Gathering Evidence from Android OS for Mobile Forensics

[1] Srivatsa Raju S; [2] Anjan K Koundinya; [3] Bharathi R

[1] Department of Computer Science and Engineering, B.M.S Institute of Technology & Management,
Bengaluru, India

[2] Department of Computer Science and Engineering, B.M.S Institute of Technology & Management,
Bengaluru, India

[3] Department of Computer Science and Engineering, B.M.S Institute of Technology & Management,
Bengaluru, India

Abstract - Android OS forensics is a procedure which involves, preserving, extracting, documenting and analyzing digital evidence from devices, which hosts Android OS. These Techniques encloses multiple phases, which includes insights of Android OS Hosting devices internal architecture, structure and digital data footprint analysis and close examination approaches. In today's world Android devices can handle multiple tasks with low computational time and memory consumption with greater speed, which requires a correct, optimized and task specific OS. In this growing market open source as well as proprietary programs or proprietary programs with illegal access and Android OS are readily available. People use untrusted sites to gain illegal access for proprietary programs. The usage of android devices is a rapidly growing sector which in turn involves an integral part of many cybercrimes and key targets for attacks. The necessity for a proper android forensics tool is an essential need for gathering evidence for conducting a proper action against crime. This paper briefly discusses various tools for collecting the digital evidence in the field.

Keywords - *Android, Operating System, Evidences, Tools, Footprints*

1. Introduction

Android OS hosting devices and its applications have become integral part in our daily routine, which starts from checking notification, controlling home appliances, catching a ride to office, making digital payments, booking events tickets accessing emails placing phone calls messages and much more in professional life and personal life. Its programs may be exploited through scripts and cybercriminals to benefit illegal get admission to or to perform dangerous moves. In the event of a crime the evidences from this device which has the control over the various aspect of a person life, plays a vital role in providing the data to collect, analyse and document which in turn catalysis the process of resolving the crimes in further phases [1].

IT Security problems expanded with plethora of smartphones. Therefore, the software of digital forensics to cellular telephone devices has these days been uttered by means of some researchers. It also gives greater perception for both Operating Systems (OSs) builders in addition to cellular device customers in the shape of advanced security features. Finally, it assists in growing sturdy and powerful antimalware packages as well as programs. This research depicts light on instant messages, encrypted instant messages, unlocking passcode and Tait cloning the instances.

2. Background

Android forensics is attracting researchers as well as industrialists for conducting efficient forensics [2]. Android as a mobile operating system developed based on Linux kernel by Google. Android architecture is built with four primary components: Linux Kernel, Android Libraries, Application Framework and Applications. Linux kernel implicit all low-level device functionality drivers for primary hardware components of Android. Android Libraries contain programs that enable key features of an Android OS.

Mobile device forensics is a part of digital forensics that the recovery of digital evidence data from a suspected mobile device. mobile forensics tools and five stages for investigation process that are preservation, acquisition, examination, analysis, and reporting. Here, the comprehension of mobile devices' organization and the operational process should be incorporated with digital data preservation, acquisition, and presentation skills. The core idea is mainly based on understanding what type of digital evidence in a manner that preserves its evidentiary significance, and how can possibly be extracted, and from where it can be acquired. Thus, good knowledge of hardware on which Android OS hosts and software is required.

2.1 Digital Forensics

This concept of forensics analysis can be viewed as a process of presentation of digital evidences, identification of evidences, conservation of identified evidences, processing and acquisition [3].
In the IT field the view of digital forensics for electronic crimes including cyber-crimes as such the following process should be taken into consideration for presenting the legal case.

Identification: The electronic personal devices which contain the digital form of evidences should be precisely identified such that they can be investigated further such as storage space, application logs, short message services, subscriber identity modules, search history, location services, digital photographs, instant messaging services, visual digital records, files and folders, where the investigator needs access of different kinds of tools according to the identified evidence [4].

Conservation: The metadata acquired from the suspected instrument should be preserved with at most priority in several cases the investigator must take a cloned backup of the instrument and progress further to prevent loss of valuable digital evidence in analysis and examination steps [5].

