I.J. Information Technology and Computer Science, **2016, 01, 74-83**
Published Online January 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2016.01.09

Comparative Evaluation of Mobile Forensic Tools

Oluwafemi Osho*
Department of Cyber Security Science, Federal University of Technology, Minna
E-mail: femi.osho@futminna.edu.ng

Sefiyat Oyiza Ohida
African University of Science and Technology, Nigeria.
E-mail:ohidasefiyat@gmail.com

Abstract—Mobile technology, over the years, has improved tremendously in sophistication and functionality. Today, there are mobile phones, known as smartphones, that can perform virtually most functions associated with personal computers. This has translated to increase in the adoption of mobile technology. Consequently, there has been an increase in the number of attacks against and with the aid of this technology. Mobile phones will often contain data that are needed as evidence in a court of law. And, therefore, the need to be able to acquire and present this data in an admissible form cannot be overemphasized. This requires the right forensic tools. This is the focus of this study. We evaluated the ability of four forensic tools to extract data, with emphasis on deleted data, from Android phones. Our results show that AccessData FTK Imager and EnCase performed better than MOBILedit Forensic and Oxygen Forensic Suite at acquiring deleted data. The conclusion is that, finding a forensic tool or toolkit that is virtually applicable across all mobile device platforms and operating systems is currently infeasible.

Index Terms—Mobile, mobile phone, smartphone, forensics, digital investigation, digital evidence.

I. Introduction

Mobile phone usage has continued on an upward trend over the past few years. For example, in Nigeria, mobile usage increased from a meager 0.02 to 67.68 per 100 inhabitants, from year 2000 to 2012 [1]. Correspondingly, manufacturers of these phones have also continued to expend efforts at increasing the processing capabilities of these phones. Hence, today we have smartphones that can considerably compete with computers in terms of processing power. As a result of this many users, in addition to the traditional usage of mobile phones including making phone calls and sending/receiving SMS, now use mobile phones for browsing the internet, accessing e-mails, and even e-commerce transaction. It has been estimated that mobile banking, going by its expansion which is more than 40 percent annually, should exceed traditional online banking by the year 2020 [2].

The continuous increase in-built functionality of mobile phones, coupled with their portability which has helped their popularity maintain a steady rise, unfortunately has tilted the attention of their manufacturers, as well as developers of the software, away from focusing on integrating necessary security. Thus, recently, mobile technology has become easy targets for attackers. It is not surprising that number of attacks and their sophistication have been heightening [3].

Apart from the threats against mobile phones, they are used for the perpetration of cybercrimes. These crimes include spamming, identity theft, cyber-eavesdropping, malware infections [4], [5]. According to a report by Juniper Networks (as cited by [2]) between the summer of 2010 and spring of 2011, there was a 400 percent increase in malwares targeting android smartphones.

Providing evidence of attack against or via a mobile technology, for research or legal purpose requires due diligence investigation. The processes and procedures involved in the acquisition of needed evidence data are collectively known as mobile forensics. Essentially, forensic investigation is carried out with the aid of tools. However, considering the different types of mobile data and their locations vis-à-vis the fact that there are numerous mobile operating systems, and hardware manufacturers, it is unlikely to find a one-fits-all forensic tool that can acquire every required data from all phones. Willianssen [6] highlighted the need for more sound forensic procedures and tools for extracting evidence. This therefore raises the need to know which forensic tool is most suitable for a specific mobile phone or OS to acquire needed data or set of data, whether the data is OS-handled and altered, user-imported and edited, or used in the phone background by applications [7].

This study aims at conducting comparative evaluation of some existing mobile forensics tools in acquiring data, especially deleted data, from mobile devices. The study would significantly contribute to existing literatures in assisting forensic investigators to determine the appropriate tools to use when carrying out forensic examinations. It could also be useful for individuals who may need to retrieve accidentally deleted data.

