ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

A STUDY ON EXISTING TRENDS FOR FORENSIC EXAMINATION OF SOCIAL NETWORKING APPLICATIONS ON ANDROID PHONES

Aiswarya P.S.
M.Tech in Computer Science with Specialization in
Cyber Forensics and Information Security
ER&DCIIT, Trivandrum
Kerala, India
psaiswarya@gmail.com

ABSTRACT

Today android phones have become an integral part of peoples' daily lives. These android hones have built in social networking applications which allow users to exchange instant messages, share videos, audio's and pictures, and as such, they are prone to facilitating criminal activity or otherwise being involved when crimes occur. There are possibilities that potential evidences are held on these devices which can be recovered with the right tools and examination methods. This study mainly discusses about the current trends and works in the field of forensics of the three most widely used social networking applications namely Facebook, Whatsapp and Twitter. This study also aims at providing an overview of the major features of the most widely used android forensic tools.

1. INTRODUCTION

The world today is experiencing technological innovation like never before. This growth is almost exponential in the field of mobile phones. Within mobile phones, smart phones are very much becoming the norm. Improvements in the computing power and data storage of these devices enable us to perform a wide range of activities. People are increasingly becoming dependent on these mobile devices for most of their activities.

1.1 Android devices

The smartphones currently available differ from each other based on the operating system they rely upon. There are a large number of operating systems available like the android, Symbian, blackberry, iOS , windows etc. Among them android is the most widely used operating system. Any operating system (desktop or mobile) takes responsibility for managing the resources of the system and provides a way for applications to talk to hardware or physical components in order to accomplish certain tasks. The Android operating system is no different. It powers mobile phones, manages memory and processes, enforces security, takes care of networking issues, and so on. Android is open source and most of the code is released under the Apache 2.0 license. Practically, this means that mobile phone device manufacturers can access it freely, modify it, and use the software according to the requirements of any device. This is one of the primary reasons for its popularity. Android has become the software of choice for companies who require a low-cost, customizable, lightweight operating system for their smart devices without developing a new OS from scratch. Android's open nature has further encouraged the developers to build a large number of applications and upload them onto Android Market. Later, end users can download the application from Android Market, which makes Android a powerful operating system.

Android devices can perform various functions ranging from the routine tasks such as making calls, sending messages, and so on, to specialized activities such as sending e-mails, surfing the Internet, recording videos, creating and storing documents,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

identifying locations with Global Positioning System (GPS) services, managing business tasks, and much more. These smartphones also contain social networking applications installed in them which allow users to interchange instant messages, share videos, audio's and pictures, and as such, they are prone to facilitating criminal activity or otherwise being involved when crimes occur. In other words, mobile devices are now a repository of sensitive personal information, containing a wealth of user data. Quite often, the data sitting on a device is more valuable than the device itself. With the increasing prevalence of mobile phones in peoples' daily lives and in crime, data acquired from phones become an invaluable source of evidence for investigations relating to criminal, civil, and even high-profile cases.

1.2 WhatsApp, Facebook and Twitter

Instant messenger applications such as WhatsApp and social networking applications like Facebook and Twitter are the most widely used applications on an android device.

WhatsApp is cross-platform instant messenger service that has over 700 million users. It was purchased by Facebook in February 2014 and continues to grow in popularity. WhatsApp allows a user to create an account with the phone number, add profile information, add contacts, sending and receiving a text message, image, video and location information which can be valuable to examiners looking to recover evidence for a variety of different investigation types. Whether analyzing the mobile device of a suspect or a victim, these chat artifacts can contain valuable information to help solve a case.

Facebook is a website providing social network service, launched in February 2004, operated and privately owned by Facebook Incorporation. Its goal is to give people the power to share, and make the world more open and connected. Facebook users may create a personal profile, add other users as friends, and exchange messages including automatic feed notifications when they update their profile information. Additionally, users may share their status, news stories, notes, photos, videos, and allow their friends (or friends of friends) to comment on them. Furthermore, users may join common-interest groups, organize events, and create fans pages for a workplace/business, a school/college, or even a brand/product. However, it is unavoidable that this platform may also provide incentives for criminals to carry out illegal activities.

