ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/312151606

Forensics Analysis of Android Mobile VoIP Apps

Chapter · October 2016

DOI: 10.1016/B978-0-12-805303-4.00002-2

CITATIONS
6

READS
519

3 authors:

Tooska Dargahi
University of Salford, Greater Manchester, UK
31 PUBLICATIONS **200** CITATIONS
SEE PROFILE

Ali Dehghantanha
University of Guelph
143 PUBLICATIONS **1,456** CITATIONS
SEE PROFILE

Mauro Conti
University of Padova
319 PUBLICATIONS **4,845** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project BEBA - BEhavioural BAsed Forwarding View project

Project DroidAnalyst View project

All content following this page was uploaded by Tooska Dargahi on 05 July 2017.

The user has requested enhancement of the downloaded file.

https://t.me/learningnets

This is authors accepted copy, for final version of the paper please refer to: Tooska Dargahi, Ali Dehghantanha, Mauro Conti, "Forensics Analysis of Android Mobile VoIP Apps", Pages 7-20, Chapter 2, (Elsevier) Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications, 2017. DOI: 0.1016/B978-0-12-805303-4.00002-2

Forensics Analysis of Android Mobile VoIP Apps

Tooska Dargahi[a], Ali Dehghantanha[b] , and Mauro Conti[c]

[a] *Department of Computer Engineering, West Tehran Branch, Islamic Azad University, Iran*; [b] *The School of Computing, Science & Engineering, University of Salford, United Kingdom*; [c] *Department of Mathematics, University of Padua, Italy*

Abstract

Voice over Internet Protocol (VoIP) applications (apps) provide convenient and low cost means for users to communicate and share information with each other in real-time. Day by day, the popularity of such apps is increasing, and people produce and share a huge amount of data, including their personal and sensitive information. This might lead to several privacy issues, such as revealing user contacts, private messages or personal photos. Therefore, having an up-to-date forensic understanding of these apps is necessary.

This chapter presents analysis of forensically valuable remnants of three popular Mobile VoIP (mVoIP) apps on Google Play store, namely: *Viber*, *Skype*, and *WhatsApp Messenger*, in order to figure out to what extent these apps reveal forensically valuable information about the users activities. We performed a thorough investigative study of these three mVoIP apps on smartphone devices. Our experimental results show that several artefacts, such as messages, contact details, phone numbers, images, and video files, are recoverable from the smartphone device that is equipped with these mVoIP apps.

Keywords: Android Forensics, mVoIP, Viber, Skype, WhatsApp Messenger, Digital Forensics

https://t.me/learningnets

1. INTRODUCTION

In the recent years, we have witnessed a rapid increase in the use of Voice over Internet Protocol (VoIP) services as an online communication method on mobile devices. This is not surprising due to the increasing penetration of smartphones: it has been predicted that by 2019 the number of smartphone users will be more than 2.6 billion [1]. These days, people use their smartphone devices not only for making voice calls and exchanging SMS, but also for obtaining several services which are offered due to ubiquitous access to Internet, such as mobile banking, and location-based services. Meantime, the use of VoIP applications, which could be delivered easily through mobile VoIP applications (mVoIP apps), would enable people to interact, share information, and to become socialized at a very low cost compared to most of the traditional communication techniques. However, such applications could also be exploited by criminals or be targeted by cybercriminals (e.g., with malware infection to steal financial data) [2, 3]. For these reasons, mobile devices (including smartphones) attracted a lot of attention from the security research community [4], in particular from the perspective of malware [5, 6, 7, 8, 9, 10, 11, 12], security enforcement [13, 14, 15, 16], and authentication mechanisms [17, 18, 19].

Smartphones are a common source of evidence in both criminal investigations and civil litigations [20, 21, 22, 23, 24, 25]. However, the constant evolution and nature (e.g., closed source operating system and diverse range of proprietary hardware) of mobile devices and mobile apps complicates forensic investigations [26]. Among the existing smartphone operating systems in the market, *Android* dominated the market with more than 80% of the total market share in 2015 Q2 [27, 28]. Therefore, Android popularity attracted several researchers to focus on investigating several different security aspects of Android, ranging from user identification [29, 30], feasibility of encryption methods on Android [31], cloud storage apps forensics [32], and social networking apps forensics [3]. Due to the increasing use of mVoIP apps for malicious activities on different platforms including Android, forensic investigation of such apps needs an extensive

https://t.me/learningnets

coverage [33, 34], and therefore in this chapter, we provide an investigative study of the three popular VoIP apps for Android on Google Play (see Table 1), namely: *Viber* [35], *Skype* [36], and *WhatsApp* [37]. The features of these VoIP apps are summarized in Table 2. In particular, we aim to answer the following question: "What artifacts of forensic value can be recovered from the use of Viber, Skype, and WhatsApp Android apps?".

Table 1: Number of installations for each application [35, 36, 37].

Application	**Number of Google Play Downloads and Installations as of March-2016**
Viber	100,000,000 - 500,000,000
Skype	500,000,000 - 1,000,000,000
WhatsApp	1,000,000,000 - 5,000,000,000

Table 2: Features of mVoIP applications.