II. Literature Review

2.1 Overview of Mobile Forensics

Forensics is the science of investigating and presenting ideas or digital evidence in the court according to the law [8]. Forensics involves procedures, steps, phases or processes in order for the investigation to be successful. According to [9] and [10], the forensics phases include preparation and planning, accessing crime scene, collection, preservation, transportation, analysis, documentation, and presentation. These phases apply also to mobile forensics.

Mobile phones, being a digital tool, are used today for committing different crimes. Specifically, as a communication tool [11] they can be used as to aid traditional crimes. On the other hand, mobile phones can also be a target of or used outrightly for cybercrimes. In all cases, the phones would contain evidence data. For example, a typical smart-phone contains potential evidentiary data including user-created information like contacts, audio, video, and files; internet-related information, including e-mail messages and web browser history; and installed third-party applications [12], [13].

Table 1 presents some of the data and their location. These data are volatile in nature. Scientifically proven and derived procedures are therefore needed to preserve, collect, validate, identify, analyze, interpret, document and present the digital evidence for the aim of facilitating or furthering the reconstruction of events found to be criminal [14].

Brothers [15] identified five different levels of analysis utilized in mobile forensics for acquiring data. These are manual acquisition, logical acquisition, hex dump analysis, chip-off, and micro read. At the lowest level is the manual acquisition manual browsing of the phone using keypad and reviewing of phone documentation in order to acquire data in the phone. The next level, logical acquisition, is used to gain access and acquire data using AT commands. This functionality is available on many forensic software tools. Hex dump analysis is used to acquire data in its raw form. It involves removing chips from the circuit board of the mobile phone or connecting to a cable and running specific forensic software. For chip-off, as the name implies, the memory chip is removed and read in or by a separate device. The last level, micro read, provides physical view of the entire internal circuit of the mobile phone memory. To achieve this, high-power microscope is used.

2.2 Comparison between Mobile Forensics and Computer Forensics

One of the primary differences between computer and mobile devices is that a computer device does not incorporate SIM card. While both use operating systems, mobile devices need SIM cards for any form of communication to be possible.

In the area of forensics, [16] discussed some key factors in differentiating between mobile and computer forensics including reproducibility of evidence when performing dead forensic analysis, operating and file systems, hardware, and available forensic tools and toolkits.

Evidence reproducibility in dead forensic analysis on mobile devices is almost infeasible. This is due to the continuous functioning of device clock on mobile phones which causes data on the memory to change constantly. The effect of this is that a different value is gotten each time a hash function is applied on the contents of the memory.

In respect of operating systems and file systems, investigation is more difficult on mobile systems. One reason is the use of volatile memory for storing user data on mobile devices. One consequence of this is that there is a possibility of user data being lost if a phone is disconnected from a power source and the internal battery depletes. Another reason is short cycle of operating systems release. Some operating systems developers release new versions with substantial changes from previous versions annually. And between these major releases, patches and minor upgrades are released periodically.

Hardware architectures are as diverse as there are different mobile phones. This diversity also applies to operating systems. Manufacturers of mobile devices make effort to customize operating systems to accommodate the specific functionality built into their phone hardware. An in-depth understanding of a phone's hardware together with its OS will be required to develop a forensic tool that can effectively acquire data from such device.

2.3 Mobile Phone Forensics Challenges

Conducting successful a digital investigation on a mobile phone is a challenging task. This difficulty arises from many factors. For instance, the continuous functioning of device clock on mobile devices makes producing exact bit-wise copy of the complete contents of the memory of the device unattainable [16].

Another challenge is the short release cycle of OS used by different mobile phones. This makes timely development of updated versions of forensic tools to keep pace with changes in operating systems difficult. The diversity in mobile hardware and customized operating systems, and increasing prevalence of proprietary hardware, coupled with increase in mobile sophistication and connectivity options are capable of causing developers of forensic tools to struggle to cope with developing effective tools.

