Comparative Evaluation of Mobile Forensic Tools

Chapter *in* Advances in Intelligent Systems and Computing · January 2018

DOI: 10.1007/978-3-319-73450-7_11

6 authors, including:

John Alhassan
Federal University of Technology Minna
40 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Sanjay Misra
Covenant University Ota Ogun State, Nigeria
302 PUBLICATIONS **1,059** CITATIONS
SEE PROFILE

Adewole Adewumi
Covenant University Ota Ogun State, Nigeria
51 PUBLICATIONS **46** CITATIONS
SEE PROFILE

Rytis Maskeliunas
Kaunas University of Technology
94 PUBLICATIONS **164** CITATIONS
SEE PROFILE

Comparative Evaluation of Mobile Forensic Tools

J. K. Alhassan[1(✉)], R. T. Oguntoye[1], Sanjay Misra[2], Adewole Adewumi[2], Rytis Maskeliūnas[3], and Robertas Damaševičius[3]

[1] Federal University of Technology, Minna, Nigeria
jkalhassan@futminna.edu.ng
[2] Covenant University, Otta, Nigeria
ssopam@gmail.com
[3] Kaunas University of Technology, Kaunas, Lithuania
robertas.damasevicius@ktu.lt

Abstract. The rapid rise in the technology today has brought to limelight mobile devices which are now being used as a tool to commit crime. Therefore, proper steps need to be ensured for Confidentiality, Integrity, Authenticity and legal acquisition of any form of digital evidence from the mobile devices. This study evaluates some mobile forensic tools that were developed mainly for mobile devices memory and SIM cards. An experiment was designed with five android phones with different Operating System. Four tools were used to find out the capability and efficiency of the tools when used on the sampled phones. This would help the forensic investigator to know the type of tools that will be suitable for each phone to be investigated for acquiring digital evidence. The evaluation result showed that AccessData FTK imager and Paraben device seizure performs better than Encase and Mobiledit. The experimental result shows that, Encase could detect the unallocated space on the mobile deice but could retrieve an deleted data.

Keywords: Mobile · Mobile phone · Smartphone · Forensics
Digital investigation · Digital evidence

1 Introduction

Currently, one of the major tools in this world is mobile devices with high storage capability that allows mobile device to store huge amount of data, which includes a rich set of personally identifiable data [1]. They have numerous functions and they contain sensitive personal information. The rates of crime committed by mobile devices are increasing daily, and there is a need to have evidence of such in the court of law. In acquiring such evidence, authenticity, integrity and consistency of such evidence must be taken care of in the process of acquisition, [2]. Mobile forensic is used to access erased information from the phone without any alteration and can serve as satisfactory evidence in the court of law [3]. The sensitive personal information in mobile devices is used by the criminals with aid of software on such devices like Operating System (OS) for instance

Á. Rocha and T. Guarda (eds.), *Proceedings of the International Conference on Information Technology & Systems (ICITS 2018)*, Advances in Intelligent Systems and Computing 721,
https://doi.org/10.1007/978-3-319-73450-7_11

Android and iOS. Malware are developed to threaten the personal information on such mobile devices thus, there is a need for mobile forensic to fight such malwares [4]. The process of recovering of digital evidence from mobile devices is referred to as digital forensic. This process does not cause alteration to the information nor the content of such mobile devices, [4]. The use of scientific technique in finding, removing, evaluating data and presentation of evidence that can be used in the court of law is referred to forensics, [5]. In the case of mobile forensic, it includes the techniques trailed in acquiring, analyzing, preserving mobile data and reporting Subscriber Identity Module (SIM) cards and phone memory [6]. The increasing upgrade rate of mobile apps, hardware and operating systems (OS) has made forensic investigating very complex and highly challenging. In addition, researchers of mobile forensics has shown tremendous interests in this area [1]. Therefore, this study gave a comparative performance analysis of the most widely used mobile forensic tools for acquiring erased data from mobile phone. The remaining part of this paper is organized as follows; literature review, mobile phone evidence guide, methodology, results and discussion, analysis, and conclusion.

