RESEARCH ARTICLE OPEN ACCESS

User Trail Identification Using a Guided Software

Khushboo Sharma, Mudita Sharma, Garima Chhaparwal, Kanchan Chowdhari
Cummins College of Engineering for Women
Pune - India

ABSTRACT
In digital forensics one of the primary objectives of forensic data collection is identification, analysis, interpretation of seized devices. However many a times it is observed that when a stray mobile device is seized, a common man does not have the expertise to identify the owner of the device. Hence there is a need of easy mechanism for getting the traces of the owner of the mobile device. This paper proposes a prototype of a guided software that can help in identification of owner of mobile device.

Keywords:- Data extraction, android, mobile forensics, adb, Smartphone, SQLite.

I. INTRODUCTION

When a handheld device is recovered from a location, many a time it is a challenge for police or any other person to identify the owner of this handheld device. A guided software can be used to recover vital information from an handheld device .This includes identification parameters, browser data, contacts and data from various installed applications. Guided software can be developed for any kind of operating system .This paper proposes a guided software for a specific android version. Rest of the paper is organized as follows: Section II gives a brief description of related works done on this topic .Section III deals with a brief description about android file system .Section IV deals with digital evidences present in an android smartphone. Section V presents working of guided software developed s Section VI includes the scope of the system and Section VII concludes the paper.

II. RELATED WORKS

Lessard and Kessler were the ones who first conducted works in this area. The authors investigated the smartphone by a acquiring a logical and physical image of the device and analyzed it using Access Data's Forensic Tool Kit (FTK). Felix Freiling, Michael Spreitzenbarth and Sven Schmitt steps up a quite similar environment like we do by explicitly dumping the SQLite databases from the device**.** But this tool gives information only about telephone book and call lists, calendar entries, SMS messages ,GPS locations from different sources on the Smartphone. Lee et al suggested another method in which they use a prepared SD card on which they have placed an own forensic software in order to analyze the Smartphones data. Here the databases were accessed through android system call and SQL commands.

III. ANDROID FILE SYSTEM

There are mainly 6 partitions in Android phones they are as follows:

1./boot- It includes the android kernel and the ramdisk. The device will not boot without this partition.

2./system- This partition contains the entire Android OS, other than the kernel and the ramdisk. This includes the Android GUI and all the system applications that come pre-installed on the device.

3./recovery- The recovery partition can be considered as an alternative boot partition, that lets the device boot into a recovery console for performing advanced recovery and maintenance operations on it.

4./data- Again as the name suggest, it is called userdata partition. This partition contains the user's data like your contacts, sms, settings and all android applications that you have installed. While you perform factory reset on your device, this partition will be wiped out, Then your device will be in the state, when you used for the first time or the way it was after the last official or custom ROM installation.

/cache- This is the partition where Android stores frequently accessed data and app components.

/misc- This partition contains miscellaneous system settings in form of on/off switches. These settings may include CID (Carrier or Region ID), USB configuration and certain hardware settings etc. This is an important partition and if it is corrupt or missing, several of the device's features will will not function normally.

IV. DIGITAL EVIDENCES PRESENT IN AN ANDROID DEVICE

1.Call logs- gives information about the call activities of the owner The investigator can see with whom the owner has contacted including their time and durations.
2.Contact list- The contact list provides contact names and their numbers along with this it also provides many other types of information such as contact title, company name, address and emails.
3.Text messages/ Emails -Text messages and emails gives information that can be used to understand exact text received or sent by the owner of the Smartphone device.
4.Browsing history/internet search-The browsing history and internet searches in the Smartphone device helps the investigator to understand which website the user frequently vists.
5.Media files-Pictures can be used as to find out the recently accessed files by the user