Table 1. Mobile data evidence and their location [15]

Mobile Data Evidence	Location
Service provider	On the back of SIM
Unique Identity Number	On the back SIM
Location Area Identity (LIM)	Saved Inside the SIM
Call logs	Stored on both SIM and phone memory
Contacts	Stored on both SIM and phone memory
International Mobile Subscriber Identity (IMSI)	Is unique to each subscriber and stored inside the SIM
Text message data	Stored inside the SIM and phone memory
Multimedia messages	Stored on phone memory
Images/videos/sound	Stored on phone memory
WAP/Browser history/Emails	Stored on phone memory
Calendar	Stored on phone memory
Previous SIM data	Not all phones stores the previous SIM data
Telephone number	Sometimes present in SIM memory
Integrated Circuit Card Identifier (ICCID)	Stored inside SIM
International Mobile Equipment Identity (IMEI)	Stored and printed on mobile phone

In addition to the above, [15] and [17] extensively discussed other challenges often faced by forensic investigators. These include:

i. Quick battery drain as a result of signal blockage. Blocking of signal is essential to carry out forensic analysis.
ii. Limitation of most forensic analysis tools in handling physically damaged mobile phones.
iii. For a mobile phone already shut down, there is a possibility of phone data loss or activation of security measures if it is restarted.
iv. Determining which communication protocol to use for the mobile device under investigation for remote connection with the computer of the investigator. This challenge is caused by the fact that the choice of protocol is contingent on the operating system which often place restrictions on the usage of the protocols.
v. Security mechanisms integrated on the mobile devices for data protection. For instance, one of the mechanisms that can be used to secure data on mobile phones is encrypting the data. In the event that the encryption algorithm is proprietary, even after gaining access to a mobile phone, making sense of the data would be almost impossible.
vi. Lack of standard data format. There are no standards that define default storage formats and locations for different types of data. A particular type of data, say text messages, may be stored on the SIM of a phone, but on the phone memory of another phone. Also, proprietary file formats are used to store some categories of data.

From the foregoing, no doubt, it would be extremely difficult to find a forensic tool or toolkit that is virtually applicable across all mobile device platforms.

2.4 Review of Related Works

Most literatures on forensic investigation are focused on assessment of performance of one or more forensics tool on one or more mobile device. In some cases, the performances of the tools are evaluated. In other studies, two or more tools were used, with each tool achieving a section of the overall objectives. A summary of some literatures are classified under different objectives and methodologies, and presented in Table 2.

Most literatures often involve the use of forensic tools, available as open source or commercial, which use remote-way procedure, in which case, acquisition of data entails connecting mobile device under investigation with investigator's computer via either cable or by a wireless medium [18]. Other means of forensic evidence acquisition is via tools which are on-phone, through manual examination of backed-up data, or even some unconventional means.

On-phone forensic tools are advantageous over remote-way procedure tools in that they require less equipment, since they don't involve connecting device to computer. Also, they have the potency of retrieving the volatile information that resides on the phone, such as running processes [14]. These tools also allow parallelization. In the case where multiple phones need to be acquired, once it is installed on the phones, acquisition is in parallel. In the case of tools that require remote connections, acquisition from one phone must be completed before starting the other [18]. For instance, SMIT, developed by [20] using C++, worked on all tested Symbian phones, with version 9.x. Images of the user data volume were successfully acquired. Mokhonoana and Olivier [14] cautioned that using on-phone tool could cause considerable changes to the data on the device. However, [18] reported that their tool, MIAT, caused less changes on files than Paraben Device Seizure. This tool, when tested on a phone using Symbian version 9.3, was found to be compatible.

