World Essays Journal / 5 (1): 46-51, 2017

A Windows based Design and Implement of Mobile Forensic Software for Android Smart Phone via USB Cable

Mohammad Roohi[1], Ali Bozorgmehr[2]

1. Islamic Azad University, Science and Research Branch, Tehran, Iran
2 .Nanotechnology & Quantum Computing lab, Shahid Beheshti University, G. C., Tehran, Iran

***Corresponding Author email**:* mohammad.roohi@srbiau.ac.ir

ABSTRACT: Recently, by increasing the popularity of Android smart-phones, the applications of this operating system is getting increased. This increasing is continued as far as it become to a high production in our life. One of the important features of the smart-phones is their large storage database; this storage makes the smart phones to a great provider of digital evidences in crimes in different applications from evidence on the court to checking commuting in military areas. In this research, a new forensic software is introduced that can connect mobile devices to the Android operating system by the USB hub and copy mobile data into the computer. By using the proposed software, after connecting the device into a computer and running it as an embedded program, we can gain and store various information such as text messages, phone numbers, calls log, images, videos, audio files and images and social networking videos with just a few clicks on the computer. This research is based on National Institute of Standards and Technology (NIST) the digital forensics and regulations and to analyze the forensics of Android smart-phones with new proposed digital forensics software.
Keywords: Mobile forensics, Smart phone, Android, USB cable.

INTRODUCTION

According to marketing research from the International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker, a total of 347.4 million smart-phones are shipped by phone companies worldwide in the first quarter of 2017 (1Q17) (ADC). The smart-phone marketing research report in 2017, Android's OS has up to 80.7% beyond all smart phones. By increasing the marketing of smart-phones, there is also come out an increasing potential for criminals to use this technology as well (Petraityte et al., 2017).

Smart phones can be utilized by criminals for different activities like committing fraud over e-mail, trafficking of child pornography, harassment through text messages, communications related to narcotics, etc (Rogers, 2017). In other words, with the spread of the use of smart-phones, one of the most important signs of crime can be the corrupted information on the cell phone of the person (Dlamini et al., 2016).

The occurrence of crime and the increasing spread of crimes and the need to deal with such threats require lawyers and crime specialists to work together and help legislators to create a strong barrier to crime. In this regard, the identification and discovery of crime and the analysis of the causes and factors affecting the crime can help the government to adopt appropriate strategies to reduce crime and thereby increase the welfare of the people.

Research studies indicate that the police of developed countries have examined the use of the crime analysis process with a new approach and, as a result of this attention is the further development of the scientific discovery of crime and the promotion of crime sciences (Baechler et al., 2017).

Therefore, we can consider the positive feedbacks for this stored data like analyzing through the course of an investigation (Wu et al., 2017).

Indeed, smart-phones have extensive information of their user such as call history, contact, text message data, e-mail, browser history, and chat logs (Wilson and Chi, 2017). This reason makes digital evidence to become a significant issue of innocence proof when enterprises have suspicions of personal information leakage.

Different types of operating systems are generated to smart-phones. Good forensic software should have the ability of detecting for more smart-phones. In the last years, Android based smart-phones have become to a popular operating systems in the world wide.

Therefore, designing a forensic software for detecting the Android based smart-phones can resolve more problems (Sitova et al., 2016). According to the raised mobile security issue in smart phones applications, the main purpose of this study is to acquire the important evidences from smart-phone by using new developed Android forensic software to examine smart phone digital forensics.

Digital Evidence

Any information or data of value to an investigation which is received by, stored on, or transmitted by an electronic device is digital evidence. Emails, text messages, pictures and videos and internet searches are some of the most common types of digital evidence (Romanosky and Goldman, 2016).

The applications of digital evidence are increased since the courts have allowed to use the e-mails, digital photographs, word processing documents, ATM transaction logs, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, Global Positioning System tracks, computer printouts, logs from a hotel's electronic door locks, and digital video or audio files (Casey, 2010).

Digital forensics

Digital forensics is one of the branches of legal crime in the field of computer tools which includes the retrieval and technical review of all content found from any digital device, which is often related to computer crime. Digital legal forensics is essentially synonymous with computer legal forensics, but the term "legal forensics" is generally used to check the technicality of all devices that are capable of storing data (Sunde et al., 2017).