Features	**Viber**	**Skype**	**WhatsApp**
Text-chat	✓	✓	✓
Send and Receive Image	✓	✓	✓
Send and Receive Video	✓	✓	✓
Send and Receive Audio	✓	✓	✓
Incoming and Outgoing Calls	✓	✓	✓
Group Call		✓	
Group Chat	✓	✓	✓
V-Card and Contact Sharing			✓

2. RELATED WORK

These days, several trusted and untrusted providers lunch various category of applications for mobile devices. This has lead to the ever increasing trend in using mobile devices in order to benefit from the services offered by these applications. This tendency motivated the forensic community to concentrate on forensic investigation of the mobile devices. In this regard, Dezfoli et al. [26]

https://t.me/learningnets

perused the future trends in digital investigation and determined that mobile phone forensics is receiving more and more attention by the community and is one of the fastest growing fields. In [38], the authors provided a comprehensive discussion on the nature of digital evidence on mobile devices, along with a complete guide on forensic techniques to handle, preserve, extract and analyze evidence from mobile devices. Moreover, they presented examples of commercial forensic tools that can be used to obtain data from mobile phones, such as Access Data Forensic Toolkit (FTK), Cellebrite Physical, XACT, along with use case example of the adopted Digital Forensic Framework (DDF) plug-in. In the same line of study, Mohtasebi and Dehghantanha [39] presented a unified framework for investigation of different types of smartphone devices. Parvez et al. [40] proposed a forensics framework for investigation of Samsung Phones. Several researchers have proposed various frameworks for the investigation of Nokia mobile devices and Firefox OS [41, 25].

A comparison of forensic evidence recovery techniques for a Windows Mobile smartphone demonstrates that there are different techniques to acquire and decode information of potential forensic interest from a Windows Mobile smartphone [42]. Furthermore, forensic examination of the Windows Mobile device database (the `pim.vol`) file confirmed that `pim.vol` contains information related to contacts, call history, speed-dial settings, appointments, and tasks [43]. Moreover, in [44], the authors provided a number of possible methods of acquiring and examining data on Windows Mobile devices, as well as the locations of potentially useful data, such as text messages, multimedia, e-mail, Web browsing artefacts and Registry entries. They also used *MobileSpy* monitoring software as a case-example to highlight the importance for forensic analysis. They showed that the existence of such a malicious monitoring software on a Windows phone could be detectable on the device being investigated by forensics analyst. In another recent study, Yang et al. [45] carried out an investigative study on two popular Windows instant messaging apps, i.e., Facebook and Skype. The authors showed that several artefacts are recoverable, such as contact lists, conversations, and transferred files.

https://t.me/learningnets

A research project published in DFRWS 2010 Annual Conference discussed technical issues which are in place when capturing Android physical memory [46]. A critical review of seven years of mobile device forensics [47] demonstrated that, there are several research studies in the area of Android device forensics in the literature. However, very few of them support the varying levels of Android memory investigation. Lessard and Kessler [48] showed that it is possible to acquire a logical image of Android-based smartphones, such as Samsung Galaxy, using either a logical method or a physical method. The logical acquisition technique consists of obtaining a binary image of the device's memory, which requires root access to the device. More so, Vidas et al. [49] discussed an acquisition methodology based on overwriting the "Recovery" partition on the Android device's SD card with specialized forensic acquisition software. Likewise, Canlar et al. [21] proposed *LiveSD Forensics*, which is an on-device live data acquisition approach for Windows Mobile Devices. They proposed a method to obtain artefacts from both the Random-Access Memory (RAM) and the Electronically Erasable Programmable Read Only Memory (EEPROM). In [50], the authors proposed a methodology for collection and analysis of evidential data on Android devices, which used the principles of Martini and Choo's cloud forensics framework [51]. The steps within this methodology are as follows: the collection of the physical image of the device partitions with the aid of a live OS bootloader, and the examination of app files in private and external storage, app databases and accounts data for all apps of interest, on the android device. Using this methodology, in [52], the authors carried out an analysis of seven popular Android apps within three categories: storage (Dropbox, OneDrive, Box and ownCloud), note-taking (Evernote and OneNote) and password syncing (Universal Password Manager,UPM). Such analysis proves the validity of their proposed methodology.

In order to facilitate the forensic investigation of mobile devices that are rapidly changing in their structure, Do et al. [53] proposed a forensically sound adversary model. Azfar et al. [54] considered this adversary model as a template to map a potential adversary's capabilities and constraints, in order to evaluate

https://t.me/learningnets

the usefulness of such a model by carrying out a forensic analysis of five popular Android social apps (Twitter, POF Dating, Snapchat, Fling and Pinterest). They showed that useful artefacts are recoverable using this model, including databases, user account information, contact lists, images and profile pictures. They could also discover timestamps for notifications and tweets, as well as a Facebook authentication token string used by the apps.