Table 2. Summary of related works

S/No.	Objective(s)	Methodology	Author(s)
1.	Assessment of performance of one or more forensics tool on one or more mobile device	Testing of on-phone + remote-way procedure tools on a phone	[19]
		Testing of on-phone + remote-way procedure tools on different phones with the same OS, but different versions	[18]
		Testing of on-phone tool on a phone	[14]
		Testing of on-phone tool on different phones with the same OS, but different versions	[20]
		Testing of remote-way procedure tools on a phone	[21], [22], [23]
		Testing of remote-way procedure tools on different phones and OS	[24], [25]
		Testing of remote-way procedure tools on different phones with the same OS of different versions	[26], [27]
2.	Analysis of social networking applications on mobile devices	Manual examination of back up files using text editor	[24]
		Testing of remote-way procedure tools on a phone	[23]
3.	Demonstration of possibility of forensic acquisition through unconventional means	Use of mobile phone flasher boxes.	[28]

Most data acquisition tools, whether on-phone [14] or otherwise [26] and [19], are unable to recover deleted files. Mubarak and Ali [23] however reported that CelleBrite Universal Forensic Extraction Device (UFED) was able to acquire some deleted data. It is believed that if Android smartphones could be successfully rooted, all information stored potentially could be read [22].

Al Mutawa, Baggili, and Marrington [24] and Mubarak, and Ali [23] focused their study on acquisition of social network activities. While the former used manual examination of back up files using text editor, forensic tools were used in the latter. Comparing the possibilities of acquiring data relating to social network activities from three different phone types – Blackberry, iPhone, and Samsung, [24] discovered that no trace of social network activities could be recovered on Blackberry, while the other two store some significant amount of data that could be recovered that could be used for evidentiary purpose. This fact was corroborated in [23] who discovered the ability of Oxygen Forensic Suite to acquire social network data from an iPhone 4 device.

III. Methodology

The main objective of this study is to evaluate the capacity of some existing mobile forensics tools in acquiring data, especially deleted ones, from mobile phones. In this section, we discuss the materials used and methods adopted for evaluation.

3.1 Evaluation Environment and Requirements

The materials, hardware and software, used to achieve the objective of the study include:

i. Samsung Galaxy (GT-S5300), running Android v2.3.6.
ii. HTC Desire 300, running Android v4.1.2 (software number 1.10.401.4)
iii. Toshiba Satellite Laptop (C655D-S5200), running on Windows 7, 64 bits.
iv. USB Cable.
v. MOBILedit Forensic v7.5.
vi. Oxygen Forensic Suite 2014 v6.4.0.67 (trial version).
vii. AccessData FTK Imager v3.1.2.0.
viii. EnCase v4.20.
ix. Nokia Asha 302
x. 3 SIM cards (2 MTN and 1 Airtel)
xi. Applications, including Facebook.

The study was focused on data that could be acquired from both phone and SIM memories. Consequently, all external memory devices were removed. Also, the initial scope of the study was to evaluate the capacity of the forensic tools on both Windows and Android phones. Once we found out that the tools would not function on Windows phone, focus was shifted to only Android OS.

3.2 Evaluation Procedure

In many mobile devices, the mobile data evidence often present in the phone internal memory include contacts, text messages (SMS), stored audio recording, image files, logged incoming calls and dialed numbers, calendar and possible events, settings (language, date/time, tone/volume, GPRS, WAP and internet), Bluetooth contents, and International Mobile Equipment Identification (IMEI). On the other hand, some of the mobile data that often reside on SIM memory include text messages, service provider identity number, call logs, contact, International Mobile Subscriber Identity (IMSI), and Integrated Circuit Card ID (ICCID).

The two mobile phones on which the forensic tools were evaluated were the Samsung Galaxy (GT-S5300) (Fig 1) and HTC Desire 300 (Fig 2) phones. Both phones have been in use by different users before they were collected for the purpose of this study. A newly bought and registered SIM (Airtel) was inserted into each of the phone. Their USB storage was formatted, to wipe off the memory of the phones. To allow mobile device discovery, USB debugging was enabled.

In order to have a controlled environment, in addition to data already present on the phones, including applications' data, web browser cache history, and call logs, some data were generated over a period of five days. Equally, over a period of five days, the generated data

were gradually deleted. The type and amount generated are presented in Table 3.