2 Literature Review

The use of systematic procedures in identifying, analyzing, interpreting, documenting and presenting digital evidence acquired from digital source to carefully plan the events in a criminal offence is known as Digital Forensic Investigation [7]. However, the changes in mobile phones hardware and operating system are due to the difference in functionality of the product designed by the developers. Hence, an effective forensic investigator must understand the phone operating system and hardware in order to develop an efficient and compatible tool [8].

[9] presented a comparative survey for android forensic tools, the paper analyzed different tools and techniques used in android forensic and concluded that forensic tools such as OYGEN are enriced with several features and device supports. [10] performed a comparative analysis for the different commercial mobile device forensic tools with open source mobile forensic tools using the cross-device and test-driven approach. The study concluded that commercial tools are more superior in speed and accuracy during data extraction and analysis than the open source tools. [11] presented a performance measurement analysis on Firefox OS for mobile forensic data Acquisition. The analysis was done on five existing mobile forensic tools. The study concluded that Mobiledit detected the Operating System (OS) running on the mobile device and could also only access pictures from removable memory.

[12] carried out a comparative evaluation on two mobile devices Samsung HTC (Desire 300) and Galaxy (GT-S5300) using five trial versions of mobile forensic tools. In conclusion, Mobiledit and Encase v4.2 provided evidentiary report related to the SIM card while AccessData FTK Imager could not access any information. [10] analysed some mobile forensic tools for retrieving evidentiary information from mobile phones. Two mobile forensic tools were evaluated for reliability and accuracy using two mobile devices. The evaluation result shows that XRY 5.0 perform better than the UFED Physical Pro1.1.3.8.

[12] presented a smartphone forensic on Nokia E5-00 mobile phone. The study was done using four mobile forensic tool on Nokia E5-00 mobile phone. The result shows that the forensic toolkit could not retrieve the erased evidence from the Nokia E5-00 phone. [13] analyzed a smartphone forensic on a crime using WhatsApp messages. Two forensic tools were analyzed and the result concluded that WhatsApp message are not cellular network dependent only but also Wi-Fi or wireless network as well.

2.1 Mobile Phone Evidence Guide

The United States Department of Justice enumerated some mobile phone evidence which act as a set of rules to the United State Secret service on whether to turn or off a mobile device when conducting an investigation [13]. The following are a set of rules guiding the turning on or off of a mobile device:

1. If phone is met "ON", then do not turn it "TURN OFF".
2. "TURNING IT OFF" could activate authentication pattern feature.
3. "NOTE" and "PHOTOGRAPH" all information displayed on the screen.
4. If phone is met "TURNED OFF", do not "TURN ON".
5. Evidence could be altered or modified, when device met "OFF" is "TURNED ON"..
6. "Alert forensic Expert" immediately you get hold of the mobile devices.
7. Call "1-800-LAWBUST" if "No expert is available" they are available 24 h in a week.
8. Ensure you get the manual of the mobile phones.

In order to acquire proofs/evidence from a mobile phone, some recommendations must be adhere to however; there are some pitfalls when using such recommendations. The National Institute of Justice (NIJ) under United States Department of Justice listed some evidentiary document which includes: Calendars/information, phone book, text messages, electronic serial number, password, caller identification information, voice mail, e-mail, memos and web browsers [13] as crucial information in the court of law. In addition, some evidence is considered as miscellaneous such as the mobile phone cables, cloning equipment, applications on Symbian, mobile linux and windows mobile phone may also contain information of evidence value that is not included in the recommendation. Symbian and windows mobile devices are used for executing malware code such as Trojans and viruses that are transferred through the use Bluetooth technology. Therefore, it is important that every malicious application present on mobile phones should be considered as evidentiary value [14–16].

