Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Optimistic Approach for Implementing a Forensic Systems for Android Devices based on Cloud

Richa Singh, Saurabh Gupta
CSE Dept., PSIT, Kanpur
Uttar Pradesh, India

Abstract- During these days the demand of the smart phones continues to grow, due to this a lot of security problems are arises. Cybercrime is very familiar.Cybercrime increases dramatically in recent years and investigators have been facing the problem of acceptability of digital evidence on smart phones. To remove this problem, we must collect evidence by digital forensics techniques and analyse the digital data, or recover the damaged data in the phones. Our design is based on guidelines from the National Institute of Standards and Technology to ensure the effectiveness of digital evidence and credibilityof the evidence on judicial review. The alteration of original evidence source in smart phones are minimized by using cloud computing platform which select proper forensic software to storethe forensic results.

Keywords- Digital Forensic, Mobile forensics, Smart phone, Android, Cloud computing.

I. INTRODUCTION

Due to the rapid development of information technology it brings people convenience in their daily lives and work. Despite the lagging economy, smart phones remain in the market [1]. In 2011 worldwide smart phone sales are 58% increased from 2010.With the trend, smart phones become very popular in daily life and work, and it has become an indispensable tool. Crime issue is considerable when it comes to the utilization of smart phone technologies. People decide to take the actions through smart phones; it also raises the security issue. Therefore, smart phones become an important item in digital forensics. Digital forensics provides the technical skills to collect evidences. Smart phone forensics acquires digital evidence sources from the SIM cards, smart phone memory,and SD card in smart phones. The purpose of this research is to design and implement a forensic system which acquires the digital evidence ofAndroid smart phones. Our research is based on the NIST guideline for the smart phone forensics [2].

II. METHODOLOGY

1) Digital Forensics:

Digital forensics[3] is the science of obtaining, preserving, analysing, and documenting digital evidence from electronic gadgets such as tablet PC, server, digital camera, PDA, fax machine, smart phone, and various memory storagedevices. The purpose of digital forensic is to investigate the digital evidence whichmight be involved in computer intrusion,unauthorized access, data alteration etc.
Digital forensics can be performed in fourdistinct phases of collection, preservation, analysis, and presentation[7] shown below.
The four phases are described as follows:

A. Evidence Collection/Acquisition:

This phase gathers physical data having potential digital evidence and establishes a copy of information according to the defined set. For Example, use of Forensic tool to create image on disk in computer.

B. Evidence Preservation:

This phase is focus on the preservation of digital evidence in reliable and verifiable manner.

C. Evidence Analysis:

This phase focus on the addresses of extraction of digital information.

D. Evidence Presentation:

This phase focus on analysing the result and after that document the result for present the digital evidence.

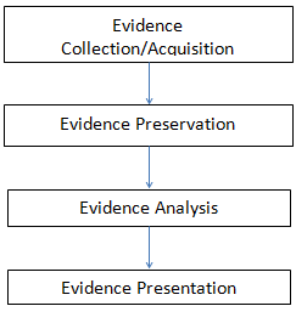


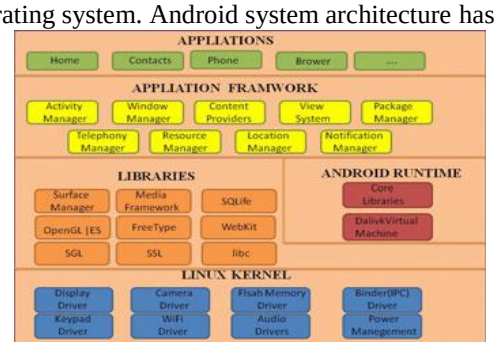
Figure 1: The Phases of Computer Forensic

At present, the analysis of digital evidence must depend on the forensics tools such as the Forensic Toolkit (FTK)[Garber L. ,2001] .Forensic Toolkit are commercial software that are more expensive for the small enterprises or individual.. The typical goal of an investigation is to collect evidence using generally acceptable methods. The final forensic report must include[Volonino L.et all,2006]

(1) Where the evidence was stored?
(2) Who had obtained to the evidence?
(3) What had been done to the evidence?