There is also a vast interest of digital investigators in studying the instant messaging artefacts in the stream of research in this area of digital forensics. The first claimed work to carry out a forensic analysis of Skype on the Android platform [55] investigated both the NAND and RAM flash memories in different scenarios. Their obtained results showed that chat and call patterns can be found in both of NAND and RAM flash memories of mobile devices, regardless of whether the Skype account has been signed out, signed in or even after deleting the call history. In [34, 56], the authors showed that, whilst conducting recoveries of digital evidences relating to VoIP applications in computer systems, the Skype information is recoverable from the physical memory. Moreover, [57] presents another forensic analysis of several instant messaging applications including Skype and WhatsApp focusing on encryption algorithms used by these applications. Similar work has also been conducted by forensically analyzing WhatsApp on Android platforms [58, 59]. In the same line of study, a forensic analysis of four popular social networking applications (Facebook, Twitter, LinkedIn and Google+) have been carried out which showed that artefacts useful as evidence in a potential criminal investigation are recoverable from smartphone devices using such applications [3]. Moreover, Yang et al., suggested an approach for forensics investigation of instant messaging applications on Windows 8.1 and applied it for detecting remnants of Facebook Instant Messaging and Skype application. Another important research direction which has always been a concern for digital investigators in investigation of instant messaging applications is *privacy* [60, 61, 62]. Ntantogian et al. [63] evaluated thirteen Android mobile applications focusing on the privacy. They tried to recover artefacts that provide information relating to authentication credentials. They showed that, the users' credentials

https://t.me/learningnets

are recoverable in the majority of the applications. Moreover, they determined specific patterns for the location of such credentials within a memory dump. In another research study [64], Farden et al. explored the privacy of user data with regards to mobile apps usage by evaluating the privacy risks that are inherent when using popular *mobile dating Apps*. They showed that in almost half of the investigated applications, the chat messages are recoverable, and in some cases details of other nearby users could also be extracted. Likewise, Azfar et al. [65] provided a forensic taxonomy of Android mHealth apps, by examination of 40 popular Android mHealth apps. Their findings could potentially help facilitate forensic analysis of those particular mobile health applications.

In this paper we thoroughly analyze forensics remnants of three popular instant messaging applications namely Viber, Skype, and WhatsApp on Android platform to provide a guideline for forensics practitioners in conducting similar investigations. In compare with previous studies, this research is delving into forensically valuable evidences in the context of Android platform and provides a comparative study of different VoIP applications remnants. Moreover, it is furthering forensics attention to lesser studied Viber and WhatsApp applications forensics.

3. EXPERIMENT SETUP

Our investigative methodology is based on the digital forensic framework proposed by Martini and Choo [51]. In this study, we first identified the potential evidence sources and set up the experimental environment (Section 3.1). Thereafter, we carry out logical acquisition in order to collect evidential data (Section 3.2). Finally, by analyzing the collected data, we investigate possible remnant artefacts (Section 3.3). We further demonstrated and discussed the experimental results in Section 4, and presented the conclusions drawn from our investigation in Section 5; both of which exemplify the third and fourth steps of the framework methodology [51], i.e., 'Examination and Analysis' and 'Reporting and Presentation', in which the results of the forensic study should

https://t.me/learningnets

be analyzed and presented appropriately.

Due to the fact that without a rooting the smartphone device, we would not be able to access some of the stored files (we will explain in Subsection 3.2), we utilized a rooted Android phone, i.e., Samsung Galaxy S3 GT-i9300, in order to conduct our experiments. We set up and configured necessary workstations and tools (including both software and hardware), as listed in Table 3. Moreover, Table 4 reports the authentication methods required for our considered mVoIP applications, and their details.

Our examination and analysis process consist of three phases, which we explain in the following.

Table 3: Adopted forensic tools.

Tool	**Version**	**Details**
Android Platform Phone	Samsung S3 GT - i9300, Firmware version 3.0.31	Mobile Device used for this study
mVoIP Applications	Viber - 4.3.3 Skype - 4.9.0.45564 WhatsApp - 2.11.238	Applications that are investigated
AccessData FTK Imager	V 3.1.4.6	Used to explore the acquired logical image (internal memory) of the phone
SQLite Database Browser	2.0bl	Visual tool which is used to explore the database extracted from each application after identifying the folders using AccessData FTK Imager
Internet Evidence Finder Timeline	IEF v6.3	Provides a view of each artefact on a visual timeline without any need to convert artefacts like timestamps
Root-Kit	Frameware CF-Auto-Root- m0 m0xx-gti9300	Frameware is used to root the device
Odin3	version 3.07	Enables uploading of the root-kit frameware to the Android device
Epoch & Unix Timestamp Converter		Used to convert the timestamp found in hex format

https://t.me/learningnets

3.1. Phase I- Setup Phase – First Iteration

The first phase of our study is to identify and preserve the source of evidence, which is the first iteration. In this phase, we downloaded three mVoIP applications from the Google Play Store and installed on a Samsung Galaxy S3 GT-i9300 smartphone. For WhatsApp and Viber applications, an active mobile SIM is required to activate the application, while Skype could be activated by the username and password of the registered account (see Table 4). For each application, we performed several activities, as described in Table 5, continuously for one month before the logical acquisition.

Table 4: Application details and authentication methods on the supported Android 4.3 Platform.

mVoIP Applications	**Size**	**Version**	**Authentication Method**
Viber	20 MB	4.3.3	Mobile phone number (e.g. +1 xxxxxx)
Skype	15 MB	4.9.0.45564	Username and password
WhatsApp	15 MB	2.11.238	Mobile phone number (e.g. +1 xxxxxx)

Table 5: Performed activities using the mVoIP applications.