Table 3. Type and amount of data generated

Data	Number Generated
Pictures	50
Contacts	50
SMS	12
Audio	30
Videos	25

For the pictures, some were generated through snapshots, while others were transferred from the Nokia Asha via Bluetooth. The audio and video files were all transferred from the same phone, also via Bluetooth. Contacts were inputted and stored on SIM memory. To store some on the phone memory, an MTN SIM was inserted and contacts transferred from the SIM into the phones' memories. To generate text message data, SMS were both sent from the two phones to, and to them from, the Nokia Asha device. During the period of experiment the mobile phone was kept on flight mode in order to avoid incoming calls and messages.

IV. Results

Upon evaluation, MOBILedit was able to identify the IMEI number of both mobile phones, IMSI and ICCID of the registered SIM cards for both phones. For Oxygen Forensic, it could not extract information about the IMSI and ICCID of the SIM cards. However, it was able to identify the IMEI number of the mobile phones, names of SIM cards service provider, the name of the mobile devices, the operating system versions of the phones. On the other hand, AccessData FTK Imager and EnCase could not extract the IMEI number, IMSI, and ICCID.

Fig.1. Samsung Galaxy (GT-S5300) [29]

Other results for Samsung Galaxy, as shown in Table 5, show that AccessData FTK Imager and EnCase performed significantly better in acquiring some deleted data. While MOBILedit was able to extract application and web browser cache history data, Oxygen Forensic could not extract any data.

Table 6 reveals that both AccessData FTK Imager and EnCase, similar to their performance on Samsung Galaxy, were able to extract deleted pictures, audios, and videos from the HTC phone. However, MOBILedit and Oxygen Forensic were unable to acquire any data.

Fig.2. HTC Desire 300 [30]

Table 4. Comparison between Samsung Galaxy (GT-S5300) and HTC Desire 300 [30]

	Samsung Galaxy (GT-S5300)	HTC Desire 300
Technology	GSM / HSPA	GSM / HSPA
Launched	2012, February	2013, September
SIM	Mini-SIM	Micro-SIM
OS	Android OS, v2.3 (Gingerbread)	Android OS, v4.1.2 (Jelly Bean)
CPU	832 MHz ARM 11	Dualcore 1 GHz CortexA5
Card Slot	microSD, up to 32 GB	microSD, up to 32 GB
Internal Memory	3 GB	4 GB, 512 MB RAM
WLAN	WiFi 802.11 b/g/n, hotspot	WiFi 802.11 b/g/n, hotspot
Bluetooth	v3.0, A2DP	v4.0, A2DP, aptX
USB	microUSB v2.0	microUSB v2.0
Messaging	SMS(threaded view), MMS, Email, Push Mail, IM	SMS(threaded view), MMS, Email, Push Mail

V. Analysis

The objective of this study is evaluate the performance of some existing mobile forensics tools in acquiring data from mobile devices, with emphasis on deleted data. Specifically, four mobile forensic tools – MOBILedit, Oxygen Forensic, AccessData FTK Imager, and EnCase – were used on two mobile phones running different versions of Android OS.

While MOBILedit and Oxygen Forensic provided some SIM-related information, including IMSI and ICCID, both AccessData FTK Imager, and EnCase could not acquire any of the information. One reason for this is that AccessData FTK Imager and EnCase, essentially, are used for obtaining root access to the mobile device. Both cannot have access to the SIM memory.

The study also reveals that, on both phones, none of the forensic tools was able to extract deleted contacts, SMS, and call logs, though two of the tools, AccessData FTK Imager and EnCase, were able to extract deleted pictures, audios and videos. Extracting deleted contacts and SMS has been shown to be possible only with a dd analysis [21].

The performance of MOBILedit and Oxygen Forensic (trial version) corroborates the findings of [19] and [23], though the authors in both studies had tested the tools on a Nokia E5-00 phone which uses a Symbian v9.3 and iPhone 4 respectively. While Oxygen Forensic have been demonstrated to be effective at extracting useful information, including phonebook entries, call logs, text messages [22], and social network data [23], its effectiveness to extract deleted evidentiary data would need further investigation.

