Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.4 No.2, 2015, pp.1-5

DOI: https://doi.org/10.51983/ajcst-2015.4.2.1758

Proposed Methodology for Smart Phone Forensic Tool

Mohammad Junaid, Jai Prakash Tewari, Rajeev Kumar and Abhishek Vaish
MS(Cyber Law & Information Security), Department of IT, Indian Institute of Information Technology Allahabad, India
E-mail: smj165@yahoo.com, jai110990@gmail.com, rajiv6795@gmail.com, abhishek.infosec@gmail.com
(Received 3 June 2015; Revised 29 June 2015; Accepted 25 July 2015; Available online 6 August 2015)

***Abstract* - It has been found that no such tool is available that uniformly support image acquisition, analysis and recovery from different smart phone (regardless of their make, model, OS and its version). Research aim is to understand smart phone forensic tools feature, limitation, usability and proposing the generic methodology for smart phone forensic tool. Explosive development of smart phone, variety of OS, its version adds the complexity to tool developer and forensic professional as well. It's nightmare for digital forensic professional to get expertise on different available forensic tools. The factor shows the urgent need of a standard /generic methodology for smart phone forensic tool. This will help to resolve the interoperability and limitation found on different tools on phone to phone, case to case basis. The Proposed methodology will reduce the total time required for investigation by professional, reduce the tool ownership cost, and improve the professional expertise by just focusing on few tools.**
Keywords: **Smart phone Forensic, Digital Forensic, Digital Evidence, Internal Memory, forensics tool**

I. INTRODUCTION

Now-a-days, the Smart phones are indispensable piece of our day to day lives and these are utilized in view of their improved functionality e.g. Audio/Video calling, web access, support to wide range of application (free and paid), utilities like- WhatsApp, Viber, VPN, games, GPS location, high storage capacity, portability, enhanced security features, increased battery life, enhanced inbuilt camera quality, and pleasant interface. [1]According to International Telecommunication Union (ITU) cellular subscriptions increasing, this is expected to attain almost 7 billion at the end of 2014.

With the evident increase in its use, Smartphone has become integral part of our daily life and technological boon to current generation. Same time, this technology is being targeted and misused by bad guys (attacker, criminal) to carry out criminal and malicious activity. Hence, it became the prime focus/attention of the security authorities, forensic analyst, legal agencies and government agencies. Involvement of these authorities ensure the fruitful and secure use of this technology for betterment of society .A critical information of scientific worth in light of messages, call-history, geo locations, contact numbers, notes, voice records, web history, photographs, datebook occasions, SMS, MMS, GPS guides, perusing history and phone message recording is critical for measurable experts.

As there is excessive use of the smart phones, the personal, social and National security issues have been expanded [Use of Technology in Mumbai Taj Hotel attack]. The smart phone forensic are used to extract/produce the proofs for the court and other concerned authorities. Chain of custody and data integrity should be maintained to ensure the admissibility of evidence in the court of law.

Below are the some limitation/issues observed during comparative study of Smartphone forensic tools.

a. Mass production of forensic tools with lack of standardization in their development. This adds complexity and confusion in finding the right tool for use.
b. Anti forensic tools add one more layer of complexity.
c. Mass production of mobile/smart phone.
d. Diversity in OS and application used by these devices.
e. Types of Data created, maintained , shared and used in these phones.
f. Types of memory used in these phones to store data.
g. Interoperability and supporting capability of forensic tools with different types of Smartphone's.

II. LITERATURE REVIEW

There are lots of limitations in current available smart phone forensic tool. Some tool worked effectively with only one smart phone but not for others smart phone. These are the key points to be considered while developing smart phone forensic tool :a)Generic b)Usability c)Accuracy d)Backup[2].The researcher worked on demo/trial versions of four widely used mobile forensics tools namely, *Oxygen Forensic Suite*, *Paraben's Device Seizure*, Mobile Internal Acquisition Tool, and *MOBIL edit! Forensic Lite* in extracting data from a Nokia E5-00 Smartphone. These tools were not able to find out complete artifacts from this phone and none of them were able to retrieve all deleted information. Neither GPS nor communities applications logs were extracted by these tools [3].