Technical digital forensic experts in the field of digital crime have various tools to prove or reject allegations of criminals or citizens to submit to the court. Digital forensics is technically divided into several sub-divisions: legal computer forensics detection and detection of criminal offenses, Legalization of malware Legal corruption and Legal analysis of mobile forensics (Wolverton, 2016).

Digital forensics is the process of discovery and interpretation of electronic data. The purpose of this process is to preserve any evidence in its original form for a structured survey, which is done by collecting, identifying and validating digital information in order to rebuild past events (Nance and Bishop, 2017). The process of digital forensics includes the following cases:

Seizure of digital devices.
Copying of all data carriers (whether internal or external)
Analyze all existing content.
Provide a complete report of all the evidence obtained from documentation.

Android Operating System

Android is a mobile operating system which is developed by Java language and Android SDK application based on Linux operating system and includes variety of modern devices, the most popular being smart-phones (Yovine and Winniczuk, 2017).

It is generally a piece of software to command your hardware to do something. The Android OS allow us to have the access to the apps, including many of Google's own creation. These characteristics made us an ability to look for information on the web, check our location on a map, play music and videos, take photos using our device's camera, etc (Perumal et al., 2017).

Android OS includes four layouts from the Linux 2.6 Kernel in the bottom layout, libraries and Android Runtime on the third layout, application framework on second layout and Android applications on the top layout (Developers).

System Architecture

The proposed method is performed on the smart-phones for forensic application. The operating system is Android OS. For performing digital forensic, the user should download the application, install the system, and then execute the mobile forensic. The results will instantly upload to the computer hardware by using the USB hub, and then generate forensic report. The system architecture is illustrated in Fig.2.

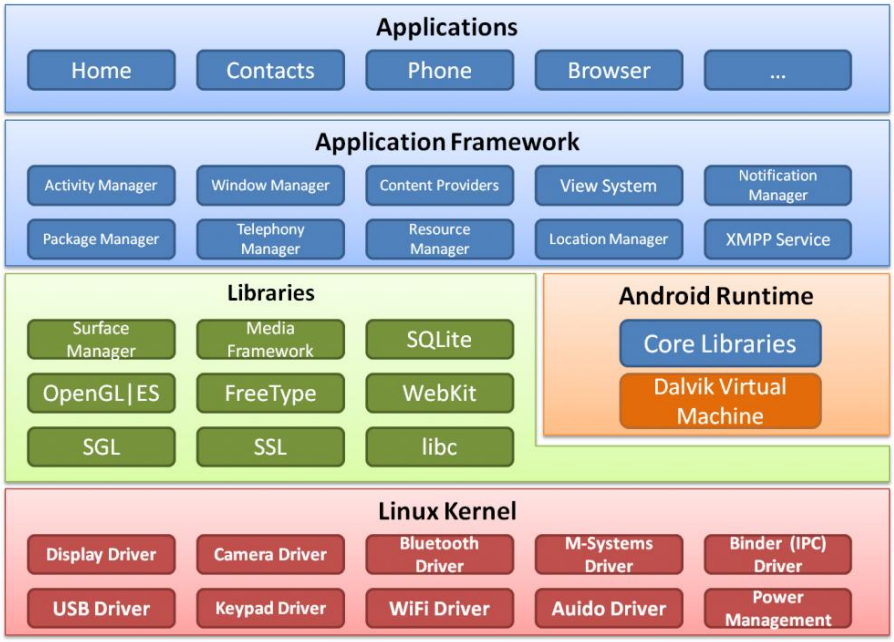

Figure1. Android Architecture (Atkinson and Lorenzo Cavallaro, 2017)

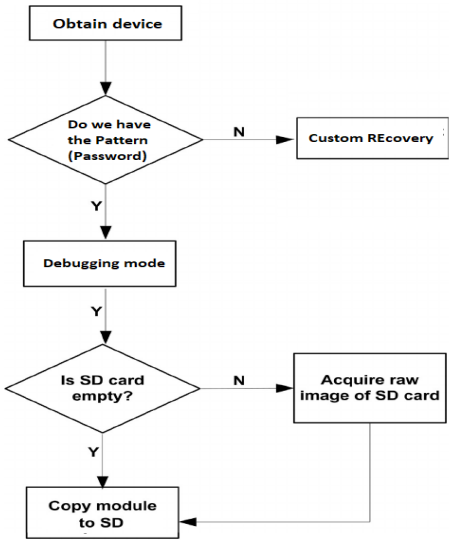

Figure 2. System Architecture

System Implementation

In this research, the data is collected from the powered on evidence smart-phones at the crime scene, based on the Android OS open source forensics tools and develops the integrities of the forensics tool to obtain the digital forensics collecting evidence process.