3 Methodology

This section discusses the various materials used for this research study. However, quite a number of existing researches have outlined methodology to adopt for mobile forensics investigation. The materials adopted for this research work are divided into two parts:

1. Hardware devices:
   (a) Fly Fly IQ4503, OS 4.4.2 kitkat, processor 1.20 GHz
   (b) Three SIM cards: MTN, Airtel and Etisalat
   (c) Samsung Galaxy (GT-S5300), OS 2.3.6 Gingerbread, processor 832 MHz ARM11.
   (d) Tecno L3, OS 4.1 Jelly bean, processor 1.0 GHz.
   (e) USB Cable.
   (f) Tecno phantom A7, OS 4.4.2 kitkat.
   (g) HP650 laptop, running on Windows 8, 64 bits OS.
   (h) Tecno M7, OS 4.2.2 jelly beans, processor 1.3 GHz dual core
2. Software devices:
   (a) Mobiledit Forensic v8.6. (Trial)
   (b) AccessData FTK Imager v3.2.0.
   (c) Paraben Device Seizure v7.5.
   (d) Encase v6.18.1

This study focuses on data acquired from both phone and SIM memories using five different operation systems such as Ginger Bread, jelly bean and Kitkat on five android phones. Consequently, in this study external memory was not in use, it was removed from the device.

3.1 Procedure Used for Acquiring Data

For the purpose of this study, five mobile phones were collected from five different users with a newly bought SIMs card inserted to each mobile phone. The five phones were formatted to restore factory settings while USB debugging was enabled for device visibility. The same mobile data evidence was generated on each phones for a five days' duration where the first day data was collected on Tecno L3 using five mobile forensic tools. Tecno A7 was analyzed on the second day using the mobile forensic tools to collect erased data while the third day analysis was done on Fly Fly IQ4503. Tecno M7 was also analyzed on the mobile forensic tools on the fourth day, while Samsung Galaxy Pocket GS5300 was analyzed on the fifth day using the same data created on all the five android phones. However, the generated data were gradually deleted from the mobile devices. The mobile evidence (data) gathered during these five days was transferred via the use of Bluetooth and flash share to the android phones. Table 1 shows the type of data and number of data that were generated.

Table 1. Mobile data evidence creation.

Data	Number of data generated
Pictures	80
Contacts	80
Videos	35
Audio	50
Message	15
Documents	15

Pictures were generated by using the phone camera to take snapshots while others data such as Audio and video files were generated from HTC Incredible S via Flash share. Contacts were inputted manually into the phone memory and SIM card with text messages sent from different phones and from each mobile phone. After the experimental environment was completely setup the airplane mode was enabled to avoid any communications into the mobile phone.

4 Results and Discussion

In this section, evaluation outcome for the different mobile forensic tools when analyzed on the mobile devices are discussed.

4.1 Mobiledit

The evaluation of the five mobile devices on Mobiledit forensic tool gave extremely important information from the SIM card and the mobile phone memory. Examples of information acquired from each mobile phone include International Mobile Equipment Identification (IMEI) number, International Mobile Subscriber Identity (IMSI) for each registered SIMs and Integrated Circuit Card ID (ICCID) or SIM Serial Number for enrolled SIM cards. A typical example of acquired information collected from examining Tecno L3 is shown on Table 2.

Table 2. Information acquired on Tecno L3 mobile phone

Type of Phone	IMSI	ICCID	IMEI	USB port
Techno L3	621300107418186	89234010002214161948	861350022780164	8B56F7AC

Mobile evidence (data) analysed in this study on the mobile forensic tools include: Contacts, pictures, SMS, audio files, video files and documents. This evidence was gradually deleted from the mobile phones and the investigation result shows that Mobiledit could not retrieve the erased evidence from mobile the phone, therefore, it can be said that Mobiledit tool can only be useful to forensic investigator for backing up information before evidence is being tampered with. Tables 3 and 4 shows the evaluation result for Tecno L3 and Tecno phantom A7 respectively.

Table 3 and 4 shows the evaluation result of Tecno L3 and Tecno phantom A7 on the four different mobile forensic tools. It can be deduced from the table that Mobiledit and Encase could not retrieve any of the erased evidence from the mobile device while Access FTK Imager and Paraben device Seizure was able to retrieve some erased evidence such as pictures, audio, video and document.