2) Android Forensics:

Due to the advanced IT technological development, people rely heavily on smart phones as a result the selling of mobile phones was decreased in 2012 as compared to smart phones. Android [10] is an open source operating system for smart phones, which is based on Linux operating system. Android system architecture has four main levels.



The lowest level of Android architecture is Linux Kernel. The second level is Library and Android Runtime, and the third level is the Application Framework, which is designed to simplify the reuse of components so that developers have full access to the same framework that APIs used by the core applications. The highest level is the Application. The top-level Application is shipped as core programs with the Android handset and it includes a bundle of programs such as the contact manager, web-browser, an email client, calendar, SMS program, etc. Digital evidences on smart phones might come from three areas:

A. SIM (Subscriber Identity Module): A SIM is a special type of removable smart card that contains essential information about the subscriber. Forensic tools shall acquire data on SIM, including the International Mobile Subscriber Identity (IMSI), last numbers dialled, or SMS messages.

B. Memory chip: Micro SD card are used to store images, music, and applications.

C. Handset: Android handset provides most valuable source of evidence. The International Mobile Equipment Identifier (IMEI), contact numbers in the Phone book, geo-referenced data, numbers called, SMS sent, web browser history etc., all these are obtained with the forensic software.

3) Cloud Computing:

NIST [Mell P., 2011] defines cloud computing as

"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g. networks, server, storage applications, and services) that can be rapidly provisioned and released with minimal management afford or service provide interaction". Cloud computing automatically provides service according to user's need while it doesn't require user to know where his/her data stores over cloud platforms.

Essential Characteristics	On-demand self-service Broad network access Resource pooling Measured service
Service models	Software as a Service Platform as a Service Infrastructure as a Service
	Private cloud

Deployment models	Community cloud Public cloud Hybrid cloud

III. THE PROPOSED FORENSIC SYSTEMS

There are three approaches that process the forensic evidence to collect the evidence from the smart phone. We have implemented two approaches, one is based on the memory card, the other is based on cloud computing.

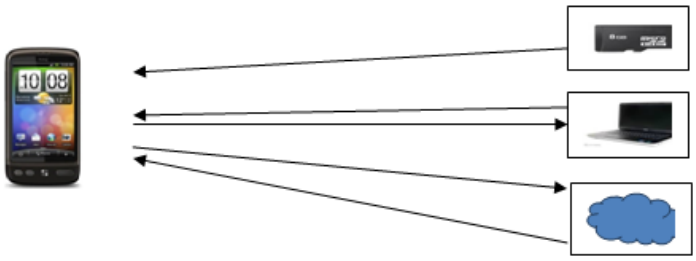


Figure 2: Three approaches for Android forensics

The first approach is to use the memory card, such as SD card or micro-SD card to store the developed forensics tools. The flowchart of this approach is as follows. At crime scene, when forensic investigators receive the smart phones, first record external appearance status of smart phones (such as through text, sound recording or taking pictures recorded phone screen state), and then check whether a SD memory card was mounted in this particular smart phone by operating the phone. If a SD card was originally mounted, then the investigator shall select un-mount option to process the digital forensic of memory card using some computer forensic tools .The smart phone forensics by using the forensic SD card that mounts on the smart phone when the smart phone didn't mount any original user SD card. When the smart phone had no SD card mounted, the investigators would mount the forensic SD card, in which contained in the forensic tools in the SD card, to collect volatile digital evidence. After the investigation at the crime scene, the collected evidence will be stored in the SD card.

Investigators need to select the options of forensic digital evidences and forensic report will be saved to the SD card, such as browser, records, communications records, newsletter, etc. Forensic investigators must returned to forensic lab, and then through process the SD card which stored the forensic evidence collection document file on a Linux computer, in order to inspect the collected evidence statements.

When cloud computing environment is available, we will download forensic software from the Google Cloud Service, without using memory card for fetching software. This will require a network connection from the targeted smart phone to the Google Cloud Service, but it has the benefit of large storage space with high analysis power.