Twitter is an online social networking service that enables users to send and read short 140-character messages called "tweets". Registered users can read and post tweets, but unregistered users can only read them. Twitter enables a user to create an account, update profile information, follow or unfollow some accounts, comment posting, share location information, send private message to a friend, search a trending topic. These artifacts can play a vital role in an investigation process.

2. RELATED WORKS

In this section, the trends and current state of art in android forensics and forensics of Whatsapp, Facebook and Twitter have been analyzed.

2.1 Android forensics

Andrew Hoog in his book "Android forensics: investigation, analysis and mobile security for Google android" [7] has provided the information about history of the Android platform but also discusses the Android Open Source Project (AOSP), the internationalization of the platform, the Android Market. Further, various Android releases, the Android software development kit (SDK), the Davlik virtual machine, key components of Android security, and several other concepts core to Android forensics such as the Android debug bridge (adb) and the USB debugging setting have also been discussed. It also covers the information needed to understand how data are stored on an Android device and the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

various file systems used in an android device in great detail including the YAFFS2, EXT, FAT32/FAT16. It also provides a review not only of how data can be exfiltrated from an Android device is covered but also of how an Android device can be used as an active attack vector. Various techniques to analyze an acquired Android device have also been discussed.

2.2 WhatsApp forensics

Shubham Sahu has published a paper [1], which describes the process of conducting forensic data analysis by extracting useful information from WhatsApp and from similar applications installed on Android platform. The paper presents that the WhatsApp Database Encryption Project has made known a vulnerability in the Android implementation of the AES Cipher: the 192-bit key can be detected performing both static or active analysis on the software package. A python script is designed which uses this same key to decrypt the encrypted db file and presents the result in a well organised HTML page. The paper implies that the same encryption key is used for all WhatsApp installations on Android. In the proposed methodology, a Python tool is used to decrypt and read the encrypted database on WhatsApp 2.11.186. It also suggests that the database files can alternatively read through the 'SQLite browser' but the timestamps and representation of data is not straightforward. It also suggests retrieving the artifacts after the factory reset of the phone or retrieving the deleted data as the future enhancement.
In [5] Aditya Mahajan et al. have illustrated the forensic data analysis conducted on two major instant messenger applications namely WhatsApp and viber. The tests and analysis were performed with the aim of determining what data and information can be found on the device's internal memory for instant messengers. In the analysis Cellebrite UFED Classic Ultimate (V 1.8.0.0) has been used for extracting the files and folders. File system Extractions were carried out using UFED so as to understand the data stored in files and folders of the phone's internal memory. UFED physical Analyzer has been used to view the information extracted from UFED. The result of the analysis showed that Physical Analyzer was able to provide the artifacts related to

"WhatsApp" app only but in manual and folder by folder Analysis of the Extracted data all possible artifacts related to "WhatsApp" and "Viber" applications were found along with Timestamps.

In a paper presented by Neha S. Thakur [4] the extraction and analysis of WhatsApp application related user data from non-volatile external storage and the volatile memory (RAM) of an Android devicehas been explained. The approach followed was to perform live analysis on the android device to extract user interaction information. The evidence collection process concentrated on WhatsApp data acquisition and analysis from both non-volatile and volatile memory. A tool named whatsappRamXtract has been developed to extract information from the heap dump and show the binary contents to the user in a readable format. The tool could carve out numbers, messages and database data from a file. The results of the research showed that critical application data was present in the RAM and it could be extracted for further analysis. It also showed that to get easy access to data in the database, the device memory also cached it in the volatile memory.