Table 3. Performance evaluation result of Tecno L3

Mobile data evidence	Encase	Mobiledit	Paraben Device Seizure	Access FTK Imager
Unallocated Space	✓	✓	✓	✓
Audio			✓	✓
Pictures			✓	✓
Video			✓	✓
Document			✓	✓
Contacts				
Messages(SMS)				

Table 4. Performance Evaluation result for Tecno phantom A7

Mobile data evidence	Encase	Mobiledit	Paraben Device Seizure	Access FTK Imager
Unallocated Space	✓	✓	✓	✓
Audio			✓	✓
Pictures			✓	✓
Video			✓	✓
Document			✓	✓
Contacts				
Messages(SMS)				

4.2 AccessData FTK Imager

From the experiment, AccessData FTK imager was able to detect, retrieve, analyze, report findings and save digital evidence (data) from phone memory for court validation. On contrary, this mobile forensic tool could not detect or retrieve data from the SIM card. Figure 1 shows the Interface of the captured Disk Image.

Figure 1 shows that AccessData FTK Imager was able to detect unallocated and slack spaces and could also retrieve all erased data on the phone memory with retrieved data starred to show the duration and date when such data was erased from the phone memory.

4.3 Encase Forensic

In this study, the Encase mobile forensics tool was only able to access the mobile device that is the phone memory and not the SIM card memory. Therefore, information about the SIM card could not be detected using this mobile forensic tool. In addition, the unallocated space on the phone device was detected but could not retrieve any deleted data.

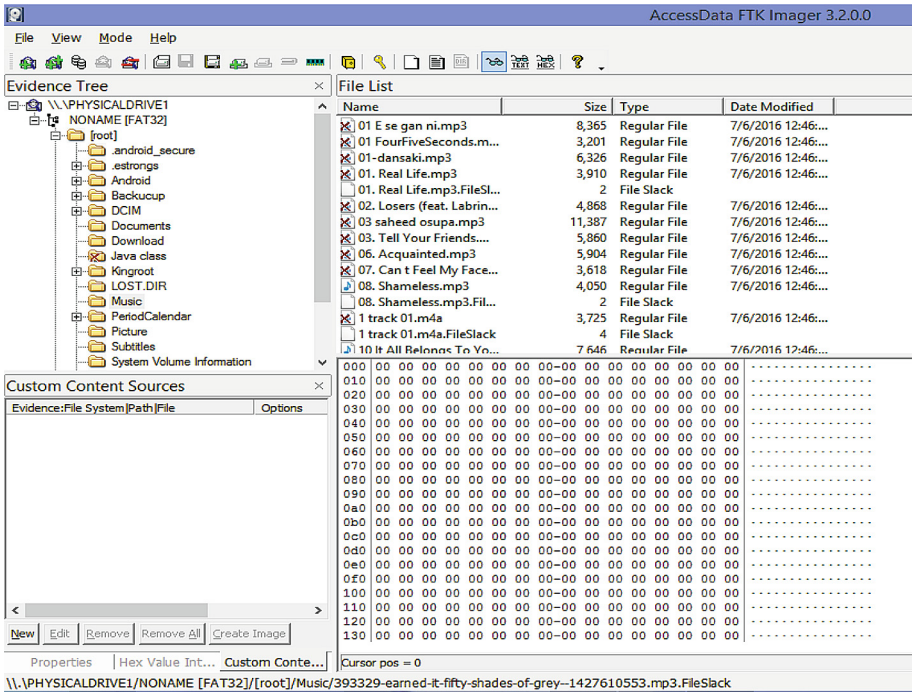


Fig. 1. Interface of the captured disk image

4.4 Paraben Device Seizure Result

Paraben device seizure is an effective mobile forensic tool with effective access to phone memory when connected to an android phone. This tool can access contacts and other multimedia data that was erased from the mobile device.

