis of social media apps on mobile devices, have required ~~the PC~~Windows-based forensic software tools that could not always extract all relevant evidence. ~~Hence~~Thus, in this paper we present a new investigative approach ~~with~~ using a forensics app that can be installed on a mobile device~~s~~ in ~~the~~ a forensically sound manner. This app allows the investigator to ~~collect~~ extract artefacts ~~on~~ from mobile devices. In addition, we present the results of our experiments, ~~of~~ utilizing our new approach to~~on~~ forensic~~s~~ acquisitions and analysis for many popular social networking apps, found on mobile devices, including Skype, Viber, WhatsApp, Facebook Messenger, Google ~~H~~hangout, Nimbuzz, Tango, etc. without using Root Access.

Keywords— social media ~~application~~investigations; VoIP; Forensic tools; m~~M~~obile forensics; Instant Message forensics, Android, Skype, Facebook, WhatsApp

I. INTRODUCTION

Smart devices, such as smartphones~~,~~ and tablets~~, etc.~~ have the capacity to store a broad range of information about the user, including e-mail ~~history~~, historical location information, usernames, passwords, wireless access point ~~associations~~ connections and other valuable information [1]. Today, social networking apps on smart devices offer diverse methods of communication, ~~such as~~including instant messaging, audio, video, file exchange and image sharing [n1]. However, despite being primarily used to communicate and socialize with friends, the diverse and anonymous nature of social networking websites make~~s~~ them highly vulnerable to ~~cybercrimes~~hackers and other criminals. Phishers, fraudsters, child predators, and other cyber criminals can ~~register to~~enroll in these services with fake identities, thereby hiding their malicious ~~intentions~~ intent behind ~~innocent appearing~~seemingly innocuous profiles. Social networks also encourage the publication of personal data, ~~such as~~like age, gender, habits, ~~whereabouts~~location, and schedules. The wealth of personal information uploaded to these websites makes it possible for cyber criminals to ~~manipulate~~ capture this information ~~to their advantage~~ and ~~subsequently~~ use it to commit crime~~inal acts~~ [4].

Due to the popularity of social networks, ~~criminal~~ cyber criminals started using social networking apps to communicate, either with potential victims [5] or amongst themselves to avoid ~~interception~~ law enforcement intercepting their communications [6]. ~~It becomes obvious that, due to their popularity,~~The pervasiveness of social networks means that they have the potential ~~of being biggest~~to be the most significant source of ~~forensic value~~evidence in a criminal investigations. Europol has ~~identified~~ highlighted the criminal ~~threat~~ use of ~~misused~~ social networking apps to communicate~~ions by criminals to~~and facilitate their illegal activities. ~~due to the fact~~The challenge for investigators is that it is harder to monitor and~~or~~ regulate these services [7].

~~In addition, the increased use~~The exponential growth of social networking applications on smartphones, makes these devices a goldmine for forensic investigators. Potential evidence ~~can be held~~saved on these devices ~~and~~ can recovered with the right forensics tools.

The f~~F~~orensic examination of smartphones is rather challenging. ~~So far~~To date, most of the approaches to~~of~~ extracting and analyzing artefacts from, mobile devices, are mostly Windows-based ~~on the support of PC Software such as~~tools, like XRY [ref], UFED [ref], Oxygen Forensics ~~XYGEN~~[ref] or Paraben [ref]~~, etc~~. These approaches however have several issues (@Faheem: adding issues of using PC forensic sofware vs. tool installed directly on the mobile devices). Therefore, in this paper we present a new approach to acquiring~~e~~ and analysing~~e~~ artefacts from mobile devices through the development of an app, which~~that~~ is directly installed on the device~~s~~ in the forensically sound manner. ~~We also~~Additionally, we ~~evaluate~~ tested our novel approach ~~with~~ to forensic acquisitions ~~and analysis of many~~on a number of popular social media apps ~~which~~ that provide Instant Message

Comment [DH4]: What "publication"? Perhaps you mean that "Social networks seek to harvest large amounts of personal identifiable information"

Comment [DH1]: I suggest adding more about the results in the Abstract, e.g. successfully extracted the SQLite db for Skype using the app, which contained call logs, contacts and chats in plaintext. Also, perhaps mention the significance of not having to root the device.