For avoiding the evidence disappear when powered off, the forensic data can be record by investigators from the smart-phone in time using Java language as the main program and Android provide API development as the forensics system.

After utilizing the proposed forensics system, it will be shown in the computer screen which contains different information like contacts, call logs, photos, videos, music, telegram, whatsapp, viber, instagram for investigator to input the information, as shown in Fig.3.

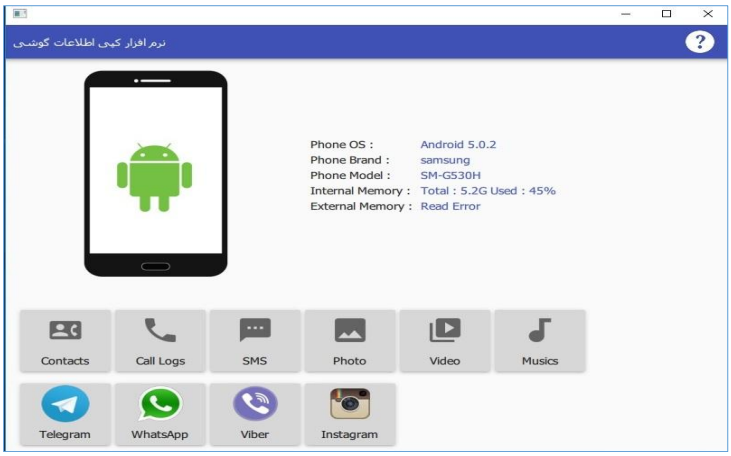

Figure3. Proposed forensic tool

The main features of the software are listed in below:
Display mobile data on a computer (such as installed firmware version, phone model and memory capacity)
Transfer Contact, SMS and Call Log as an Excel file
Easy and effortless transfer of music, movies and pictures to the computer
Transferring files (photos and videos) of social networks such as Telegram, Instagram, Viber, WhatsApp (the text file is also copied to the Watts app)

After installing the forensic software, you can connect your phone to a computer via a USB cable and run the program; here are two general options: (These guides are written in the program help in more detail)
First option: we have (Or we can get) the pattern or password to open the phone screen:

In this option, activate the USB debugging mode on the mobile phone, connect the phone, run the program, identify the phone program and then any file that we want to fit the features of the program can be transferred from the mobile to the computer.
Second option: we have not the Pattern or the Unlock Code:

In this option, the handset is off and Android OS mobile OS should be a version below 5. For each mobile phone model, a custom recovery file (for example, the Samsung S3) is created. This file can be connected to the computer using the USB cable as described in the program guide on the computer. Using the Volume+ Volume- and Home buttons, we bring the phone into Recovery Mode (there's no need to upgrade Android and turn the phone off). Now, we run the program. Identifies the mobile model program, and then we can copy the information from the cell phone into the computer. (In this case, the handset is not turned on and we do not need to know the Pattern or the mobile password at all)

To copy the contact numbers to Contacts, select the storage path. Finally, we give the MySQL information in an Excel file.