Mobiledit provided information about the SIM while AccessData FTK Imager, Encase and Paraben Device Seizure could not retrieve any of the erased data. This is because AccessData FTK Imager, Encase and Paraben Device Seizure are used for obtaining data on the mobile device and not to the SIM memory.

This performance analysis shows that none of the mobile forensic tools could retrieve erased contacts and messages on the five different android phones evaluated. However, three of the mobile forensic tools which include: AccessData, FTK Imager and Paraben Device Seizure, were capable of effectively retrieving erased data such as deleted pictures, audios, videos, document, unallocated space and slack space from the mobile phone.

Based on existing literatures, it can be said that there is no forensic tool which has the capability of retrieving all the types of data on different categories of mobile device. Thus, the type of evidence data required from the mobile devices can be determine by the type of analysis to be adopted, and the appropriate forensic tool(s) needed to carry out the analysis.

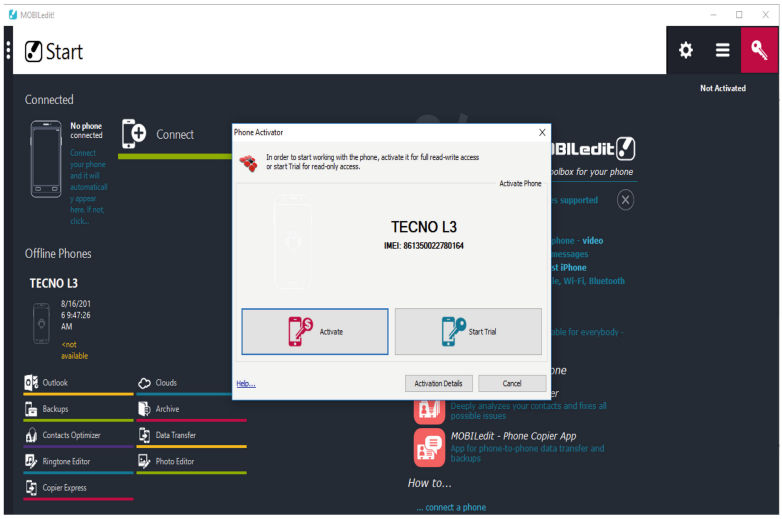
5 Conclusion

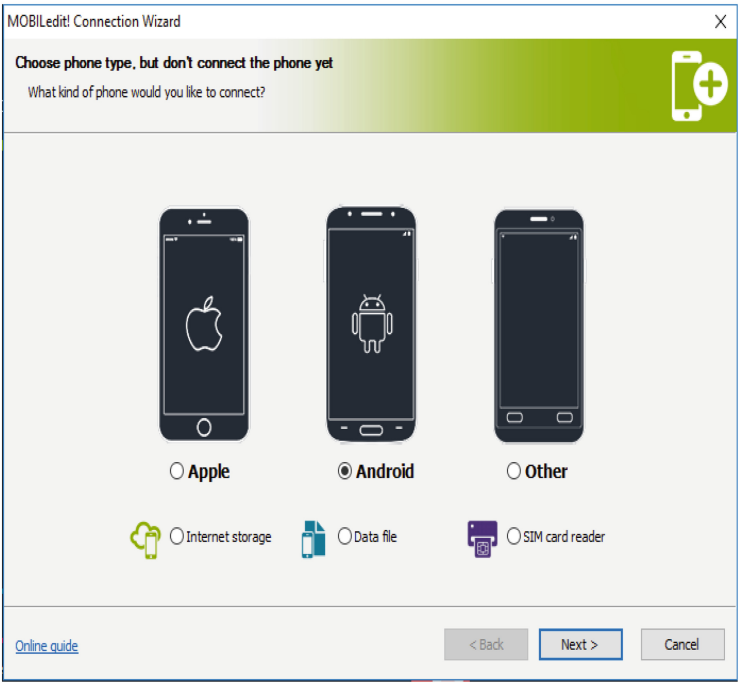
In this research study, a comparative analysis of four mobile forensic tools were carried out on five android phones using different operating systems. The result evaluated from this study shows that AccessData FTK Imager and Paraben device Seizure mobile forensic tools presented a better result than the Encase and Mobiledit. In addition, AccessData FTK Imager and Paraben could retrieve erased data such as videos, music, pictures, document from the phone memory but do not have access to the SIM card. While Encase only indicated that a device was connected no deleted data was retrieved and Mobiledit only showed the status of the phones and some basic information on the SIM card such as IMEI, ICCID, IMSI etc.

