Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal

Vol. 1, No. 2, September, 2015

Digital Forensics System for Retrieving Contacts on Mobile Phones

Aborisade, D.O.
Department of Computer Science
Federal University of Agriculture Abeokuta (FUNAAB)
Abeokuta, Ogun State, Nigeria.
aborisadeda@funaab.edu.ng

Alowosile, O.Y., Odumosu, A.A. & Adedeji, A.A.
Department of Computer Science
Abraham Adesanya Polytechnic
Ijebu-Igbo, Ogun State, Nigeria.
alowosile78@gmail.com, adesoladapo2000@gmail.com, adedejibdm@gmail.com
+234-805-438-8100

Banjo, O.A.
Department of Computer Engineering
Abraham Adesanya Polytechnic
Ijebu-Igbo, Ogun State, Nigeria.
steadydoo70@gmail.com

***Corresponding Author: alowosile78@gmail.com**

ABSTRACT

Mobile Phones have been observed to be an indispensable tool to every user in the World today, owing to its usefulness and importance. Whenever this device is stolen or lost, the owner feels traumatized and devastated mostly because of the contacts on the phone. In this paper, a two-level digital forensic system is proposed to help retrieve their lost contacts on phone. The proposed architecture was implemented to evaluate its effectiveness. Implementation of the proposed system showed that the proposed system is effective for helping phone owners recover their lost contacts on phone.

Keywords—Digital forensics, Forensics system, Mobile phone, Phone contacts retrieval

Aims Research Journal Reference Format:
Aborisade, D.O., Alowosile, O.Y., Odumosu, A.A., Adedeji, A.A. & Banjo, O.A. (2015): Digital Forensics System for Retrieving Contacts on Mobile Phones. Advances in Multidisciplinary Research Journal. Vol 1, No. 2 Pp 135-140.

1. BACKGROUND TO THE STUDY

The digital age that the World is presently going through is characterized by the application of computer technology as tools to enhance traditional methodologies. The advent of computer systems as a tool into private, commercial, educational, governmental, and other facets of modern life has improved the productivity and efficiency of these entities (Mark et al.,2002).

Maher (2000) reported that the introduction of computers as a criminal tool has enhanced the criminal's ability to perform, hide, or otherwise aid unlawful or unethical activity. Each year, there is an increase in the number of digital crimes worldwide. As technology evolves, software changes, and users become digitally savvy, the crimes they commit are becoming more sophisticated (Maher, 2000). Digital Forensics is an emerging area within the broader domain of computer security whose main focus is the discovery and preservation of digital evidence for proof of criminal wrong-doing and ultimate prosecution of criminal activity. Computer evidence is becoming a routine part of criminal cases with nearly 85% of the current caseloads involving digital evidence (Carol et al., 2007).

*A mobile phone (also known as a cellular phone, cell phone, hand phone, or simply a phone) is a phone that can make and receive telephone calls while moving around a wide geographic area. It does so by connecting to a cellular network allowing access to the public telephone network. By contrast, a cordless telephone is used only within the short range of a single, private base station. In addition to telephony, modern mobile phones also support a wide variety of other services such as text messaging, Multimedia, Messaging, Service, email, Internet access, short-range wireless communications (infrared, Bluetooth), business applications, gaming, and photography. Mobile phones that offer these and more general computing capabilities are referred to as smart phones. Mobile phones have become a very important tool for personal communication.

It is therefore of great importance that forensic investigators have possibilities to extract evidence items from mobile phones. Modern mobile phones store evidence items on SIM-cards as well as internal memories. Mobile Phone Forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device. Mobile Forensics is the science of retrieving data from a mobile phone under forensically sound conditions. This includes full data retrieval and examination of data found on the Sims /USIM, the phone physical memory itself and the optional memory cards* Forensic Science is the use of forensic techniques and values to provide evidence to legal or related investigations (Jansen et al., 2008). Digital forensics is a relatively new science, derived as a synonym for computer forensics, Digital forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for proof of criminal wrongdoing and ultimate prosecution of criminal activity. The process of digital forensics can be broken down into three categories of activity which include acquisition, analysis, and presentation.