Comment [DH2]: Not sure if this should be a keyword

Comment [DH5]: Might want to mention Santoku (santoku-linux.com), which may be similar to your app

Comment [DH3]: ?

(IM) services. ~~They are~~We selected the most popular IM apps ~~as their~~where the total number of users ~~already exceeded~~exceeds 1.5 billion [23] [24] [26]. Our forensic tool works on all Android versions Nougat (7.1.2), Marshmallow (6.0.1), Lollipop (5.1.1), and KitKat (4.4.4). We ~~also~~ subsequently compared our ~~approach with PC forensic~~forensic tool with Windows-based software.

The ~~rest of this~~remainder of the paper is organized as follows: Section 2 is Related Work on mobile device forensics and social media application forensics. Section 3 ~~is due with~~focuses on the forensic acquisition and analysis of artefacts. ~~We discuss on experimental results i~~In Section 4 we discuss our experimental results. In Section 5 ~~is for the conclusion~~we have our concluding thoughts and provide suggestions for future work.

II. Background and Related Work

In this section we discuss ~~on related work~~existing research on ~~m~~Mobile ~~d~~Device ~~forensics~~ and ~~s~~Social ~~m~~Media forensics.

A. Mobile Device Forensics

Digital Forensics is the process of inspecting and proving computer crimes in the cyber world [8]. Mobile forensics is a part of digital forensics. Mobile forensics is the process of gathering digital evidence from a mobile device under forensically sound conditions using well-developed tools and techniques. Mobile forensics deals with the process of gathering evidence from a mobile device in forensically sound conditions using well-developed tools and techniques.

There are a number of steps involved in the ~~mobile device~~ forensically seizing and analyzing a mobile device: ~~procedure is divided into stages such as~~ preservation, acquisition, examination and analysis, and reporting [9]. Preservation is the process of seizing and securing a suspected mobile devices without modifying the ~~contents of~~ data stored on the devices. Isolation is a technique ~~of evidence~~used to preserve digital evidence~~ation~~ and ~~the three common procedures for~~there are three steps involved in isolating the mobile device from radio communications ~~are~~: activate ~~the~~ airplane mode, ~~turn off the device~~, remove the SIM card, deactivate Bluetooth and WiFi and finally, place the device in a shielded container [10]. It ~~is~~ has been proved that placing a device in a shielded container did not provide ~~a~~ complete isolation due to three factors~~s~~: shielding materials do not ensure enough attenuation, there can be leaks in the shield and a conductive shield can work as an antenna [4]. Therefore, an evidence custodian is advised to use radio isolation techniques to ensure ~~better~~ improved isolation. Acquisition is the process of retrieving digital ~~information~~ data from a mobile device and ~~peripheral equipment~~associated storage. Examination and analysis ~~apply~~ utilize forensic tools to discover potential evidence on~~f~~ ~~the~~ mobile devices ~~including hidden or obscured evidences~~. During the examination, if there are any changes in the hash values of two file system extractions, it is necessary to ~~identify the reason~~account for the changes to the files and corresponding hash values [11]. The data extraction process ~~some way or the other modifies~~can potentially modify the data [13]. The final phase of the investigation ~~of the case comes to an end with~~is ~~-~~reporting the investigator's findings ~~that maintains a record of all conclusions drawn from the previous phases~~ [9]. Most ~~of the~~ mobile forensic tools ~~are capable of generating automatic~~incorporate an investigative reporting feature. A ~~p~~Physical acquisition ~~easily ingresses images~~ of a mobile device~~s~~ ~~into another tool for reporting and permitting analysis of unused file system space while logical acquisition offers a natural and understandable reporting form of acquired information~~will include both the user data and operating system files and sometimes produce deleted files; a logical forensics image from a mobile device will display just the user data. [9].