Acquisition: This is a critical step a forensic investigator must know of identifying potential records by using the best available tools and analysis methods for collecting digital data [6].

Analysis and Examination: From the previous steps the acquired digital evidences has to be precociously classified in an orderly manner before proceeding to further steps of analyzing and examining. With the usage of various tool for the same data set one can acquired various results from each tool, identifying the valuable data from the acquired results is a key function in forensics which required experience and knowledge [7].

Presentation: After the following previous procedure of evidence analysis, it has to be present in court of law where one can understand it effectively. This step plays a key role of serving the evidence in front of individuals irrespective of technical understanding capabilities [8].

2.2 Mobile Digital Evidence

The rapid exchange of data using e-devices generates a trail of evidences which can be useful for forensics. Where the data can be categorized based on its size and structure thus helping in acquisition, analysis conservation, and presentation of the effective evidences.

The following tools support for collecting theses various data types for collecting the digital evidences such as bypassing the passcode screen, cloning the android device to process behavioral changes, deep analysis of images and social media applications, checking user logs, hashing, encrypting and decrypting evidences. All halftone illustrations or pictures should be clear black and white prints. Supply the best quality illustrations or pictures possible.

3. Tools

3.1 Androsics

A forensic tool for Android Operated smart device to collect digital footprints from a personal mobile phone. The Androsics is an open source tool with ADB utilities for forensics information gathering which includes the cracking of lock screen which is an essential and primary security of any android device. With the ADB command utility the investigator can have command line interface access to the device storage and system services.

The ANDROSICS tool also supports extraction of data on device such as manufacture, model, version, activity information. The backup and restore from the Android Debug Bridge command helps in creating a backup and cloning of the device which is a valuable feature for investigation. Live Log Data features in logcat which can collect and view various system application circular buffer with filters, Dumpsys displays information about the system status, Dumpstate views the detailed information of the storage state of the device, CPU Process shows the PID of running sleeping process states which can enable the investigator to view the metadata, virtual key provides button feature of the device without physically accessing the hardware, Dead analysis at the scenario of a seizure the hardware device might be found at power less state which might cause the loss of volatile memory this technique can bypass and decode screen lock reboot option cryptography and deep analysis, the bypass screen lock first uses the USB debugging mode with RSA key for authentication of root access, decode screen lock extracts the pattern password pin security of the hardware which can be found at file locations of the Android OS example - */data/system/gesture.key* for pattern */data/system/password.key* for pin and */data/system/locksettings.db* or */data/com.android.providers.settings/databases* the location varies for different versions of android.

The reboot option support when the device needs to be restarted for gaining access into devices safe mode which can provide root access of the files. Cryptography the process after gathering the required information from the device the investigators needs to collect evidence this is done with help of popular algorithms like hex string, text string and file for encryption and decryption. Deep analysis for imagining and social media application where one can capture the memory image by this feature.

3.2 Instant Messaging Applications

The growth of social media services such as Facebook, Twitter, Instagram as such provides a brief insight of a person social lifestyle on the internet the analysis of this data can be a key evidence to determine the cause or motive of the crime, instant messaging services like Blackberry messenger, WhatsApp, WeChat and Line are multiplatform with more number of users the paper shed light on forensic tool namely, Oxygen Forensic Suit, Metasploit, Andriller, WhatsApp DB extractor and Key Extractor. The success rate of each framework such as the oxygen Forensic Suit is about 57% on BlackBerry messenger and WhatsApp, 42% on Line messenger, 42% on extracting WhatsApp Db and Key extractor

The instant messaging forensic procedure follows NIST model to gather, identify, analyze and report the collected digital evidence according to these four stages. Collection is the first step where the specifications, operating system version, IMEI, and other related data is carried out.

Andriller: The evidence extraction process can be carried by physical because this tool does not support backup and imaging.

Oxygen Forensic Suit (OFS): The OFS is a tool with good capabilities with backup and restore feature so the extraction process can be done both physically and logically.