V. WORKING OF THE GUIDED SOFTWARE

A. Welcome window

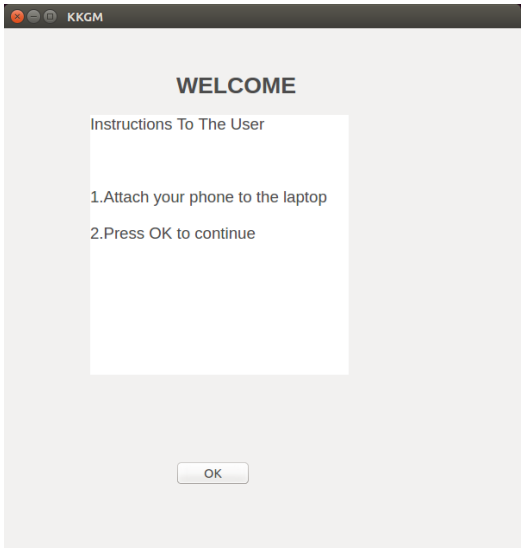

Fig 1. welcome window
This page provides instructions to the user for operating the guided software

B. Phone information

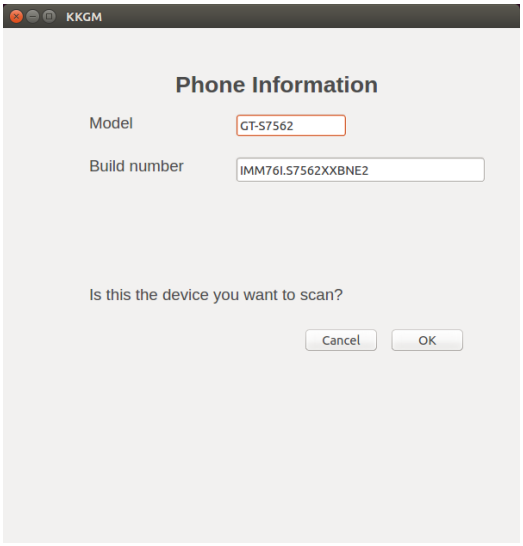

Fig 2. Phone information
This page displays the build number and model number of the connected mobile device. It provides an option to check if the connected device is the target device.

C. Extraction Window

Every android device stores data in database in SQLite format. This data can be extracted in many ways . The proposed guided software uses Android debug bridge for extraction of data from the Smartphone. Android Debug Bridge (ADB)-It is a component of Android Software Development Kit (Android SDK) and is used to dump data from an Android device. In order to get access to android databases using adb the android device must be rooted and at the same time the adbd must also be rooted. Now by using adb pull command we pull the required databases and store it on investigators machine. These databases are extracted according to data and time thus every time when we extract databases new folder is created. Once the databases are extracted the Smartphone is detached from the Investigators machine and the further investigation is performed on the acquired databases.

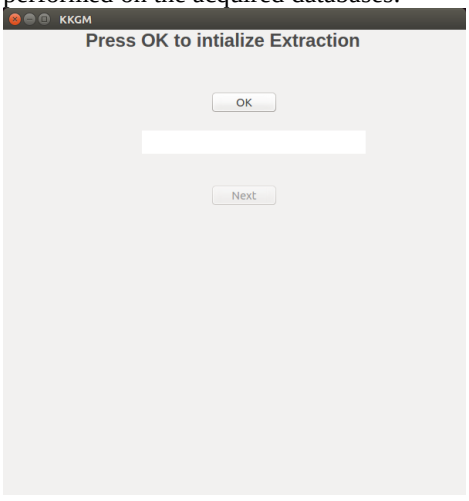

Fig 3.Extraction window

This window enables the extraction process. Further operations can't be processed until complete extraction of data.

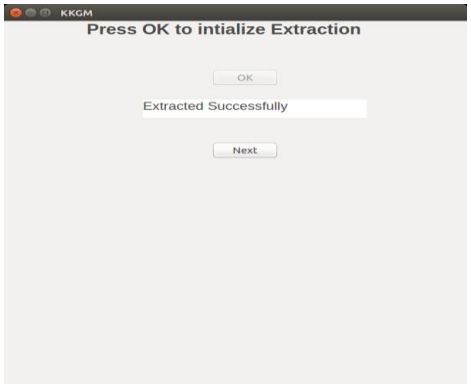

Fig 4.Extraction window

"extracted successfully" status is displayed after successful completion of extraction process. After this the android device must be disconnected from the system.

D. Examination and analysis

After extraction we perform examination and analysis on the acquired databases this is done by querying the databases using SQLite queries. In this system the integrity of databases is checked by calculating the hash values immediately after extraction and also after report generation and these hash values are compared to find out whether data integrity is maintained or not.