*B. Social Media Ff*orensics

Like any mobile application, large amounts of data, associated with ~~that runs on mobile phone~~ social networkings applications, ~~activities may be~~are stored locally on smartphones. Social networking applications are an integral part of smart-phone usability and therefore scientific research is needed in order to develop an effective tool that will ~~help in~~facilitate the acquisition of social media artefacts. ~~In~~ According to a research paper entitled xxx [15], ~~authors~~ the researchers conducted a forensic analysis ~~for~~ of both Viber and WhatsApp on Android devices, using professional forensic ~~acquisition equipment~~tools to perform the ~~file system~~evidence extraction on~~f~~ the smartphones. The a~~A~~uthors also conducted work ~~towards the definition of a general~~focused on the development of a methodology for collecting data on Android devices.

The paper entitled "Guidelines for the digital forensic processing of smartphones" ~~In [14], authors give~~provides ~~guidelines on~~a comprehensive overview of ~~the digital~~ forensic ~~capabilities in~~value of smartphones, and in particular highlighted the ~~where they considered~~ Skype application as an important source of evidence [14]. ~~They~~ This paper also refers~~red~~ to VoIP applications ~~being~~ used to communicate ~~without leaving~~yet do not produce call logs ~~in the~~like a traditional telephone ~~functions of the~~call made with a smartphone~~s~~. [15].

~~Different~~ A variety of forensics tools and methodologies have been used when examining IM associated with~~in the investigations of~~ ~~s~~Social ~~n~~Networks and documented in the literature~~IM Forensics were described in~~ [16]. ~~Such~~ These tools include Wireshark for packet sniffing~~er~~, AccessData's Forensics Tool Kit (FTK) and via ~~-~~Forensics mobile forensic toolkit. ~~In~~ One group of researchers ~~[17], authors~~ used a UFED ~~for tool Forensics Acquisition and Analysis of~~to forensically acquire and analyse instant messaging and VoIP applications [17]. ~~Authors in [4] describe the use of different~~Other utilities and tools, ~~such~~ including ~~as~~ SQLite Database Browser, EnCase, Odin3, and Plist Editor, have been used by researchers ~~for forensic analysis of~~examining social networking applications on mobile devices [4].

~~The existing~~Based on our literature review, ~~has identified the issue that~~ there is no effective framework in existence ~~available in the market that will~~to extract ~~the~~ IM artefacts ~~of~~ for fourteen social media apps. To our knowledge, this framework is the only free forensic software tool that is

Formatted: Highlight

Comment [DH6]: Digital forensics is not just used for computer crimes but is used in homicides, rape, embezzlement and other traditional investigations.

Comment [DH7]: Mobile forensics is not just the examination of mobile devices but also the examination of cloud backups, cell site data, etc. I usually describe it as the examination of digital evidence that is derived from a mobile device.

Formatted: Strikethrough

Comment [DH8]: Because of encryption, investigators will never turn off a cellphone

available ~~freely~~ to law enforcement. ~~It's being tested~~Following our initial testing by law enforcement, we have been encouraged to ~~member and they have recommended rolling out this~~publish our framework ~~in there force with some improvements that will include~~to improve and contribute to the field ~~local/device~~of mobile device forensics.

III. Acquisition and Analysis of Artefacts

Currently, there is no forensic tool which could directly run on the mobile device. ~~Those that are available need the support of PC Software such as~~Most existing mobile forensics tools are Windows based, including XRY, ~~UFED~~, Oxygen~~XYGEN~~ or Paraben, etc. xx The MCFT.apk file is installed directly onto mobile phone from any external storage device or by using the Linux adb push command.

The first step is to set up an investigation environment for various mobile devices in with many popular social network apps are installed. Following the environment setup, we define a list of target artefacts where we are extending what we proposed in [n2]. The next steps are dedicated to the whole investigation itself; from the data collection to the extraction of evidence (artefacts in this case). We perform the forensic analysis on the data.

@Faheem: please highlight our approach is a postmorterm or live forensics? In addition, how can we monitor our app so that it does not change the IM's artefacts?