(i) Acquisition: This refers to the collection of digital media to be examined. Depending on the type of examination, these can be physical hard drives, optical media, storage cards from digital cameras, mobile phones, chips from embedded devices or even single document files. (Cory and Har, 2011).
(ii) Analysis: refers to the actual media examination, the identification, analysis, and interpretation of items (Cory and Har, 2011).
(iii) Presentation: refers to the process by which the examiner shares results of the analysis phase with the interested party or parties. This consists of generating a report of actions taken by the examiner, artifacts uncovered, and the meaning of those artifacts (Cory and Har, 2011).

1.1 STATEMENT OF PROBLEM

In this information age, a mobile phone is seen as an indispensable asset to every user, an average mobile phone owner finds it very difficult to cope with not being able to make or receiving calls. When such people loose their phones, they feel traumatized not only because they lost their phones but mainly because of the loss of contacts on their phones which adversely affect their communication and transactions. In addition, as mobile devices grow in popularity in everyday life they are often used for digital crime, and when such happen it is always difficult to investigate the occurrence. This paper is therefore intended to design and implement a digital forensics system that will enable a phone owner who lost their phones to easily recover their contacts.

1.2 OBJECTIVE

The main objective of this paper is to propose a two-level based digital forensics system for retrieving lost contacts on phone, through which a phone owner who lost their phones could recover their lost contacts. The remaining part of the paper is organized as follows; Section two discusses the related work. Section three introduced and discussed the system design for the proposed digital forensics system. Section four shows the implementation of the proposed architecture design. Section five gave the result discussion while section six concludes the work.

2. RELATED WORKS

This section discusses a number of reviewed related work in Digital forensics as follows; (Martin, 2008) considered the relevant differences between file systems and databases and then transfers concepts of file system forensics to Database forensics. He reported that databases are inherently multidimensional from a forensic perspective. A notation was introduced to express the meaning of various possible forensic queries within this multi-dimensional context. He also opined that the introduced notation with the multidimensional nature of databases as described, form a map for possible Database forensics research projects. Andrew et al.(2012) conducted forensic analyses on three widely used social networking applications on smartphones namely Facebook, Twitter, and MySpace.

The tests were conducted on three popular smartphones namely BlackBerrys, iPhones, and Android phones. The tests involved 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. Their results show that no traces could be recovered from BlackBerry devices. However, iPhones and Android phones store a significant amount of valuable data that could be recovered and used by forensic investigators (Andrew et al., 2012). In May 2007, a case of child abuse was reported to the hospital where he was receiving treatment for several months. A digital video recorder (DVR) was used to record the events of his maltreatment but unfortunately the recordings could not be found on the device when it was given to the hospital security employees (Wouter, 2008) detailed how the system was examined. His paper also described the steps that were taken to obtain information and how the information was interpreted.

This method used by (Wouter, 2008) could be applied to other similar devices. (Sangjin et al.,2012) proposed a new analysis techniques for fragmented flash memory pages in smartphones. Its paper also demonstrated analysis techniques on the image that the reconstruction of file system is impossible because the spare area of flash memory pages does not exist or that it is created from the unallocated area of the undamaged file system. Carsten et al. (2009) proposed novel methods for cryptographic key identification and presented a new proof of concept tool named Interrogate that searches through volatile memory and recovers cryptographic key used by the ciphers, AES. Serpent and two fish. When the tools are used in a virtual digital crime scene, they simulated and examined the different states of systems where well known and popular cryptosystems are installed. Carsten et al. (2009) experiments showed that the chances of uncovering cryptographic keys are high when the digital crime scene are in certain well-defined states. They also argued that the consequence of this and other recent results regarding memory acquisition require that the current practices of digital forensics should be guided towards a more forensically sound way of handling live analysis in a digital crime scene.

3. MATERIALS AND METHODS

3.1 Proposed System Architecture

The proposed architecture for the Digital forensics systems is as represented in Figure 1. The system operates at two different levels. It has been designed to work both at the level of local server or at the level of remote server (i.e host the database on internet).