Features	**Viber**	**Skype**	**WhatsApp**
Text-chat	✓	✓	✓
Send Image	✓	✓	✓
Receive Image	✓	✓	✓
Send Video	✓	✓	✓
Receive Video	✓	✓	✓
Send Audio	✓	✓	✓
Receive Audio	✓	✓	✓

3.2. Phase II - Logical Acquisition

The smartphone device that we used for the experiments, i.e., Samsung Galaxy S3 GT-i9300 Firmware version 3.0.31, was originally not rooted. However,

https://t.me/learningnets

without a root access on the phone, many data files would be inaccessible. Therefore, we used Odin3 (version 3.07) tool [66] to root the device by uploading the rook-kit frameware (`CF-Auto-Root-m0-m0xx-gti9300`) to the device. The installed root-kit gives the user root access, i.e., the user has the privilege control over the OS, which allows the user to attain privileged control within the Android's sub-system, and bypass the limitation placed on the device by the manufacturer. The root access grants the user the privilege to access a certain protected directory that holds some of the artefacts needed for this experiment (e.g., `[root]/data/directories`). The needed directory is then backed up and later accessed with the use of other tools mentioned earlier (see Table 3). The procedure that we adopted in our data acquisition is forensically sound according to [49]; however, there are other methods to acquire logical image on Android devices without having to root the device. After rooting the phone, the bit-by-bit physical acquisition of `dd` image is acquired using the following SSH command: `'sshroot@(Device IP Address) dd if=/dev/block/mmcblk0p12 | of=(Location on your computer)`. The "`mmcblk0p12`" (which might be different in several devices) is the internal memory block of the Android device, which is 16GB and so, it takes hours to be fully acquired.

This phase of the experiments leads to acquisition of the logical image of the Android device, which is considered to be the most crucial phase in mobile forensics investigation process, as the generated hash values play a vital role when presenting the case in court of law [67].

3.3. Phase III - Identification and Analysis – Second Iteration

This third phase of the experiment includes identification of folders and files on the logical image acquired in the previous phase. Examination and analysis of the files in order to check the existence of artefacts such as time-stamps, location, GPS coordination, contact info, text-chat, SMS, file location and any significant data that could be relevant to the research area. We conducted forensic examinations manually, with the aid of the tools listed in the Table 3. After acquiring the logical image, as described in Phase II, we used "AccessData

https://t.me/learningnets

FTK Imager" to analyze the acquired `dd` image which resulted in the creation of the directory default path. This allows us to access all the files in each directory, and therefore navigating to each one of the files. Figure 1 shows the three folders of the our three under investigation applications, Viber, Skype, and WhatsApp Messenger. After identifying these folders, in the next step, we need to carry out a deep inspection on each application's database to know whether we can find any potential evidentiary artefact.

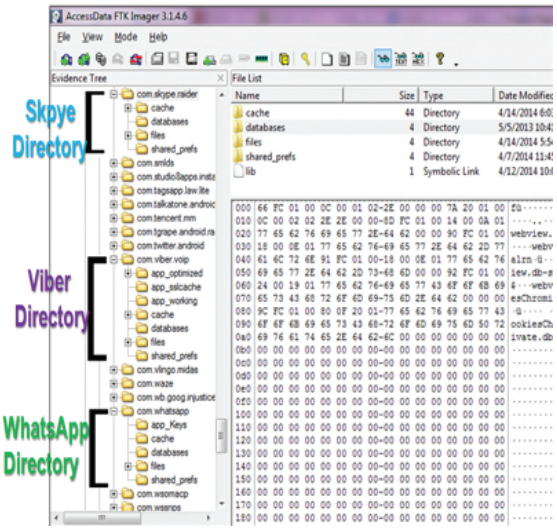

Figure 1: Folder directory of all the applications in the devices.

4. RESULTS AND DISCUSSION

This section describes the potential artefacts found in each mVoIP application's directory. Furthermore, we discuss the evidentiary values of the artefacts found for each of the mVoIP applications.

4.1. Viber Artefacts

This subsection describes the Viber artefacts found in both manual forensic analysis and using IEF tool. We found two unique database directories after examining `dd` image with the FTK imager for Viber application, which are:

https://t.me/learningnets

- [*root*]/data/com.viber.voip/databases/viber_ data.db
- [*root*]/data/com.viber.voip/databases/viber_ messages.db

The Viber application has two databases: viber_ data.db, which contains the same information as wa.db in WhatsApp; and viber_ messages.db, which has the same information as msgstore.db in WhatsApp application. Once again, using rooted device enabled us to access the database information in plaintext format. The viber_ data.db file contains data related to the outgoing calls, Viber contact names and numbers. In this experiment, we considered no blocked numbers; however, in case of having some block numbers, they would be recoverable as well. All these potential artefacts have evidentiary value relevant to a forensic investigation. On the other hand, the viber_ messages.db file stores geographical location information, contacts and all the sent or received messages in a chat database. Through preforming a forensic examination on this database, one would be able to determine the message exchange and also the actual source and destination of each exchanged message. With the aid of the IEF forensic tool, it is possible to determine whether a particular message was either sent or received by a particular sender or a recipient. These artefacts are useful in helping a forensic investigator to determine if a particular suspect is worth taking to court.