A. *Test Environment and Requirements*

Prior to conducting the experiments investigation environment for various mobile devices in with Skype, Viber, WhatsApp, Facebook Messenger, Google hangout, Nimbuzz, Tango, KIK, BBM, IMO, WeChat, Jus Talk, Line ,Kakao Talk are installed. No changes or alteration to OS and remained at factory default.

B. *Data Acquisition and Analysis*

As mentioned in [n2], tour objective is to identify the artefacts stored by each social network app in the file system of every seized device. We are focusing on the following questions during this analysis: (i) What data is generated and stored on the device for each of the used functionality of social network app? (ii) Where is this data stored on the file system? (iii) In what format is the data stored? (iv) How can the data be retrieved, accessed and analysed?

In terms of target atefacts used in our forensics analysis, we are extending what we proposed in [n2] including installation data, traffic data, content data, user profile data, user authentication data, contact databases, attachments/file exchange, location data. We also add more target artefacts such as …

After pushing, MCFT.apk file is installed directly onto target devices, we skip the local forensics module which is not in the scope of this paper and move to social media module. It has two function i.e. Basic social media details and Detailed Social media artefacts.

Basic social media: In this experiment, we get the basic details regarding social media installed on target phones which are below

- List of Social Media Apps Installed
- Time and date of installation
- User ID or number of social media used
- Version of social media app

Detailed Social media: After running the basic social media function it gives a clear idea of install social media apps on target device. Hence we can move toward more detailed acquisition of data of installed applications.

IV. Description of Results and Analysis

A. *Test environment*

We run our experiment of four different devices which has different version of OS. Samsung Galaxy S3(Firmware version 4.1), Samsung Galaxy S4 (Firmware version 4.4), Samsun Galaxy S6(Firmware version 6.0.1), Samsun Galaxy S7Plus (Firmware version 7.1).

Global Android version distribution as of August 2017,Android Marshmallow is the most widely used version of Android, running on 32.2% of all Android devices accessing Google Play, while Android Lollipop runs on 29.8% of devices.

This framework is flexible enough to work with all available versions but we have only tested this on only four test devices.

B. *Forensic Analysis*

Before describing artefacts for each social media app, we show an overview important artefacts can be recovered in Table I. For Justtalk, WeChat, KakaoTalk, Tango and BBM, their databases are encrypted and unable to open.

TABLE I. Artefact Extraction Analysis

Apps	Target artefacts		
	All contacts	*Call history*	*IM history*
Skype	Yes	Yes	Yes
WhatsApp	Yes	Yes	Yes
Viber	Yes	Yes	Yes

Comment [NL17]: Need more details here: how you get the information, by parsing SQLite databases, etc.?

Comment [DH9]: Santoku is a forensics tool that runs locally on an Android

Comment [DH10]: UFED is hardware and not software

Formatted: Strikethrough

Comment [DH11]: How about an introductory sententce about what MCFT.apk is?

Comment [DH12]: I am confused – is this the app that you developed?

Formatted: Highlight

Comment [NL18]: More details here on the forensic process. You should also need to clarify why we only use Logic Acquisition not Physical one as well as not using Root Access.

Comment [DH13]: What is an "investigation environment"? You may want to document what you did, e.g. The Our first step of our experimentation began with the procurement of two Android smartphones: Moto 90 & LG 8080. The next step involved the installation of the xx.apk, which we accomplished using...

Comment [DH14]: Suggest rewording with specific steps on what you exactly did

Comment [NL15]: Do you have any new target artefacts rather than what we listed? For each new target artifact, please also explain what is it, and why it's important? Please refer to my paper on VoIP forensics on how to explain a target artefacts.

Comment [NL16]: You need a small paragraph here to briefly describe the forensic module.

Apps	Target artefacts		
	All contacts	*Call history*	*IM history*
Facebook Messenger	Yes	Yes	Yes
Nimbuzz	Yes	Yes	Yes
Hangouts	Yes	Yes	Yes
Line	Yes	Yes	Yes
IMO	Yes	Yes	Yes
KIK	Yes	Yes	Yes
Justtalk	No	No	No
WeChat	No	No	No
KakaoTalk	No	No	No
Tango	No	No	No
BBM	No	No	No

In the following sections, we describe and analyse artefacts we found for popular social media apps such as Skype, WhatsApp and Viber.