A paper has been presented by Nedaa B. Al Barghuthi et al. [2], which aims at investigating through forensics and sniffing techniques, the possibilities of hiding communication using encryption to protect the integrity of messages exchanged. Authors used different tools and methods to run the investigations. Such tools include Wireshark packet sniffer, Forensics Tool Kit (FTK) and viaForensic mobile forensic toolkit. First, the authors installed viaForensic utility on the forensic workstation - viaForensic is a forensic utility, very useful for android logical acquisition without the need to root the device. Then, the smart phone is connected via a USB cable to the forensic workstation. After that, a logical acquisition was

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

performed on the device. Android provides a relationship database for each application using SQLlite database viewer to store data securely and efficiently. The acquired image was analyzed through viaForensics utility and SQLite database viewer and investigates any evidence related to the instant messaging. As a result of the analysis the author was able to identify the encryption algorithms used in the encryption tool to encrypt the instant message through the Wireshark packet sniffer and forensics investigating tools. Also, the author also identifies the encryption features using Wireshark packet sniffer at different instant messaging messengers.

2.3 Facebook and twitter forensics

Noora Al Mutawa et al., published a paper [6], which focused on conducting forensic analyses on three widely used social networking applications on smartphones: Facebook, Twitter, and MySpace. The tests consisted of installing the social networking applications on each device, conducting common user activities through each application, acquiring a forensically sound logical image of each device, and performing manual forensic analysis on each acquired logical image. The forensic analyses were aimed at determining whether activities conducted through these applications were stored on the device's internal memory. If so, the extent, significance, and location of the data that could be found and retrieved from the logical image of each device were determined. A forensic examination of an Android phone's logical image showed that basic

Facebook friend information is stored in the contacts database (contacts.db) as the device "synchronizes contact's Facebook status updates with the phone book. It also showed that the device stores Twitter passwords and Twitter updates performed through the Twitter application in plain text. The test procedure consisted of three stages: scenarios, logical acquisition, and analysis. The results of the tests showed that significant data such as user details, photos uploaded, chat messages were recovered from all the three applications through analysis of the logical image of the device.

In a research paper presented by Simon Leppert [3], the memory of the most widely used android apps have been analyzed. In the analysis Facebook app version 1.8.4 has been used with the sha256-hash "92f5be800bae1a96b4dad6447a3aa7e84a8694f4a74 c4f5984d0dd0c73970603" and there occurs a variation between the "logged in"- and "logged out"-state of the app. In the "logged in" state a great deal of interesting information can be found, even the username and password is visible in the plaintext. After analyzing multiple Facebook-dumps, it was found that the string "pwd" can be easily connected to the password-string because every time a Facebook-dump is analyzed, the pwd-string was found one line after the password-string. After searching for the password the username was searched. Facebook generally uses an email-address as a username. The easiest way to extract email-addresses from a text file is to use regular expressions, sometimes shortened to regex. A regular expression is a special text string for describing a search pattern.

In case of twitter the app-version 3.0.1 with the sha256-hash "e3b0c44298fc1c149afbf4c 8996fb92427ae41e4649b934ca495991b7852b855" was analyzed differing between the "logged in"- and "logged out"-state of the app. In logged in state by searching for the string "account name" many results were obtained. When "account name" was referenced with something other than the string "unknown" the username was found. Not only is the username was present in the dump, other useful information could be found too. For example all the Tweets of the user and the name of the Twitter user were present. The password was not present in plaintext in the Twitter-App unlike the password of the Facebook-App. The reason for that is that the Twitter-App uses the OAuth 1.0 Protocol. OAuth is an authentication protocol that allows users to approve application to act on their behalf without sharing their password. In the logged out state nothing changes concerning the information

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

that is present in the dump. The username, the name of the Twitter-user and all Tweets are still present in plaintext and detectable in the same way as in the "logged in"-state.

In [8], an analysis has been performed that mainly uses various physical and logical acquisition tools for memory forensics. After locating the evidence of a Facebook activity, its footprints could be examined by referring to the response from corresponding Facebook communication. The same activity may be tested several times with different contents to increase the accuracy. They conducted the following logical acquisition for Facebook forensics in Android devices: Hauwei device version 1.6 and 2.1 (not rooted), Debugging/Recovery mode (same as physical acquisition or dd imaging), Hoog's method (AndriodForensics.apk), YAFFS2 file system, YAFFS2IMG Browser. More information could be discovered from Android device with correlated Gmail account for further investigation. As a result of this analysis it was concluded that Facebook core is a social graph, with objects such as people, photos and events, as well as connections between them such as friend relationships, shared content and photo tags.