WhatsApp DB Extractor: The WhatsApp DB extractor can acquire only logical evidences; hence backup is a critical feature conducted before extraction procedure.

Metasploit: The security software that can be used for forensic has the capability to extract data for the hardware devices.

3.3 Encrypted Instant Messaging Applications

The rapid increase in interception of chat messages led to development of end to end encryption due to concerns raised on privacy and security applications namely
Viber, WeChat, WhatsApp and Telegram enforces end to end encryption the paper discusses about the Android Debugging Bridge for data gathering and some of the open source tools. The ADB pull and ADB backup commands are used for backup and imagining of the device once taken.

Viber Forensics: The Viber messaging service has over million active users, the application is available for free on google play store, after installation the application is placed in the file system *"/data/data/com.viber.voip"* and media at *"/sdcard//viber/media"* with the gathering procedure of ADB commands the viber_data database file and viber_messages database file can be obtained with the SQLite DB browser the encrypted messages can be read in plain text format.

WeChat Forensics: With more than 100 million active users worldwide and freely available on google play store after installing the application is placed in the location *"/data/data/com.tencent.mm/"* and *"sdcard/Tencent/MicroMsg"*. With the ADB commands the db of WeChat can be found in these locations these are encrypted databases which needs a unique number which the application uses the IMEI international mobile equipment identity and MD5 using this in the SQLite browser once can view the messages in plain text format.

WhatsApp Forensics: It is a cross platform service and over 1 billion active users and growing, tools required for this is a workstation with Java and Android Mobile device, with USB debugging enabled, ADB drivers, WhatsApp key DB extractor, viewer, SQLliteSpy once the connections are made the timely backup by the WhatsApp is copied from device using ADB commands and extracted in workstation the Msgstore.db can be viewed using SQLiteSpy it contains all the communication that takes place between to associated persons.

Telegram Forensics: There are over 100 million active user and the application is listed on google play store available for free the application stores data on the android file system in the location *"/data"* directory with the ADB commands the chats data can be extracted. Telegram uses four different kinds of chat: One to one regular chats, one to one secret chats, one to many channels, many to many groups, the encryption used by the application is 256- bit symmetric AES encryption, DH secure key encryption, 2048-bit RSA.

4. Conclusions

The main goal of this paper is to study and analyze the most popular applications encrypted data storage locations in Android devices. We discuss the challenges faced during data extraction from the encrypted databases. The forensic analysis of targeted application on their current versions provides important insight to the forensic investigators as well as the researchers. This work will allow the investigators having a clear perspective about where to look for the relevant data when any of those applications involved in their case.

References

[1] Tayeb, Hussein & Varo, Chan. (2019). Android Mobile Device Forensics: A Review. 1-7. 10.1109/ISDFS.2019.8757493.

[2] D. R. Hayes, A practical guide to computer forensics investigations. INpolis, IN, USA: Pearson, 2015, pp. 348-349.

[3] N. Scrivens and X. Lin, "Android Digital Forensics: Data, Extraction and Analysis," In Proceedings of the ACM Turing 50th Celebration Conference-China. 2017. DOI: http://dx.doi.org/10.1145/3063955.3063981

[4] N. R. Roy, A. K. Khanna and L. Aneja, "Android Phone Forensic: Tools and Techniques. IEEE International Conference on Computing, Communication and Automation (ICCCA). 2016, pp. 605-610

[5] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 2011. Academic Press.

[6] M. Kwan, R. Overill, K. P. Chow, J. Silomon, H. Tse, F. Law, and P. Lai, "Evaluation of evidence in Internet auction fraud investigations. IFIP International Conference on Digital Forensics. 2010, pp. 121- 132.

[7] N. Beebe, "Digital Forensic Research: The Good, the Bad and the Unaddressed," IFIP International Conference on Digital Forensics. 2009, pp. 17-36.

[8] R. Ayers, S. Brothers and W. Jansen, Guidelines on Mobile Device Forensics (Draft). NIST Special Publication. 2013, 800, 101.