4.2. Skype Artefacts

In order to examine the Skype application, after obtaining the dd image in the same way as Viber and WhatsApp, we used the IEF tool. We discovered that, Skype stores information in an SQLite database called main.db, and the file directory is: [root]/data/com.skype.raider/files/SkypeID/main.db, in which the "SkypeID" indicates a particular user account. The database contains information about a user's account such as messages, calls, group chat, voicemails, contacts, SMS messages and file transfers. We analyzed the main.db with the SQLite viewer. The timestamp was in Unix epoch time but later converted using the converting tool. Recoverable artefacts from the Skype contact lists

https://t.me/learningnets

include the Skype name, full name, birthday, gender, country, mobile number, email address and registered date timestamp. Text-chat artefacts include the text message, message type, status, chat ID and recipient ID. The call related artefacts that could be recovered are: the local user details, remote user details, call duration and whether the call was incoming or outgoing. The artefacts related to file transfer that we could recover are: timestamp, file size(bytes) and status. Voicemail related artefacts include: the caller's ID, voicemail size and status. Finally, IP location related artefacts included the userID, IP Address, and timestamp.

Most people actually believe that by physically deleting or clearing chat histories, the Skype logs will be deleted, and the data associated with a particular account cannot be recovered. In mobile devices, evidential data that contains such recoverable artefacts can prove fruitful and provide a rich source of evidence for investigating crimes related to Skype. The artefacts showing an incoming and an outgoing call have timestamps which are also captured along with the call duration. With such evidence, a suspect cannot deny initiating or engaging in such a call. This would give forensic examiners a stronger convincing power in the court of law when handling a case. Moreover, it is possible to recover full contact details of the Skype owner, i.e., full name, date of birth, phone number(if any), date of Skype creation, and email; this makes it easy for the suspect in question to be tracked down. The IP address reflects the "externally visible" IP address of the device where Skype is running, i.e., the IP address of the outermost NAT gateway connecting the device to the Internet. The IP address plays a significant role in terms of determining the geographical location of parties involved in the crime. This artefact can be useful for attribution as it indicates the IP address that the device used to connect to the Internet. This may help tie a subject to a particular IP address and activity originating from that address. Having found artefacts like name, email, mobile number, date of birth, gender and country, it would be easy for a forensic investigator to further carry out the investigation based on what has been found and also to geographically point to where the relevant subjects reside.

https://t.me/learningnets

4.3. WhatsApp Artefacts

In this subsection, we describe the WhatsApp Messenger artefacts that we found in this investigation. In fact, by examining the `dd` image with the FTK imager tool, we found out three unique directories: two of them are databases, while one is a directory path.

- [*root*]`/data/com.whatsapp/files/Avatars/60xxxx@s.whatsapp.net`
- [*root*]`/data/com.whatsapp/databases/wa.db`
- [*root*]`/data/com.whatsapp/databases/msgstore.db`

We could find the avatar icon of each contact in the WhatsApp application, along with user related MD5 and SHA1 hashes which have evidentiary value, since they can be directly linked to a particular WhatsApp account, and hence can be used to identify the user who is using this account. Alongside the avatar pictures, the name and phone number of the user are also valuable to forensic specialists.

Since we used a rooted device in the experiments, the database appeared in plain text format. We discovered that, the records and logs of all the activities carried out by the user that are listed in Table 5 are stored in two different database files: `wa.db`, and `msgstore.db`. The `wa.db` file contains all the information relating to the contacts including the contact names, contact phone numbers and WhatsApp status. These artefacts can be of great value to actually track down suspects, for example, a certain WhatsApp status update may betray information relating to a criminal activity. Having these kind of artefacts, a digital forensic specialist would be able to potentially relate the status to an actual incident and back up their case accordingly. On the other hand, the `msgstore.db` contains artefacts with timestamps relating to sent and received text-chat messages, images, videos and audios. By analyzing the same database using IEF tool, we could obtain the source and the destination of each message in order to detect the actual sender and receiver of each message.

https://t.me/learningnets

We summarized the results acquired from our investigation in Table 6. Both WhatsApp Messenger and Viber share almost the same potential evidentiary artefacts, however in WhatsApp Messenger, there is neither call duration, nor GPS coordination. Skype leaves more interesting artefacts, such as both local and private IP addresses which are capable of facilitating further investigation on a particular case.

So far only a few research studies have explored and addressed the forensic recovery and analysis of activities carried out on social network and instant messaging applications on smartphones. These work provide limited information in terms of logical acquisition and artefacts recovery. In contrary, our study explored the forensic acquisition, examination and analysis of the logical image of a smartphone. Our experiment consisted of: i) installation of three top-rated mVoIP applications, ii) carrying out the usual user activities on each of these applications, followed by the acquisition of the logical image using a forensically sound approach, and iii) performing a manual forensic analysis on each of the installed mVoIP applications. When carrying out such a digital forensic examination, however, there could be some potential obstacles which could make accurate data recovery difficult. For example, there are many varieties of lock screen apps, app lock, SMS and picture locks; some of which encrypt the data stored on the mobile device, and also lock the device interface [68]. This could be an issue for a digital forensic specialist when examining such a device.