Properties of objects can be accessed by sending HTTP requests to Facebook Graph API and all responses are JSON objects. Since these objects could be displayed on a web browser, they need to be converted to HTML format with additional layout information. Therefore, Facebook comments and chats identified could be in JSON or HTML formats with the same key ""text"". It was further identified that most of the legitimate Facebook footprints from could also be retrieved from RAM. These footprints include Facebook user profile ID, the message contents and corresponding timestamps.

3. EXISTING TOOLS

This section discusses about the android forensic tools and their major features. The tools considered here are the Cellebrite UFED, the Android debug bridge, the AFLogical, ViaExtract, Autopsy and ViaLab.

3.1 Cellebrite UFED

The Cellebrite UFED Forensic system is a stand-alone device capable of acquiring data from approximately 1600 mobile devices and storing the information on a USB drive, SD card or PC. It comes with optional desktop software. The UFED package ships with about 70 cables for connecting to most mobile devices available today. Connection protocols supported include serial, USB, infrared, and Bluetooth. UFED can extract, decrypt, parse analyze all mobile data. It also enables data retrieval through all the three extraction methods namely logical, file system and physical extraction. Cellebrite also distributes the UFED Report Manager, which provides an intuitive reporting interface and allows the user to export data/reports into Excel, MS Outlook, Outlook Express, and CSV or to simply print the report. The UFED device fully supports Unicode and thus, can process phones with any language enabled. UFED Physical Analyzer v3.9.6.7 was tested within CFTT program. Any data which the UFED extracts is hashed using SHA256 and/or MD5 algorithms, which helps to maintain data authenticity. These algorithms are included within the .UFD file.

3.2 Android Debug Bridge (adb)

Android debug bridge is a multipurpose command line tool that acts as a bridge between the connected android device and the adb installed device. It lets to communicate with connected Android-powered device. Unless an Android device has root access, the adb daemon only runs with shell permissions. As such, some of the more forensically relevant files are not accessible. adb is not only a free utility in the Android SDK but also very versatile. When connected to a device it builds a virtual network over the USB connection and creates a server on the system and a client on the phone. To copy the data from the phone to another computer "pull" command can be used. If an attempt is made to access files that

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

the shell user does not have permissions to, it simply does not copy the files. As most phones will not have root access (at least by default), this technique may appear to be of little value. However, it is a powerful utility to understand and there are several scenarios ideal for this approach. These scenarios include:

- On nonrooted devices, an adb pull can still access useful files such as unencrypted apps, most of the tmpfs file systems that can include user data such as browser history, and system information found in "/proc," "/sys," and other readable directories.
- On rooted devices, a pull of nearly all directories is quite simple and certain files and directories from "/data" would be of interest.
- When utilizing the physical technique, it is not always possible to mount some acquired file systems such as YAFFS2. If adbd is running with root permissions, a logical copy of the file system can be quickly extracted with adb pull.

As adb is not only a free utility in the Android SDK but also very versatile, it should be one of the primary logical tools used on a device. Some recursive pulls using adb can fail in the middle of the data transfer due to permission or other issues. Then the results of the command should be closely monitored to determine if any issues were encountered. Breaking the recursive pull of large directories into smaller data pulls may yield better results.

3.3 AFLogical

AFLogical is an Android forensics logical technique which is distributed free to law enforcement and government agencies. The app, developed by viaForensics, takes advantage of the Content Provider architecture to gain access to data stored on the device. Similar to commercial Android logical tools, USB debugging must be enabled on the device for AFLogical to extract the data. The current version, 1.5.1, extracts data from 41 Content Providers and provides the output information to the SD card in CSV format and as an info.xml file, which provides details about the device and installed apps. AFLogical supports devices running Android 1.5 and later, and has been specifically updated to support extraction of large data sets. The extracted data are saved to the SD card of the device in a directory called forensics and a subdirectory named after the date in YYYYMMDD.HHMM format. The CSV files can be viewed using any editor or spreadsheet. There is also a file in the directory called info.xml, which contains information about the device including the IMSI, IMEI, Android version, network provider, and more, as well as the list of all installed apps.