One other important result reveals that while MOBILedit was able to extract some data from the Samsung Galaxy phone, but not from the HTC. We searched through the list of supported HTC phones on the official site of MOBILedit [31]. It was found out that HTC Desire 300 was not part of the list. A similar search for supported Samsung phones surprisingly showed that Samsung Galaxy (GT-S5300) was also not supported [32]. The developers of the tool, on the site, had acknowledged the possibility of the tool performing on any phone they had not tested.

The failure of some of the tools to identify data in the phones could be due to the fact that the phones were not new. While it is expected that developers of forensic tools test their tools on new phones, in a tightly controlled environment, real-life scenario, in most cases, would not conform to this setting. Offenders use different type of phones including new and old ones. Forensic tools should be able to perform regardless of the period of usage of a phone.

While the reality of some of the tools being able to discover some deleted files suggests a significant progress by forensic tools in acquiring deleted evidentiary data, it corroborates the fact that these tools are currently limited in acquiring deleted data belonging to some file types. Currently there is no one-fits-all forensic tool capable of extracting every type of mobile evidence data from all categories of mobile phone. The implication is that, the type of evidence data required would determine the type of analysis to be adopted, and thus, the appropriate forensic tool(s).

VI. Conclusion

This study was aimed at evaluating the performance of some forensic tools to acquire data, with emphasis on deleted data, from Android phones. The results of our study show that two among the four tools, AccessData FTK Imager and EnCase performed better than MOBILedit and Oxygen Forensic Suite. The ability of some of these tools to acquire deleted data demonstrates significant progress in the development of quality and effective forensic procedures.

The need for forensic tools capable of extracting deleted evidentiary data cannot be overemphasized. A suspect might decide to delete all data in a phone that might link him with an offence. Being able to provide adequate and non-refutable evidence of this data would be crucial to the success of prosecuting the suspect in a court of law.

Table 5. Evaluation results for Samsung Galaxy (GT-S5300)

Mobile Data Evidence	MOBILedit	AccessData FTK Imager	Oxygen Forensic Suite	EnCase
Pictures	No	Yes	No	Yes
Contacts	No	No	No	No
SMS	No	No	No	No
Application	Yes	No	No	No
Audios	No	Yes	No	Yes
Videos	No	Yes	No	Yes
Web browser cache history	Yes	No	No	No
Call logs	No	No	No	No

Table 6. Evaluation results for HTC Desire 300

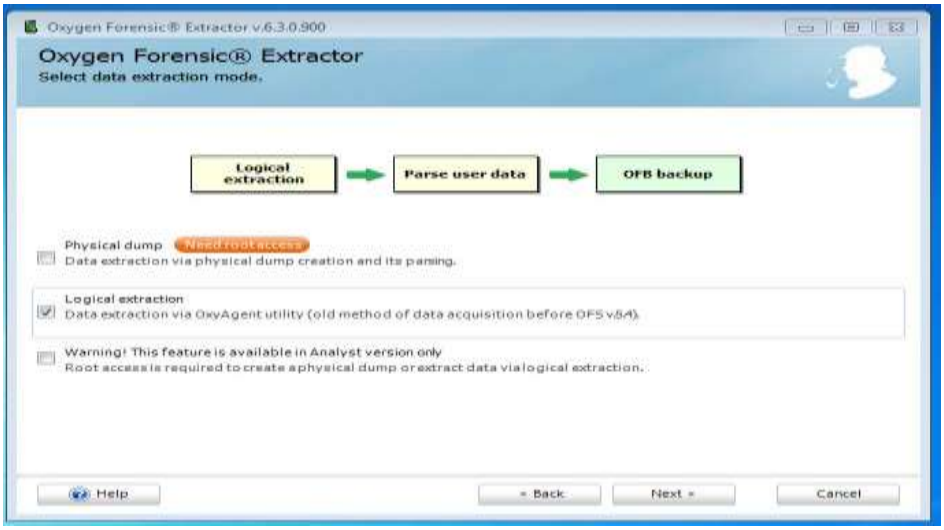
Mobile Data Evidence	MOBILedit	AccessData FTK Imager	Oxygen Forensic Suite	EnCase
Pictures	No	Yes	No	Yes
Contacts	No	No	No	No
SMS	No	No	No	No
Application	No	No	No	No
Audios	No	Yes	No	Yes
Videos	No	Yes	No	Yes
Web browser cache history	No	No	No	No
Call logs	No	No	No	No