Table 6: Summary of potential found evidentiary artefacts.

	mVoIP Application		
Potential Evidentiary Artefacts	**Viber**	**Skype**	**WhatsApp**
Messages	✓	✓	✓
Contact Details	✓	✓	✓
Phone Number	✓	✓	✓
Voicemail		✓	
Email		✓	
Images, Videos, Audios	✓	✓	✓
Location Information	✓	✓	

https://t.me/learningnets

5. CONCLUSION AND FUTURE WORK

In this chapter, we carried out a forensic analysis of the most popular mVoIP applications, i.e., Viber, Skype, and WhatsApp Messenger when running on an Android smartphone. Artefacts listed in Table 6 can provide vital evidence that can open up a case or offer a wealth of information for further investigation when dealing with crime related to mobile devices and mobile applications.

This study successfully applies a methodology adapted from an existing digital forensics framework, which uses various techniques from the existing literature, in order to perform a forensic analysis of Viber, Skype, and WhatsApp Messenger applications on an Android platform. We showed that potential evidentiary artefacts can be found on Android devices, which have forensic value to be presented in the court of law by a forensic investigator when handling a case related to cyber terrorism or cybercrime conspiracies. A possible future research direction could be a comprehensive research on different mobile operating system platforms, considering another mVoIP apps. This would provide vital information for digital forensic specialists.

References

[1] [Online], Number of smartphone users worldwide from 2014 to 2019, http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (Accessed 11 March 2016) (2016).

[2] M. I. Husain, R. Sridhar, iForensics: forensic analysis of instant messaging on smart phones, in: Digital forensics and cyber crime, Springer, 2009, pp. 9–18.

[3] F. Norouzizadeh Dezfouli, A. Dehghantanha, B. Eterovic-Soric, K.-K. R. Choo, Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms, Australian Journal of Forensic Sciences (2015) 1–20.

https://t.me/learningnets

[4] A. Dehghantanha, N. I. Udzir, R. Mahmod, Towards data centric mobile security, in: Proceedings of the 7th International Conference on Information Assurance and Security, IAS'11, IEEE, 2011, pp. 62–67.

[5] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, M. Rajarajan, Android security: a survey of issues, malware penetration, and defenses, IEEE Communications Surveys & Tutorials 17 (2) (2015) 998–1022.

[6] J. Gajrani, J. Sarswat, M. Tripathi, V. Laxmi, M. Gaur, M. Conti, A robust dynamic analysis system preventing sandbox detection by Android malware, in: Proceedings of the 8th International Conference on Security of Information and Networks, SIN'15, ACM, 2015, pp. 290–295.

[7] P. Faruki, A. Bharmal, V. Laxmi, M. S. Gaur, M. Conti, M. Rajarajan, Evaluation of Android anti-malware techniques against dalvik bytecode obfuscation, in: Proceedings of the 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom'14, IEEE, 2014, pp. 414–421.

[8] P. Faruki, V. Kumar, B. Ammar, M. Gaur, V. Laxmi, M. Conti, Platform neutral sandbox for analyzing malware and resource hogger apps, in: Proceedings of the International Conference on Security and Privacy in Communication Networks, SecureComm'14, Springer, 2014, pp. 556–560.

[9] V. F. Taylor, R. Spolaor, M. Conti, I. Martinovic, Appscanner: Automatic fingerprinting of smartphone apps from encrypted network traffic, in: Proceedings of the 1st IEEE European Symposium on Security and Privacy, EuroSP'16, IEEE, 2016.

[10] K. Shaerpour, A. Dehghantanha, R. Mahmod, Trends in Android malware detection, The Journal of Digital Forensics, Security and Law 8 (3) (2013) 21.

https://t.me/learningnets

[11] M. Damshenas, A. Dehghantanha, R. Mahmoud, A survey on malware propagation, analysis, and detection, International Journal of Cyber-Security and Digital Forensics 2 (4) (2013) 10–29.

[12] M. Damshenas, A. Dehghantanha, K.-K. R. Choo, R. Mahmud, M0droid: An Android behavioral-based malware detection model, Journal of Information Privacy and Security 11 (3) (2015) 141–157.

[13] Y. Zhauniarovich, G. Russello, M. Conti, B. Crispo, E. Fernandes, MOSES: supporting and enforcing security profiles on smartphones, IEEE Transactions on Dependable and Secure Computing 11 (3) (2014) 211–223.

[14] M. Conti, N. Dragoni, S. Gottardo, MITHYS: Mind the hand you shake-protecting mobile devices from ssl usage vulnerabilities, in: Security and Trust Management, Springer, 2013, pp. 65–81.

[15] M. Conti, B. Crispo, E. Fernandes, Y. Zhauniarovich, Crêpe: A system for enforcing fine-grained context-related policies on Android, IEEE Transactions on Information Forensics and Security 7 (5) (2012) 1426–1438.