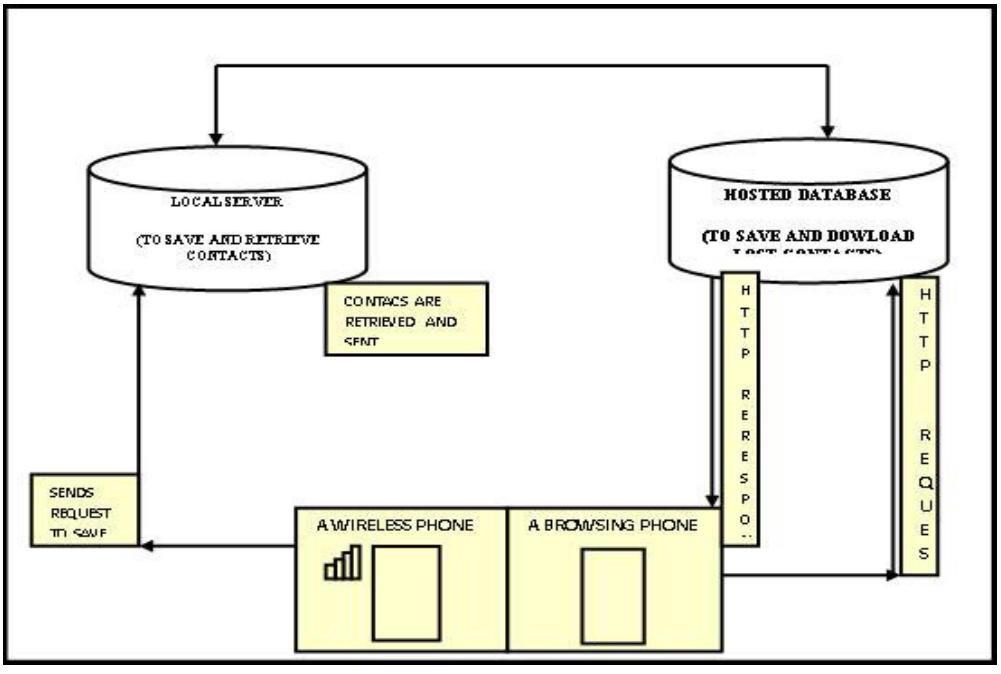

Figure 1: Architecural Framework for the proposed system

Local server: represents the local system where all the phone contacts are originally stored.

Hosting Database: is the component of the framework where a copy of every contacts saved on the local server though a mobile phone is made.

The local server requires a system with Wireless facilities and a wireless phone. The transmission between system and wireless phone work like a local area network where data can be transferred within shortest distance the phone would be able to save contact on this server and at the same time retrieve it back when it is needed, as if the database is hosted on the internet. Any phone with browsing capability and has a reliable network access would be able to save and retrieve contacts when necessary. The wireless and Browsing component represent a typical mobile phone in the forensics system with wireless and browsing facilities. Send request to save serves as a communication link between the mobile phone and the local server database. HTTP request is a component used to make retrieval request of a copy of lost contact possible from the hosted database server on user phone. HTTP response facilitates the request delivery to the user.

4. RESULTS

For the implementation of this research a Computer and a wireless Phone are used. The Phone is used to save names and contacts. While the Computer will serve as the local Server that contains the database where all names and contact saved on the phone will be stored. Wampserver, Java and Netbean were installed on the computer used as the local server. Figures 2,3,4,5 and 6 give the results of the system implementation.

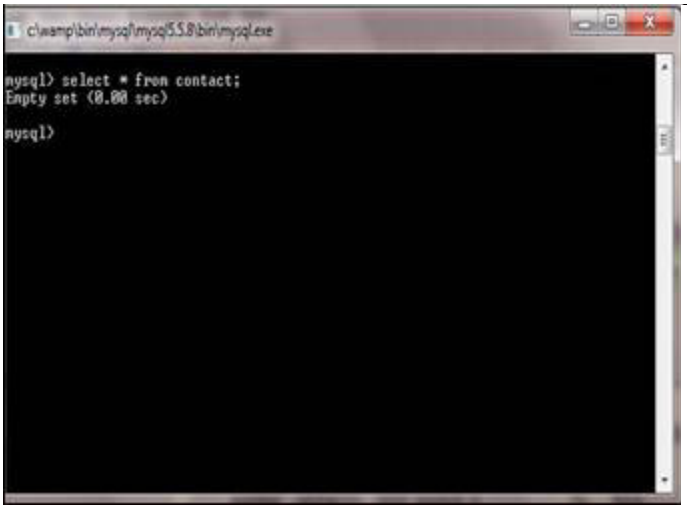

Figure 2: Screenshot showing an empty table on the Server

Figure 3: Screenshot showing how Phone accepts contacts to be saved.