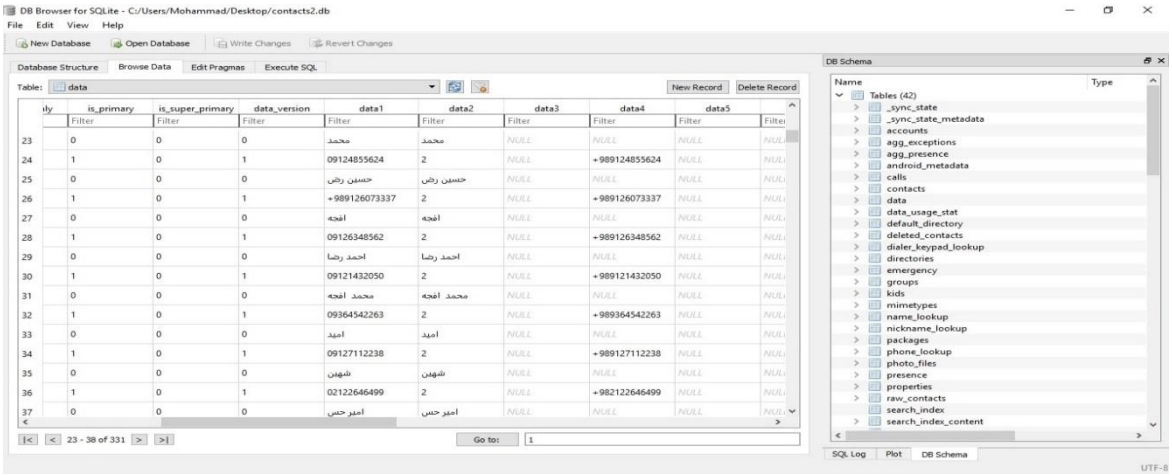

Figure 4. Output Copy of Mobile Phone Numbers

To copy SMS messages into the SMS, we click on the output in an Excel file as below:

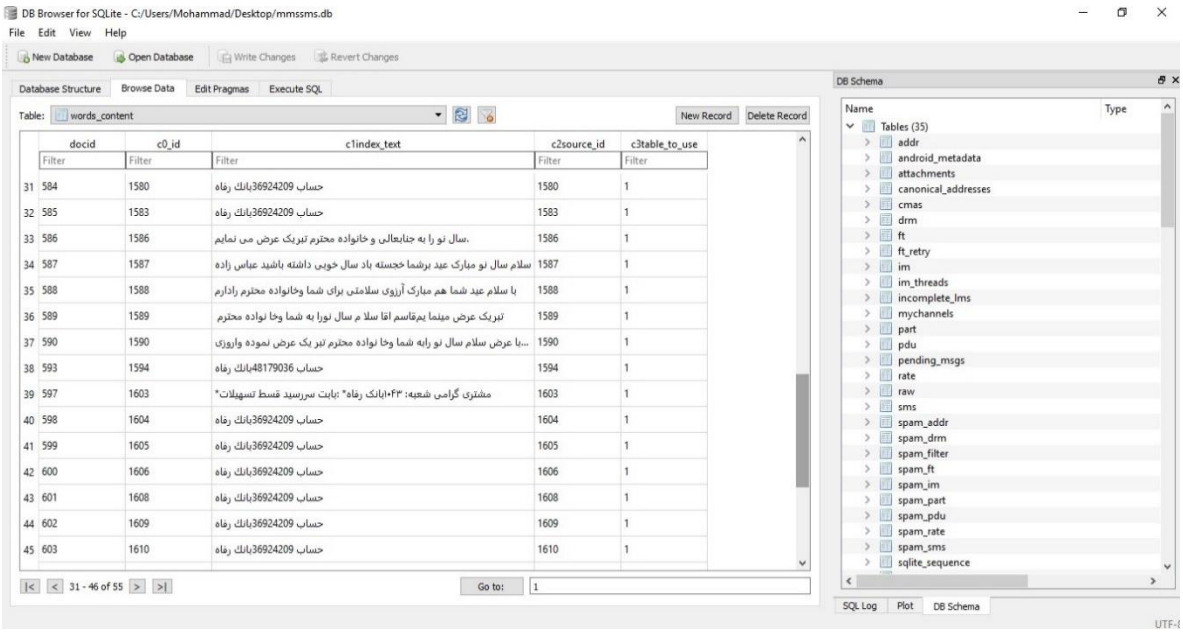

Figure 5. Output Copy of Mobile Text Messaging

Clicking on the Telegram icon to copy telegram files:

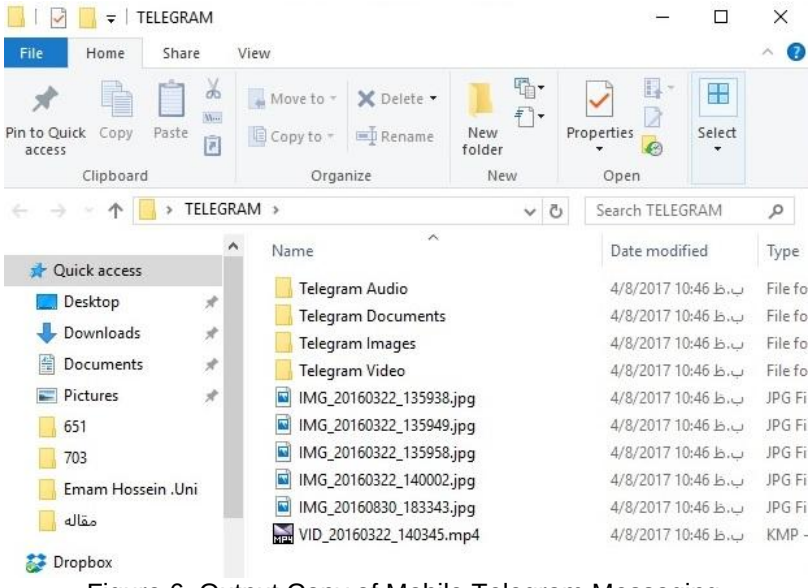

Figure 6. Output Copy of Mobile Telegram Messaging

Other information of the smart-phone can be extracted by the same way as above.