[16] T. Dargahi, M. Ambrosin, M. Conti, N.Asokan, ABAKA: a novel attribute-based k-anonymous collaborative solution for LBSs, Computer Communications(to appear).

[17] C. Giuffrida, K. Majdanik, M. Conti, H. Bos, I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics, in: Proceedings of the 11th Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA'14, Springer, 2014, pp. 92–111.

[18] M. Conti, I. Zachia-Zlatea, B. Crispo, Mind how you answer me!: transparently authenticating the user of a smartphone when answering or placing a call, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, SIGSAC ASIACCS'11, ACM, 2011, pp. 249–259.

https://t.me/learningnets

[19] V.-D. Stanciu, R. Spolaor, M. Conti, C. Giuffrida, On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks, in: Proceedings of the 6th ACM Conference on Data and Application Security and Privacy, SIGSAC CODASPY'16, ACM, 2016.

[20] H.-C. Chu, S.-W. Yang, S.-J. Wang, J. H. Park, The partial digital evidence disclosure in respect to the instant messaging embedded in viber application regarding an android smart phone, in: Information Technology Convergence, Secure and Trust Computing, and Data Management, Springer, 2012, pp. 171–178.

[21] E. S. Canlar, M. Conti, B. Crispo, R. Di Pietro, Windows mobile LiveSD forensics, Journal of Network and Computer Applications 36 (2) (2013) 677–684.

[22] M. N. Yusoff, R. Mahmod, A. Dehghantanha, M. T. Abdullah, An approach for forensic investigation in Firefox OS, in: Proceedings of the Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec'14, IEEE, 2014, pp. 22–26.

[23] M. N. Yusoff, R. Mahmod, M. T. Abdullah, A. Dehghantanha, Mobile forensic data acquisition in Firefox OS, in: Proceedings of the Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec'14, IEEE, 2014, pp. 27–31.

[24] M. Damshenas, A. Dehghantanha, R. Mahmoud, A survey on digital forensics trends, International Journal of Cyber-Security and Digital Forensics 3 (4) (2014) 209–235.

[25] M. N. Yusoff, R. Mahmod, M. T. Abdullah, A. Dehghantanha, Performance measurement for mobile forensic data acquisition in Firefox OS, International Journal of Cyber-Security and Digital Forensics 3 (3) (2014) 130–140.

[26] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani,

https://t.me/learningnets

F. Daryabar, Digital forensic trends and future, International Journal of Cyber-Security and Digital Forensics 2 (2) (2013) 48–76.

[27] IDC, Smartphone OS market share, 2015 Q2, http://www.idc.com/prodserv/smartphone-os-market-share.jsp (Accessed 11 March 2016) (2015).

[28] Gartner, Gartner says emerging markets drove worldwide smartphone sales to 15.5 percent growth in third quarter of 2015, http://www.gartner.com/newsroom/id/3169417 (Accessed 11 March 2016) (2011).

[29] M. Conti, L. V. Mancini, R. Spolaor, N. V. Verde, Analyzing Android encrypted network traffic to identify user actions, IEEE Transactions on Information Forensics and Security 11 (1) (2016) 114–125.

[30] M. Conti, L. V. Mancini, R. Spolaor, N. V. Verde, Can't you hear me knocking: Identification of user actions on Android apps via traffic analysis, in: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, CODASPY'15, ACM, 2015, pp. 297–304.

[31] M. Ambrosin, M. Conti, T. Dargahi, On the feasibility of attribute-based encryption on smartphone devices, in: Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, IoT-Sys'15, ACM, 2015, pp. 49–54.

[32] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, K.-K. R. Choo, Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices, Australian Journal of Forensic Sciences (2016) 1–28.

[33] M. Ibrahim, M. T. Abdullah, A. Dehghantanha, VoIP evidence model: A new forensic method for investigating VoIP malicious attacks, in: Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, IEEE, 2012, pp. 201–206.

https://t.me/learningnets

[34] M. Ibrahim, A. Dehghantanha, Modelling based approach for reconstructing evidence of VoIP malicious attacks, International Journal of Cyber-Security and Digital Forensics 3 (4) (2014) 183–199.

[35] [Online], Viber Android Apps on Google Play, https://play.google.com/store/apps/details?id=com.viber.voip&hl=en (Accessed 11 March 2016).

[36] [Online], Skype - free IM & video calls Android Apps on Google Play, https://play.google.com/store/apps/details?id=com.skype.raider&hl=en (Accessed 11 March 2016).

[37] [Online], WhatsApp Messenger Android Apps on Google Play, https://play.google.com/store/apps/details?id=com.whatsapp&hl=en (Accessed 11 March 2016).

[38] E. Casey, B. Turnbull, Digital evidence on mobile devices, Digital Evidence and Computer Crime. Third Edition.

[39] S. Mohtasebi, A. Dehghantanha, Towards a unified forensic investigation framework of smartphones, International Journal of Computer Theory and Engineering 5 (2) (2013) 351.

[40] S. Parvez, A. Dehghantanha, H. G. Broujerdi, Framework of digital forensics for the samsung star series phone, in: Proceedings of the 3rd International Conference on Electronics Computer Technology, Vol. 2 of ICECT'11, IEEE, 2011, pp. 264–267.