C. Skype

For Skype, the following artefacts are retrieved with our approach:

a. Installation

When app is installed on device it creates a lot of file like XML, Databases, directories and other files, usually all apps create these things but few files and directories are created on app's requirements

b. Login

In this app user name and password is required when user puts user name and password app verify username and password from server and then stores flag or key to remember user login.

c. Shared_prefs

In this directory app creates many .xml file for app configuration and app settings, server configurations, api links, login links etc, there is also an xml file with same name as user's id is, where profile settings are saved.

d. app_lib directory

in this directory contains library files for app.

e. Cache directory

In this directory app stores cache files of app.

f. Databases directory

In this directory app stores skypeRingtoneDB.db database file. this db file is empty.

g. files directory

in this directory contains data directories, some directories names end up with .mdp which contains log files inside them, files, and there also created a directory with user id name inside that directory contains other setting files for profile and database file for account.

h. Files/SkypeRT directory

In this directory there contains 2 files skypert.conf file and ul.conf file

skypert.conf contain following info

node_id2=8430367394347450095

node_uuid=e966e772-4a8b-11e7-b737-af7aaa1d7eef

ui.conf containts following info

Appender.Type=0

Console.Type=0

Trigger.File.MaxSize=204800

Trigger.File.Encoding=1

Trigger.File.Encryption=1

i. Files/DataRV directory

In this directory there contains 2 files offline-storage.data and offline-storage-ecs.data

offline-storage-ecs.data is encrypted unable to open

files/kk.20101(user name) directory

this directory is create when app logged in with user name and it created with same name which one is user name and inside this directory created many filed with database.

j. Files/ shared.xml

This file is an xml file which contains info about user account connection types info connect reconnect info and reconnect secret code encrypted IP etc.

k. Files/ app.properties

This file contains properties of app like app upgrade version, log enables and local time.

files\kk.20101\media_messaging\emo_cache_v2

in this directory app stores chached emoji images.

files\kk.20101\media_messaging\media_cache_v3

in this directory app stores cached images which send by user during chat or profile pics viewed.

files\kk.20101\media_messaging\storage_db\asyncdb

in this directory there is a database file which contains few tables and one of them contains an api link.

l. config.xml XML File

in this file there are configuration settings of skype which are managing app.

m. Database Files

1.offline-storage.data: In this database tokens and keys are stored

2. offline-storage-ecs.data(Encrypted): this database is encrypted and unable to open

3. storage_db.db: This data is used for emoji where stored emojis keys and names

4. storage_db.db: this database, it holds media links which shared by users during chat or conversation

5. storage_db.db: This database file holds uri link

6. dcons.db: This database holds contacts user ids and hash keys.

7. keyval.db: This database holds client version, its SQLite database version and Schema update Type.

8. main.db: In this database contains all information about contacts, group conversation and call histories, this is the main database file of skype for communication history.

9. msn.db: In this database, it stores communication history

10. rclib.db: In this database, it stores JSON request with unique id.

11. statistics.db: In this database, it stores chat error statistics, login statistics, message statistics, connectivity statistics etc.

12. telemetry.db: In this database, it stores session keys , logged in user id etc.

D. WhatsApp

E. Viber

V. DISCUSSION

During data acquisition of social media app using MCFT we don't require root access. We were able to extract all the contacts that are stored in the social media contacts list in mobile device. We acquired call history of the social media app's that allow making VOIP calls. Any incoming and outgoing calls all were extracted with date and time stamps. We were able to see when exactly the call was made.

IM is the most important features that many social media app's users use it on daily basis. It's important to any investigation that we acquired all IM communication that has correct date and time stamp. We were able to extract all incoming and outgoing IM communication nine social media app's while five of them have encrypted database which required further research. We were also able to get date and time stamps for KIK video calls.