One of the main challenge of investigator is to recover the data from mobile .There are so many anti forensic applications for smart phone, that are freely available on internet, that destroy, hide and counterfeit Data. No professional smart phone recovery tools such as "Device

Seizure and Oxygen Forensic Suite" were able to detect the evidences[4].Data recovery is an important part of forensic, because it helps to extract potential evidences. Data Recovery is possible from deleted file but not from erased file in the file system .The smart phone of Android OS file system is yet another flash file System 2 (YAFFS2) located in directory "fs/yaffs/". At the last researcher suggested that there is still scope of recovery software tool and process methods to recover all evidence from file system [5].This paper presented quantitative analysis technique to measure and evaluated smart phone forensic tools "UFED Physical Pro 1.1.3.8 and XRY 5.0". To compare the tools, calculated margin of error and confidence Interval (CI) based on the proportion of successful extractions. On the basis of CI and MoE factors calculation, the result should help an investigator to select a better tool for a specific investigation [6].The research shows how the smart phone forensic is distinct from other digital forensics and then moving on to potential evidences, to enlighten the development of the digital forensics process model for Smart phones, compares digital forensic methodologies, and finally proposes a systematic Smartphone forensic investigation process model and discuss about the evolving use of cloud that enables to hide the presence of data from mobiles into web[7].

III. PROBLEM DEFINITION

Based on literature review and comparative study of different Smartphone forensic tools, the research found that there is no generic forensic methodology available which can acquire, analyse, and recover evidence from most of Smart phones. This creates challenging difficulties for forensic professional to know and find out the most suitable tool for a particular case. If a correct tool is not selected, then result may not be admissible in the court of law or it may not produce the desired result. Below is the diagrammatic and mathematical representation of problem.

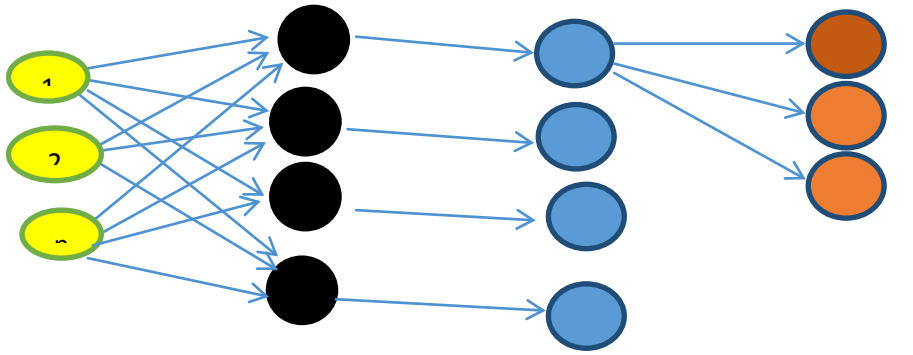

Fig. 1 Relationship between Tools, Smart Phones, OS , and OS Versions

T1=P1*M1*O1*(V1+V2+V3….+Vn)+P2*M1*O1*(V1+V2 ..+Vn)+…..+Pn*M1*O1*(V1+V2+….+Vn) …..(1)
T2= P1*M2*O2*(V1+V2+V3….+Vn)+P2*M2*O2*(V1+V2…..+Vn)+…..+Pn*M2*O2*(V1+V2+….+Vn) ….(2)
Where, T=Times,P=Tools,M=Mobile,O=Operating system,V= OS Version
Tn= P1*Mn*On*(V1+V2+V3….+Vn)+P2*Mn*On*(V1+V2 …..+Vn)+…..+Pn*Mn*On*(V1+V2+….+Vn) ….(N)
Add all above equation(1),(2)…(n)
Total Time Taken (T)= T1+T2+T3+……..+Tn

IV. RESULTS AND FINDINGS

The entire research is summarized in two parts, "Part1"- that is the comparison of various mobile forensic tools- in order to understand the diverse functional capacity of various tools and also to examine the extent of its capability in terms of platform compatibility by conducting various experiments depicted in 4.1.2."Part 2"- of research summarizes a framework that could be utilized by practitioner in order to overcome the problem of time constraint and diverse resource requirement.

A. Part 1

1. Comparison of Tools

For the purpose of this research forensic tools- iPhone Analyzer, Oxygen Forensic® Suite, Mobiledit, parabane's device seizure, phone forensic express ,bitpim,TULP2 were used. But because of limitation (free availability and licensing issue) , it was possible not able to include all mentioned tools in the study and testing. Tools iPhone Analyzer, Oxygen Forensic® Suite, Mobiledit were finalized for the features study. Out of these tools we were able to download and install the Mobiledit only. Mentioned tool was downloaded and installed on the Windows OS version 7. Three different Smart phone-named Samsung S-Duos, Redmi1S, iphone 4 were used for experiment with Mobiledit. Phones were connected using data cable with tool and recorded the result (print screen). [8],[9],[10]The detailed Comparison between the above tools has been shown in the table I.