Figure 4: Sreenshot for selecting an option to perform

Figure 5: Screenshot for menu to save or retrieve contacts

Figure 6: Screensho showing retrieved contacts

5. DISCUSSION

In implementing the proposed system, contacts on the phone are intentionally wiped off. When the applications is invoked, all the contacts from the database (Server) are fetched and displayed for the user. Figure 6 shows this by displaying professor as the last contact saved which confirms the last entry before the phone was wiped off. By this the user was able to retrieve all lost contacts. The figure above also showed that all contacts in the server are the same with the ones retrieved by the new Phone which confirmed that the numbers retrieved are correct and that the newly proposed digital forensics system is effective in helping to retrieve lost contacts on user's phone.

6. CONCLUSION AND FUTURE WORK

Mobile Phones can be analyzed to gain insight into the activities of the user to know who they have been speaking or interacting with. This can ultimately provide valuable evidence in prosecuting individuals. This research provided a means to retrieve contacts on lost phones by developing a mobile forensics system. This is so important because mobile phone users encounters the challenge of getting back all contacts on lost Phones, whenever their Phones get lost, the Global System for Mobile Telecommunication service although provides a solution to this challenge of retrieving contacts but it is limited to retrieving lost line. Future research effort would be geared toward improving the system to allow the secure exchange of contacts on the system using Hypertest Transfer Protocol-Secured.

7. CONTRIBUTION(S) TO KNOWLEDGE

This research work has been used to entrench the design of an architecture that was implemented for the purpose of recovering lost contacts at two different levels on mobile phone in digital forensics.

REFERENCES

1. Aborisade,D.O., Alowosile,O.Y., Odumosu,A.A., Adedeji,A.A., and Odunayo,O.(2015). Digital Forensics System for Retrieving Contacts on Mobile Phones. Proceedings of International Multidisciplinary and Interdisciplinary Conference on Science, Technology,Education, Arts, Managements and the Social Sciences (ISTEAMS 2015), University of Benin, Benin, (pp307-312): The Creative Research and Technology Education Networks.
2. Andrew M., Ibrahim B and Noora Al M.. (2012). Forensic Analysis of Social Networking Applications on Mobile Devices. Elsevier Journal of Digital Investigation 9 , 2012 S24–S33.
3. Carol T., Barbara E P. and Deborah F. (2007). Specifying Digital Forensics: A Forensics Policy Approach . Digital Elsevier Limited.
4. Carsten M. M., Steffen E., and Thorkildsen A. A. (2009). The persistence of memory: Forensic Identification and Extraction of Cryptographic Keys. Elsevier Journal of Digital Investigation 6, 2 0 0 9 S 1 3 2 – S 1 4 0.
5. Cory A and Har C.(2011). Digital Forensics with Open Source Tool, Elsevier Inc. ISBN:9781597495875. 4
6. Jansen W., Delaitre A. and Moenner L.(2008). Overcoming Impediments to Cell Phone Forensics, Proceedings of the 41st Annual Hawaii International Conference on System Sciences,, pp: 483-483, ISBN: 978- 0-7695-3075-8.
7. Maher, H. (2000). Online and Out of Line: Why is Cybercrime on the Rise, and Who's Responsible?" Article dated December 17, 2000 http://abcnews.go.com/sections/us/DailyNews/cybercrime_000117.html
8. Mark R. M., Clint C. C. and Gregg G.G.(2002). An Examination of Digital Forensics Models. International Journal of Digital Evidence..Vol.1, pp:1-10.
9. Martin S. O. (2008). On Metadata Context in Database Forensics. Elsevier Journal Digital Investigation. Elsevier 5 (2009) 115–123 . Page 1 1 5 – 1 2 3.
10. Sangjin L, H. C. and Jungheum P. (2012). Forensic Analysis Techniques for Fragmented Flash Memory Pages in Smartphones. Journal of Digital Investigation 2012 Page 1-10.
11. Wouter S. van Dongen. (2008). Case Study: Forensic Analysis of a Samsung Digital Video Recorder. Elsevier Journal of Digital Investigation 5, 2 0 0 8 , 1 9 – 2 8.