VI. CONCLUSION AND FUTURE WORK

In this research paper we were only focus on getting artefacts of social media apps. We were successful in retrieving contacts, chat history and call history, nine out fourteen apps while five have advance encryption lock on their databases.

In order to get those artefacts we didn't require any root access of target devices. MCFT is integral part of our Mobile Cloud Forensic Framework. Evidence collected in this phase is correlated and is part of comprehensive forensics report.

In near future we will publish the local forensics module. We are also working on finding the solution for five social media apps which has encrypted databases and deleted data in order to perform complete physical acquisition.

.

REFERENCES

[1] Ayers, Richard, "Mobile Device Forensics - Tool Testing", National Institute of Standards and Technology, pp. 1- 23, 2009.

[2] R. Lovell, "White paper: Introduction to cloud computing", ThinkGrid, 2011.

[3] W. Zhenyu, Z. Chunhong, J. Yang, and W. Hao, "Towards Cloud and Terminal Collaborative Mobile Social Network Service," in Proceedings of the 2nd IEEE International Conference on Social Computing (SocialCom), pp. 623, 2010.

[4] N .A. Mutawa, I .Baggili, A.Marrington" Forensic analysis of social networking applications on mobile devices" Digital Investigation 9 (2012) S24–S33

[5] UNODC, "Comprehensive Study on Cybercrime," 2013.)

Comment [NALK21]: : you need to add more discussion here on the artefacts you found in the previous section for Skype, WhatsApp…, if possible compare what you found with your tool and popular forensic tools such are XRY etc.

Comment [NALK22]: I'm going to rewrite this section

Comment [NALK23]: : To complete at the end

Comment [NALK19]: you add WhatsApp artefacts here with the same structure as the Skype one in the previous section.

Comment [NALK20]: : … and also for Viber

[6] McAfee, "Hackers Using IM for Cyber Crime," 2013: http://home.mcafee.com/advicecenter/?id=ad_cybercrime_huifcc. (as of Sep 2014)

[7] Europol, "Threat Assessment - Italian organised crime," 2013.

[8] Finn Ruder. "New study shows 'intent' behind mobile Internet use" Retrieved on 18 February 2012 from: http://www.prnewswire.com/news-releases/new-study-shows-intent-behind-mobile-interetuse-84016487.html, 2012.

[9] Zhu, M, "Mobile Cloud Computing: Implications to Smartphone Forensic Procedures and Methodologies", AUT University, 2011.

[10] Feng Gao, and Ying Zhang, "Analysis of WeChat on IPhone" 2nd International Symposium on Computer, Communication, Control, and Automation (3CA), pp. 278- 281, 2013

[11] Levinson, A., Stackpole, B., Johnson, D. "Third Party Application Forensics on Apple Mobile Devices" 44th Hawaii International Conference on System Sciences, pp. 1-9, 2011

[12] Mohammed I. Al-Saleh, and Yahya A. Forihat, "Skype Forensics in Android Devices" International Journal of Computer Applications, Vol. 78, No.7, pp. 38- 44, 2013

[13] A. Mahajan, M. Dahiya, and H. Sanghvi, "Forensic Analysis of Instant Messenger Applications on Android Devices," International Journal of Computer Applications, vol. 68, no. 8, pp. 38–44, 2013

[14] K. Alghafli, A. Jones, and T. Martin, "Guidelines for the digital forensic processing of smartphones," in 9th Australian Digital Forensics Conference, 2011, no. 1, pp. 1–8.

[15] T. Vidas, C. Zhang, and N. Christin, "Toward a general collection methodology for Android devices," Digital Investigation, vol. 8, pp. S14–S24, Aug. 2011

[16] N B. Al Barghuthi1 and Huwida Said" Social Networks IM Forensics: Encryption Analysis" Journal of Communications Vol. 8, No. 11, November 2013

[17] W. Daniel, I. Baggili,A. Marrington" Network and device forensic analysis of Android social-messaging applications" Digital Investigation S4(2015)

[18]

End of the Sample Work