3.4 ViaExtract

ViaExtract is a logical and physical extraction tool created by NowSecure (formerly known as ViaForensics). Logical acquisitions (including backups) are available with the free version, while the paid version adds physical extractions. It is freely distributed inside of a virtual machine file (either VMWare or Virtual Box formats) running NowSecure's Santoku Linux distribution. An active Internet connection is required while using the free version. ViaExtract can also attempt to root a device and bypass the passcode. This is a useful tool because unlike the manual methods, it does not require root access. During the logical extraction through this tool, the ViaExtract application will be pushed to the device and further actions may be required on the device. This tool also supports backup extraction and filesystem extraction if the device is rooted.

3.5 Autopsy

Autopsy is a free and open source analysis tool initially developed by Brian Carrier. Autopsy started as a Graphical User Interface for the underlying Linux-based SleuthKit toolset, but the latest release

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 5, February 2016 in association with
HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM
Organizes
NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)
(12th -13th February 2016)

(version 3) is a standalone tool built for Windows. Autopsy is not intended to perform acquisitions of mobile devices, but can analyze the most common Android filesystems (such as YAFFS and ext). It allows keyword searching, hash lists, and other forensic methods. this tool has a powerful timeline feature. The most important advantage of this tool is that it can recover deleted data from supported filesystems.

3.6 ViaLab

ViaLab Community Edition is another free tool developed and released by NowSecure. It is shipped as a standalone virtual machine. The VM is actually very similar to the Santoku download but includes the ViaLab Community Edition tool. ViaLab requires the examiner's computer to have an Internet connection, in order to use the tool. The main purpose of ViaLab is to analyze the behavior of an APK, although many of the features to do so are unavailable in the free Community Edition. ViaLab allows to either manually load an APK file into the Android emulator or run the application on a rooted device. It is a valuable tool to show an examiner where data is stored in an app's directory, as well as see the functionality of the application.

4. CONCLUSION

As the number of people using android phones is rapidly increasing, the number of crimes involving these phones is also increasing. The social networking applications installed in these phones act as a repository of personal information. These information can be of great help during an investigation if one knows where to search and what data can be captured. This study provides detailed information about the trends and current works in the field of android forensics and forensics of applications like Whatsapp, Facebook and Twitter. This study also discusses the major features of the android forensic tools namely the Cellebrite UFED, the Android debug bridge, the AFLogical, ViaExtract, Autopsy and ViaLab.

5. REFERENCES

[1] Shubham Sahu, An Analysis of WhatsApp Forensics in Android Smartphones, International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print) Volume No.3, Issue No.5, pp : 349-350, 01 May 2014.

[2] Nedaa B. Al Barghuthi, Social Networks IM Forensics: Encryption Analysis, *Journal of Communications Vol. 8, No. 11, November 2013.*

[3] Massimo Barone, Step by step analysis of facebook and twitter data on android device, eForensics magazine, issue 2/2013 (2) May, vol.1 no.2

[4] Neha S. Thakur, Forensic Analysis of WhatsApp on Android Smartphones, *University of New Orleans Theses and Dissertations.* Paper 1706, 2013.

[5] Aditya Mahajan et al., Forensic Analysis of Instant Messenger Applications on Android Devices, *International Journal of Computer Applications (0975 – 8887) Volume 68– No.8, April 2013*

[6] Noora Al Mutawa et al., Forensic analysis of social networking applications on mobile devices, Digital Investigation 9 (2012) S24–S33.

[7] Andrew Hoog, Android forensics: investigation, analysis and mobile security for google android, 2009.

[9] Kelvin Wong et al., Facebook Forensics, Valkyrie-X Security Research Group.