TABLE ICOMPARISION OF TOOLS, PLATFORMS & ITS FEATURE

S.No.	Tools	Remarks	Platforms	Features
1	iPhone Analyzer	Free	iOS 2, iOS 3, iOS 4 and iOS 5 devices	iPhone Backup Browsing, Native file viewing (plist, sqlite, etc), ssh access for phones (beta),Reports, Restore files, Recover backups,examine address book, sms, find and recover passwords, Export files to local filesytem, IOS6 is only partially supported (several known problems)
2	Oxygen Forensic® Suite	Paid	Android OS ,Apple iOS ,Windows Phone ,Blackberry & Symbian OS ,Feature phones (Nokia, Motorola, Samsung, Sony)	Phonebook Calendar , Calls/Event Log, Automatic deleted calls recovery, Messages , Automatic deleted messages recovery , File Browser with the device files , Passwords , WiFi , Applications , Social Networks, Messengers. Productivity Apps, Web browsers Navigation apps. Contacts, Device Backups import, SQLite Database Viewer , Deleted data recovery in SQLite Database Viewer , Apple Plist Viewer , Blackberry IPD Viewer , Nokia PM Viewer , Device Data Reports , Advanced search through phones database
3	Mobiledit	Free	WINDOWS, APPLE, BLACKBERRY and SYMBIAN OS SMARTPHONES	Sim clone, Backup, Import, Export, Report generation, Call logs, Message logs, Photo Viewer, Forensic report

2. Analysis based on Experiments

In this experiment, Mobiledit tool was used with three different Smartphone, their result are shown below:

1. Samsung S-Duos(Android OS, v4.0 (Ice Cream Sandwich), Qualcomm MSM7227A Snapdragon, 1 GHz Cortex-A5) , problem detected are -unable to detect the OS version, no artifacts found such as message details, call logs, photos, videos, apps, location, chat history, etc.

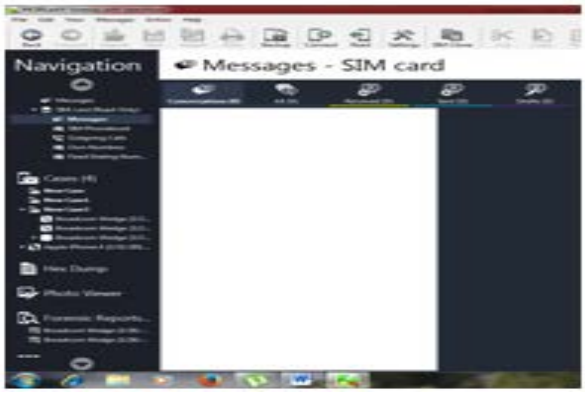

Fig.2 No message detail of phone found by tool

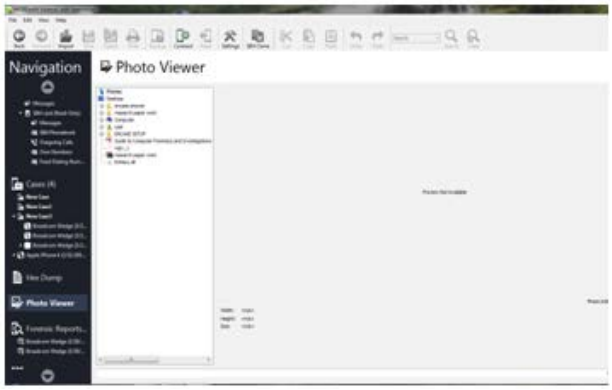

Fig.3NoArtifacts found

2. Redmi 1s (Android OS, v4.3 (Jelly Bean) Qualcomm MSM8228 Snapdragon 400, Quad-core 1.6 GHz Cortex-A7), problem detected are - unable to detect the phone, Operating system & version .