It requires forensic examiner having a Google account while executing the forensicsoftware. According to NIST forensic procedure, it needs to establish forensic files, and forensic examiner must key in the name and date. If the date is incorrect, press the "Data Error" button to correct the date, and then key in the account ID and password to begin forensics.Enter Start; it begins with inner-mobile data acquisition choice which includesphone status, SIM card status, and system log files. Forensic examiner chooses options above and then the acquisition begins with chosen options.Forensic software in this study provides cloud and mobile terminal reporting. Cloud reporting presents reporting through browser and Google Docs.

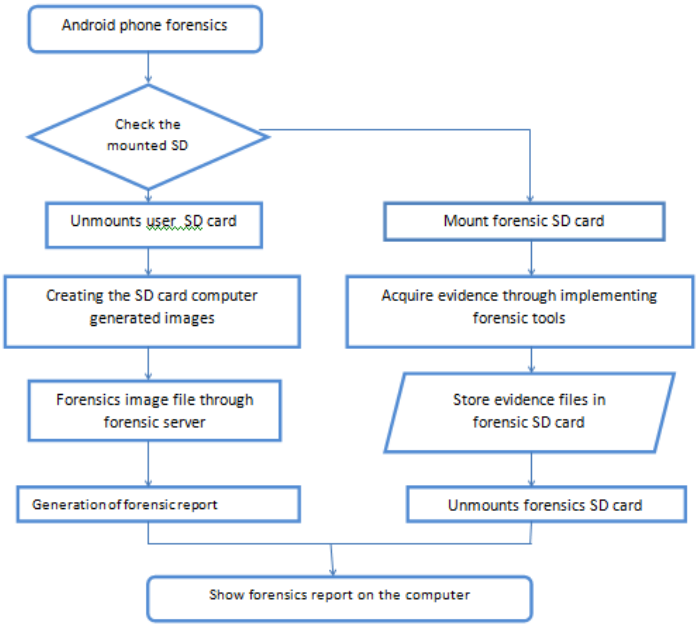


Figure 3: System flowchart of the Android forensics with memory card

Fig. 4Create Forensics File

Fig.5Digital Evidence Collection

IV. CONCLUSION

In recent years, the numbers of cybercrime case are growing due to the advanced network functions and computational powers. In this research, we design and implement forensics systems for the Android phones based on memory card or cloud computing. Our designfollowed on NIST proposed forensics process andforensic software was written with Java languagefor the crime scene forensic investigators ongathering evidence from the on-site smart phone.Future research will on creating a better forensicreporting and gather GPS-related data on the smartphone.

ACKNOWLEDGEMENT

This work was supported by Assistant professor Mr.Saurabh Gupta. I would like to thank them for his guidance and help.

REFERENCES

[1] Garner, "Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 per cent Year-on-Year; Smartphone Sales Grew 74 Per cent," Gartner, Inc., August 11, 2011.
[2] W. Jansen and R. Ayers, Guidelines on Cell Phone Forensics, NIST SP 800-101, May 2007.
[3] E. Casey, (ed.) Handbook of Digital Forensics and Investigation, Academic Press, 2010.
[4] S. Garfinkel, Digital Forensics Research: The Next 10 Years, Digital Investigation, **7** (2010).
[5] ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence (DRAFT), 2011
[6] SWDGE, Digital & Multimedia Evidence Glossary,Version: 2.2, The Scientific Working Group on Digital Evidence (SWGDE), November 2007.
[7] A. Jones and C. Valli C, Building a Digital Forensic Laboratory. Elsevier, Inc., 2009.
[8] L. Garber, Computer Forensics: High-Tech Law Enforcement, IEEE Computer, **34** (1) (2001), 202-205.
[9] L. Volonino, R. Anzaldua, J. Godwin, and G.C. Kessle, Computer Forensics: Principles and Practice, Prentice Hall, 2006.
[10] Android developers. http://developer.android.com/.
[11] P. Mell and T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145 (Draft), January 2011.
[12] NIST, Smart Phone Tool Specification, Version 1.1, April 2010.