[41] S. Mohtasebi, A. Dehghantanha, H. G. Broujerdi, Smartphone forensics: a case study with Nokia E5-00 mobile phone, International Journal of Digital Information and Wireless Communications 1 (3) (2011) 651–655.

[42] G. Grispos, T. Storer, W. B. Glisson, A comparison of forensic evidence recovery techniques for a windows mobile smart phone, Digital Investigation 8 (1) (2011) 23–36.

https://t.me/learningnets

[43] M. Kaart, C. Klaver, R. van Baar, Forensic access to windows mobile pim. vol and other embedded database (EDB) volumes, Digital Investigation 9 (3) (2013) 170–192.

[44] E. Casey, M. Bann, J. Doyle, Introduction to windows mobile forensics, Digital investigation 6 (3) (2010) 136–146.

[45] T. Y. Yang, A. Dehghantanha, K.-K. R. Choo, Z. Muda, Windows instant messaging app forensics: Facebook and skype as case studies, PloS one 11 (3) (2016) e0150300.

[46] V. L. Thing, K.-Y. Ng, E.-C. Chang, Live memory forensics of mobile phones, digital investigation 7 (2010) S74–S82.

[47] K. Barmpatsalou, D. Damopoulos, G. Kambourakis, V. Katos, A critical review of 7 years of mobile device forensics, Digital Investigation 10 (4) (2013) 323–349.

[48] J. Lessard, G. Kessler, Android forensics: Simplifying cell phone examinations., SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL 4 (1) (2010) 1–12.

[49] T. Vidas, C. Zhang, N. Christin, Toward a general collection methodology for Android devices, digital investigation 8 (2011) S14–S24.

[50] B. Martini, Q. Do, K.-K. R. Choo, Conceptual evidence collection and analysis methodology for Android devices, The Cloud Security Ecosystem (2015) 285–307.

[51] B. Martini, K.-K. R. Choo, An integrated conceptual digital forensic framework for cloud computing, Digital Investigation 9 (2) (2012) 71–80.

[52] B. Martini, Q. Do, K.-K. R. Choo, Mobile cloud forensics: An analysis of seven popular Android apps, arXiv preprint arXiv:1506.05533.

[53] Q. Do, B. Martini, K.-K. R. Choo, A forensically sound adversary model for mobile devices, PloS one 10 (9) (2015) e0138449.

https://t.me/learningnets

[54] A. Azfar, K.-K. R. Choo, L. Liu, An Android social app forensics adversary model, in: Proceedings of the 49th Annual Hawaii International Conference on System Sciences, HICSS'16, IEEE, 2016.

[55] M. I. Al-Saleh, Y. A. Forihat, Skype forensics in Android devices, International Journal of Computer Applications 78 (7).

[56] M. Simon, J. Slay, Recovery of skype application activity data from physical memory, in: Proceedings of the International Conference on Availability, Reliability, and Security, ARES'10, IEEE, 2010, pp. 283–288.

[57] N. B. Al Barghuthi, H. Said, Social networks IM forensics: encryption analysis, Journal of Communications 8 (11) (2013) 708–715.

[58] A. Mahajan, M. Dahiya, H. Sanghvi, Forensic analysis of instant messenger applications on Android devices, arXiv preprint arXiv:1304.4915.

[59] N. S. Thakur, Forensic analysis of WhatsApp on Android smartphones.

[60] A. Dehghantanha, K. Franke, Privacy-respecting digital investigation, in: Proceedings of the Twelfth Annual International Conference on Privacy, Security and Trust, PST'14, IEEE, 2014, pp. 129–138.

[61] F. Daryabar, A. Dehghantanha, N. I. Udzir, N. F. B. M. Sani, S. b. Shamsuddin, F. Norouzizadeh, A survey about impacts of cloud computing on digital forensics, International Journal of Cyber-Security and Digital Forensics 2 (2) (2013) 77–94.

[62] A. Aminnezhad, A. Dehghantanha, M. T. Abdullah, A survey on privacy issues in digital forensics, International Journal of Cyber-Security and Digital Forensics 1 (4) (2012) 311–323.

[63] C. Ntantogian, D. Apostolopoulos, G. Marinakis, C. Xenakis, Evaluating the privacy of Android mobile applications under forensic analysis, Computers & Security 42 (2014) 66–76.

https://t.me/learningnets

[64] J. Farnden, B. Martini, K.-K. R. Choo, Privacy risks in mobile dating apps, arXiv preprint arXiv:1505.02906.

[65] A. Azfar, K.-K. R. Choo, L. Liu, Forensic taxonomy of popular Android mHealth apps, arXiv preprint arXiv:1505.02905.

[66] [Online], Samsung odin, http://odindownload.com/.

[67] K. Kumar, S. Sofat, S. Jain, N. Aggarwal, Significance of hash value generation in digital forensic: A case study, International Journal of Engineering Research and Development 2.

[68] A. Skillen, D. Barrera, P. C. van Oorschot, Deadbolt: locking down android disk encryption, in: Proceedings of the 3rd ACM workshop on Security and privacy in smartphones & mobile devices, ACM, 2013, pp. 3–14.

https://t.me/learningnets

View publication stats