One of the limitations of this study was the use of trial version of Oxygen Forensic. Consequently, we cannot conclude on its capability for forensic acquisition of data. Further investigation would therefore be needed to validate, or otherwise, results in our study. Further studies are also required to ascertain the specific versions and hardware MOBILedit would effectively perform on.

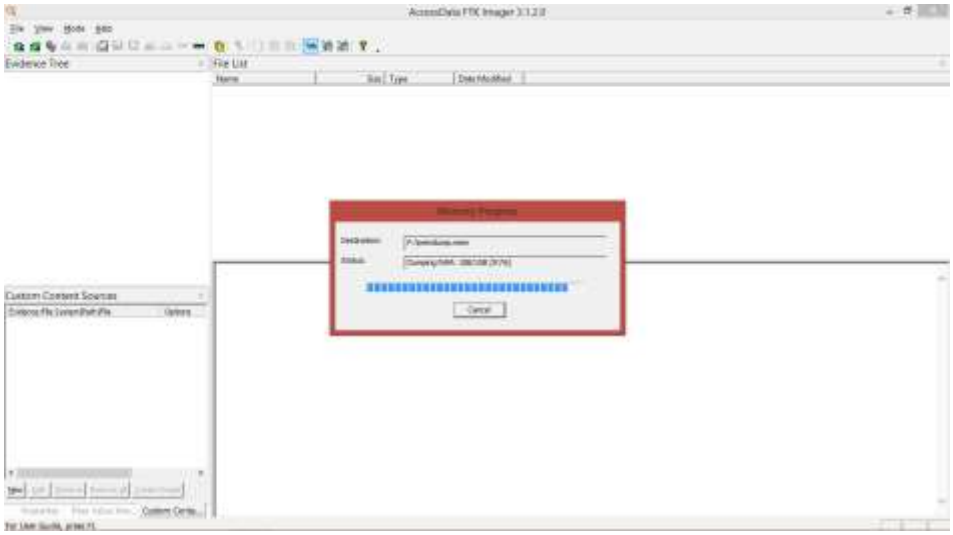
APPENDIX A: Extraction of mobile data

APPENDIX B: Connecting phone device to Oxygen Forensic

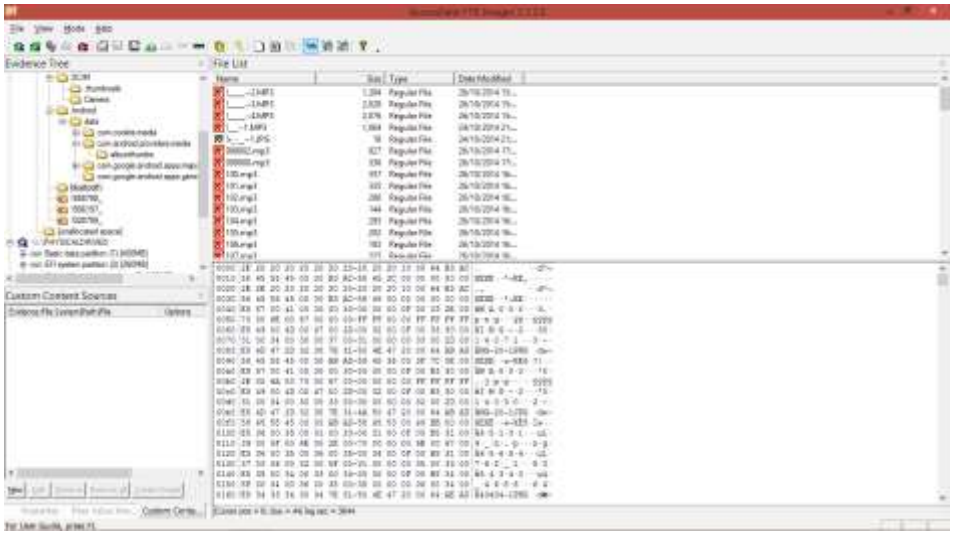
APPENDIX C: Selection of logical extraction method on Oxygen Forensic