Therefore, the need for effective and efficient forensic tools for the purpose of evidentiary data from mobile devices cannot be overemphasized. For a court of law to successful prosecute a suspect who decided to erase all evidence to a crime committed from his mobile device, there must be an appropriate and reliable evidence of the erased data. AccessData FTK Imager and Paraben device Seizure mobile forensic tools can effectively be used for that purpose.

Acknowledgements. We acknowledge the support and sponsorship provided by Covenant University through the Centre for Research, Innovation and Discovery (CUCRID).

Appendix: Some of the Graphic Pictures of the Tool





References

1. Azfar, A., Choo, K.K., Liu, L.: International Conference on Multimedia Tools Applcation. Springer (2016)
2. Lin, C., Peng, C.: Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone. In: Broadband and Wireless Computing Communication and Application (BWCCA), pp. 386–391. IEEE Xplore, Taiwan (2011)
3. Alghafi, J., Martin, M.: Forensic data acquistion methods for mobile phones. 2012 International Conference on Internet Technology and Secured Transactions, pp. 265–269. IEEE, United Arab. Emirates (2012)
4. Chandran, A.: Investigating and analysing malicious events in Android application. Int. J. Eng. Sci. Res. Technol., 1462–1467 (2013)
5. Ntantogian, A., Marinakis, X.: Discovering authentication credentials in volatile memory android mobile devices. Mob. Forensics, 110–117 (2013)
6. Farjamfar, A., Mahmod, U.: A review on mobile device's digital forensic process models. Res. J. Appl. Sci. Eng. Technol. **8**(3), 358–366 (2014)
7. Lai, Y., Lin, A.: Design and implementation of mobile forensic tool for android smart phone through cloud computing. In: Design and Implementation of Mobile Forensic Tool, pp. 196–203 (2011)
8. Kamble, J.: Digital forensic investigation procedure. Int. J. Adv. Res. Sci. Eng. IJARSE **4**, 157–168 (2015)
9. Aniar, R.R., Anshul, K.K., Leesha, A.: Anroid phone forensics: tools and techniques. In: International Conference on Computing, Communication and Automation, ICCCA 2016 (2016)
10. Padmanabhan, R., Lobo, K., Ghelani, M., Sujan, D., Mahesh, S.: Comparative analysis of commercial and open source mobile device forensic tools. IEEE (2016)
11. Osho, O., Ohida, A.: Comparative evaluation of mobile forensic tools. I. J. Inf. Technol. Comput. Sci., pp. 74–83 (2016)
12. Yusof, M., Abdullah, D.: Performance measurement for mobile forensic data acquisition in firefox OS. Int. J. Cyber-Secur. Digital Forensics (IJCSDF), 130–140 (2014)
13. Kubi, S., Saleem, P.: Evaluation of some tools for extracting e-evidence from mobile devices. I. J. Inf. Technol. Comput. Sci., 64–73 (2011)
14. Mohtasebi, A., Dehghantanha, G., Broujerdi, H.: Smartphone foresics: a case study with Nokia E5-00 mobile phone. Int. J. Digital Inf. Wireless Commun. **1**(3), 651–655 (2011)
15. Al Mutawa, N., Baggili, I., Marrington, A.: Forensic analysis of social networking applications on mobile devices. Digital Invest. **9**, S24–S33 (2012)
16. Ahmed, R., Dharaskar, R.V.: Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective. In: 6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government, pp. 312–323 (2008)