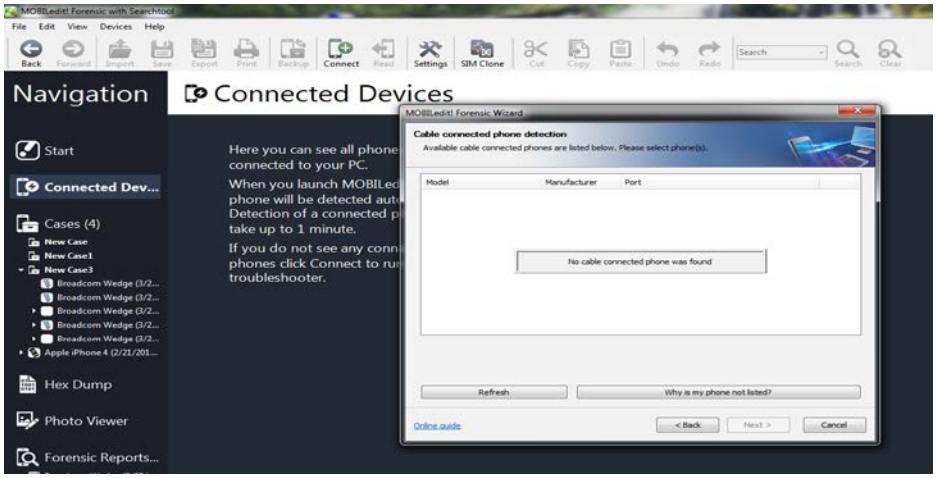

Fig.4 Unable to detect Redmi 1s mobile

3. Apple iphone4 (iOS 4, Apple A4, 1 GHz Cortex-A8) , successfully detected the phone , its OS and version , but unable to recover deleted apps, contact numbers, message, chat history, etc.

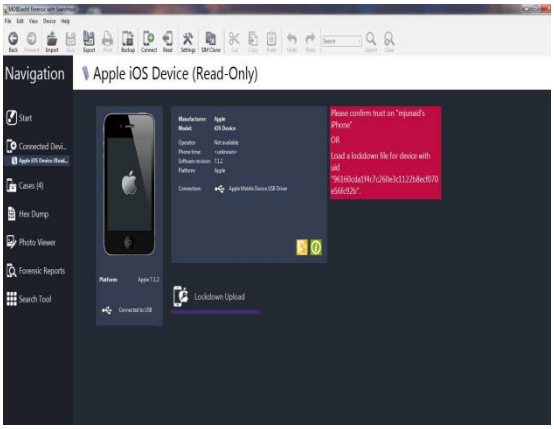

Fig.5Apple iPhone4s detected with tool

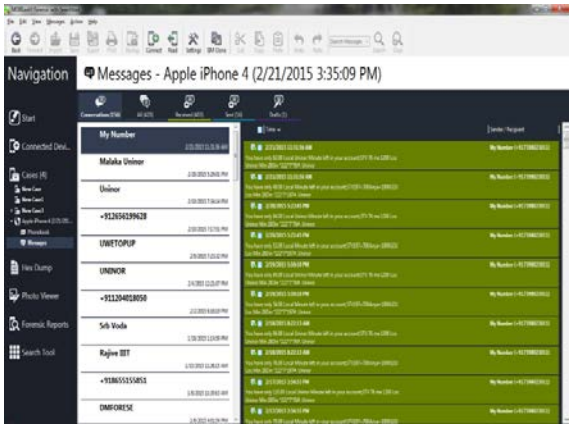

Fig.6 Message extracted from iPhone4s

B. Part 2 Flow Diagram for proposed Methodology

Given approach is to widen the detection, and support for wide range of Smartphone, this feature will help in reducing the requirement of different tools and add other related benefits. This can be accomplished by adding a Database to the forensic tool. Each time a new Smartphone is attached to tool, respective OS and its version is checked, if it's not supported currently, automatically these requirement will be installed and updated in the Database.