CONCLUSION

In this research, a new forensic tool based on Android OS is proposed to develop the forensic applications. Java language is utilized as the main operating language to design the programs for the crime scene forensic investigators on immediate gathering evidence from the smart-phone at the crime scene.

This tool help investigators to achieve the important information without carried the collected smart-phone evidence on powered off status back to the lab. The approach includes an extra option for collecting the smart-phone information and status in the crime scene and saving the evidences in the SD card immediately.

The proposed method also has an extra option to achieve the forensic information even if we don't know the Pattern or the Unlock Code.

REFERENCES

ADC. USA: International Data Corporation. Available: http://www.idc.com/getdoc.jsp?containerId=prUS42507917 2017].

ATKINSON, T. & LORENZO CAVALLARO, I. 2017. Hunting ELFs: An investigation into Android malware detection.

BAECHLER, S., GÉLINAS, A., TREMBLAY, R., LU, K. & CRISPINO, F. 2017. Smartphone and Tablet Applications for Crime Scene Investigation: State of the Art, Typology, and Assessment Criteria. Journal of forensic sciences, 62**,** 1043-1053.

CASEY, E. 2010. Chapter 1 - Introduction. Handbook of Digital Forensics and Investigation. San Diego: Academic Press.

DEVELOPERS, A. Available: http://developer.android.com/guide/basics/what-is-android.html.

DLAMINI, I., OLIVIER, M. S. & GROBLER, M. M. The smartphone evidence awareness framework for the users. 11th International Conference on Cyber Warfare and Security: ICCWS2016, 2016. Academic Conferences and publishing limited, 439.

NANCE, K. & BISHOP, M. Deception, Digital Forensics, and Malware Minitrack (Introduction). Proceedings of the 50th Hawaii Internatinal Conference on System Sciences, 2017.

PERUMAL, S., NAVARATHNAM, S., VOSSE, C. D., SAMSUDDIN, S. B. & SAMY, G. N. 2017. Comparative Studies on Mobile Forensic Evidence Extraction Open Source Software for Android Phone. Advanced Science Letters, 23**,** 4483-4486.

PETRAITYTE, M., DEHGHANTANHA, A. & EPIPHANIOU, G. 2017. Mobile phone forensics: an investigative framework based on user impulsivity and secure collaboration errors. arXiv preprint arXiv:1706.08048.

ROGERS, M. 2017. Technology and digital forensics. The Routledge Handbook of Technology, Crime and Justice**,** 406.

ROMANOSKY, S. & GOLDMAN, Z. 2016. Cyber Collateral Damage. Procedia Computer Science, 95**,** 10-17.

SITOVA, Z., SEDENKA, J., YANG, Q., PENG, G., ZHOU, G., GASTI, P. & BALAGANI, K. 2016. Hmog: New behavioral biometric features for continuous authentication of smartphone users. Information Forensics and Security. IEEE Transactions on, PP (99)**,** 1-1.

SUNDE, I. M., FLAGLIEN, A., DILIJONAITE, A., HAMM, J., SANDVIK, J. P., BJELLAND, P., FRANKE, K. & AXELSSON, S. 2017. Cybercrime Law. Digital Forensics**,** 51-116.

WILSON, R. & CHI, H. A Case Study for Mobile Device Forensics Tools. Proceedings of the SouthEast Conference, 2017. ACM, 154-157.

WOLVERTON, M. 2016. Digital Forensics in the Library. Nature, 534**,** 139-140.

WU, S., ZHANG, Y., WANG, X., XIONG, X. & DU, L. 2017. Forensic analysis of WeChat on Android smartphones. Digital Investigation, 21**,** 3-10.

YOVINE, S. & WINNICZUK, G. CheckDroid: a tool for automated detection of bad practices in Android applications using taint analysis. Proceedings of the 4th International Conference on Mobile Software Engineering and Systems, 2017. IEEE Press, 175-176.