E. Report Selection

Select the report you want to see .Following points can be displayed in the report:

1.Recently accessed jpg files.
2.Frequently visited URLs.
3.Recently communicated users on WhatsApp (chat application).
4.Most frequently contacted people from SMS, WhatsApp and caller.
5.Saved URLs with passwords.
6.Call logs.
7.Files shared across Gmail application

This report in generated in pdf format so that user cannot make changes in the generated output

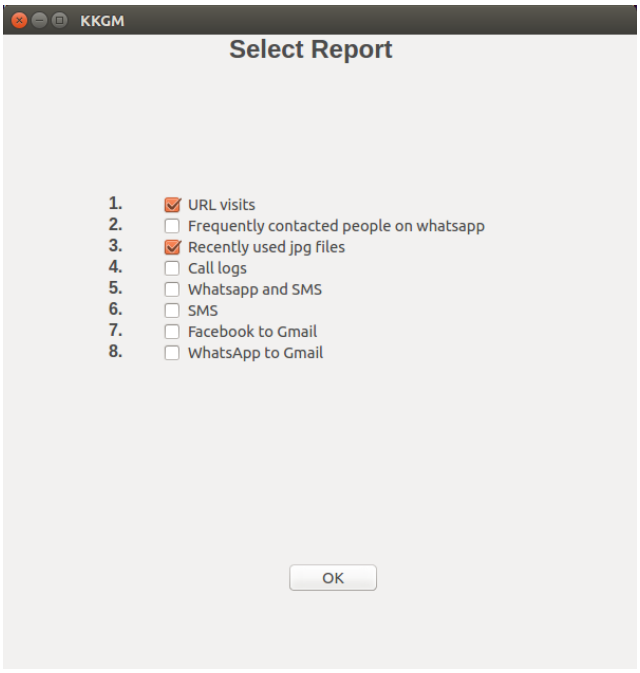

Fig 5.Report selection

F. Generated report

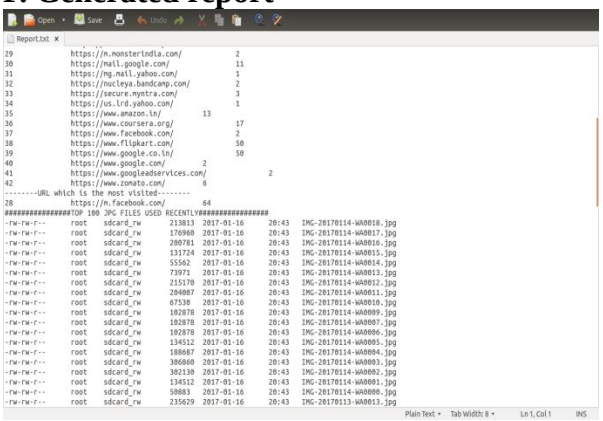

Fig 6.Generated report

VI. SCOPE OF THE SYSTEM

1.We have bypassed the authentication code for our mobile devices.

2.Data extraction is performed only on a mobile device having Android OS. Depending on the operating system, the way of extraction also differs. Hence it becomes an overhead for an analyst to go through the respective ways of data extraction of these operating systems.

.

VI .CONCLUSION

In this paper we have presented one of the methods to analyze mobile phones and produce intelligent information after analysis. We have presented a user guided software which enables automated analysis of an Android mobile device. This software accesses the device via the Android Debug Bridge in order to retrieve a copy of selected SQLite databases. Subsequently, the SQLite databases are extracted , parsed, queried upon and finally transformed into a PDF

REFERENCES

[1] Jeff Lessard and Gary C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations" , Small Scale Digital Forensics Journal Vol, No. 1,September

[2] Felix Freiling, Michael Spreitzenbarth, Sven Schmitt, “Forensic analysis of smart phones: The android data extractor lite (ADEL)”, ADFSL Conference on Digital Forensics, Security and Law, 2011

[3] Khawla Abdulla Alghafli1, Andrew Jones1, Thomas Anthony Martin, “ Guidelines for the digital forensic processing of smart phones” ,Australian conference 2011

[4] [Online]Available: https://www.andrillers.com/developers

[5] [Online]Available: http://www.tutorialspoint..com/pyqt

[6] [Online]Available: https://www.xdadevelopers.com