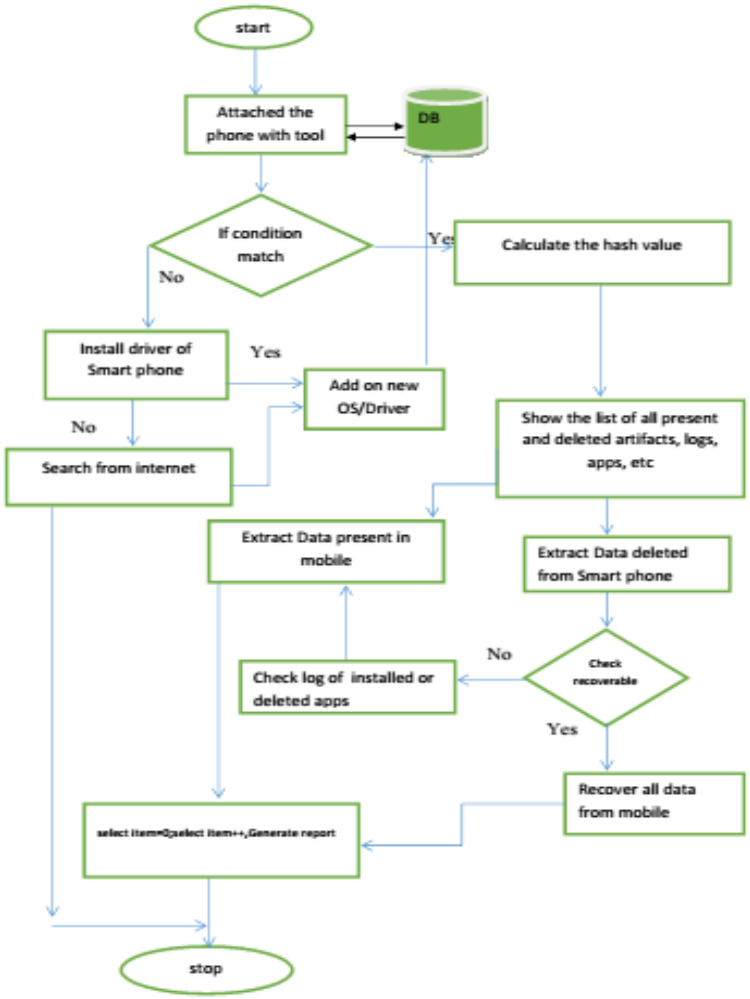

Fig.7 Proposed methodology

Below steps describe the functionality of proposed methodology in figure 7.

Step 1: Start
Step 2: Attach the Smartphone with tool.
Step 3: Tool checks the Phone, OS, and version with its data base. In case of match go to step 6, otherwise step 4.
Step 4: Download and install the driver on the tool database from the Smartphone, go back to step 3 otherwise steps 5.
Step 5: In case phone hardware is detected but unable to fetch operating system & version information, try to search from Internet and download and install on database (if found), go back to step 3 otherwise step 11.
Step 6: Calculate the hash value of image to maintain integrity of acquired image and increase possibility of being acceptable in court of law.
Step 7: Show the list of all artifacts deleted or present in Smartphone such as Apps, Message, call detail, contacts, e-mail, location, images & video.
Step 8: Extract the artifacts which are deleted, retrieve the deleted artifacts, if not possible then check Smartphone logs to know and understand applications/anti forensic tools used for deletion/hiding of the artifacts . This information can be used for further action.
Step 9: Extract all present artifacts from Smartphone and should support filtering of extracted data for further analysis and use.
Step 10: Generate a complete report of Smartphone.
Step 11: Close.

C. Validation

As shown in the equation, P1, ...Pn (multiple tool) has been replaced with P (single tool) and V1,.....Vn (different OS version) with V. Hence it is reduced the total time of the process.

Now time taken is reduced on this manner

P=P1=P2=P3=…=Pn and

V=V1=V2=…….=Vn,O=O1=O2=…=On,;

Now,

Total

Time=P*M1*O*V+P*M2*O*V+P*M3*O*V+P*O4*V+…….+P*Mn*O*V

V. CONCLUSION AND FUTURE WORK

The research paper has focused on comparison of several professional smart phone forensic tools and pin pointed the current problem as requirement of different forensic tools, effort, professional expertise, and time to find the artefacts in Smartphone forensic investigation.

Research proposed a generic methodology for Smartphone forensic tool. It will help professional to overcome from identified limitation in the paper. In proposed methodology tool will be attached with a Database. The Database will have all OS and drivers installed on it , if tool detect new OS or its version , this can be downloaded from phone itself or from Internet on the Database to expand the support and eliminate the limitation. Future research can work on the implementation of the proposed methodology and necessary enhancement can be incorporated based on the outcome of the result.

REFERENCES

[1] Maxwell Anobah, Shahzad Saleem and Oliver Popov: Testing framework for mobiledevice forensic tools: JDFSL V9N
[2] FirdousKausar:New research directions in the area of smart phone forensic analysis*:* International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.4, July 2014
[3] Seyed Hossein Mohtasebi: Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone: International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 651-655 The Society of Digital Information and Wireless Communications, 2011(ISSN 2225-658X)
[4] Ioana Sporea, Benjamin Aziz & Zak McIntyre: On the Availability of Anti-Forensic Tools for Smart phone International Journal of Security (IJS), Volume (6) : Issue (4) : 2012
[5] Chang Xu: Forensic research on data recovery of android smartphone: "Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)"
[6] Shahzad Saleem, Oliver Popov and Oheneba Kwame Appiah-Kubi Department of Computer and Systems Sciences Stockholm University, Forum 100, Isafjordsgatan 39SE- 16440 Kista, Sweden :Evaluating and Comparing Tools for Mobile Device Forensics using Quantitative Analysis
[7] Archit Goel, Anurag Tyagi & Ankit Agarwal, Smartphone Forensic Investigation Process Model: International Journal of Computer Science & Security (IJCSS), Volume (6) : Issue (5) : 2012
[8] http://www.crypticbit.com/zen/products/iphoneanalyzer
[9] http://www.oxygen-forensic.com/en/products/oxygen-forensic-suite/featureshttp://www.cellebrite.com/
[10]http://www.mobiledit.com/