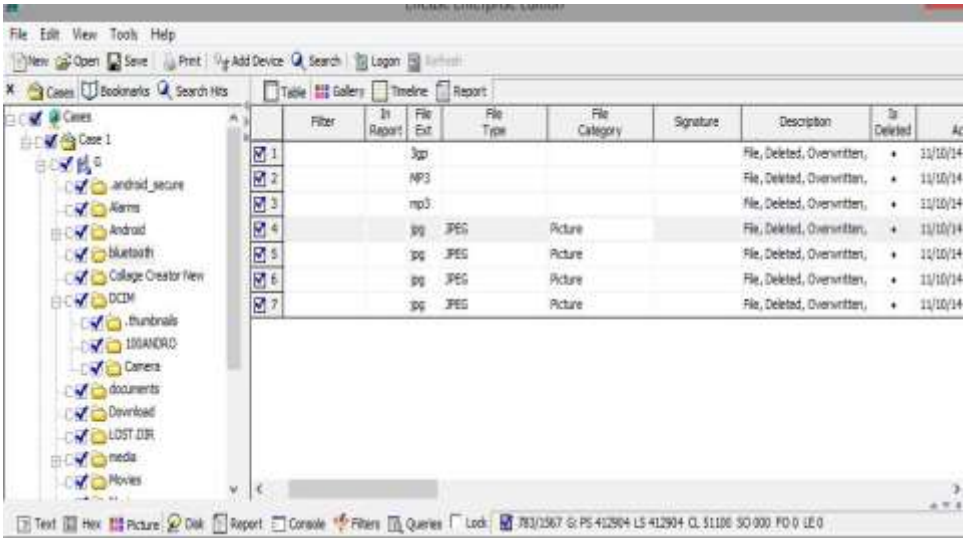
APPENDIX D: AccessDataFTK Imager Memory capturing interface



APPENDIX E: AccessDataFTK Imager captured disk



Appendix F: Encase interface showing captured data



REFERENCES

[1] ITU. Mobile_cellular_2000-2012. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Mobile_cellular_2000-2012.xls

[2] Iovation. Fighting Mobile Fraud: Protecting Businesses and Consumers from Cybercrime. Retrieved from https://s3.amazonaws.com/content.iovation.com/white-papers/PDF/iovation-mobile-fraud-white-paper.pdf (2012).

[3] Ruggiero P, and Foote J. Cyber Threats to Mobile Phones. 2011. Retrieved August 20, 2014, from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf.

[4] Felt A P, Finifter M, Chin E, Hanna S, and Wagner D, A Survey of Mobile Malware in the Wild. Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011, 3 – 14.

[5] Enck W, Ongtang M, and McDaniel P. On lightweight mobile phone application certification. Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.

[6] Willassen S Y. Forensics and the GSM Mobile Telephone System. International Journal of Digital Evidence, 2003, 2(1), 1 – 17.

[7] Barmpatsalou K, Damopoulos D, Kambourakis G, and katos V. A Critical Review of 7 Years of Mobile Device Forensics. Digital Investigation, 2013, 10, 323 – 349.

[8] Sridhar N, Bhaskari D L, and Avadhani P. Plethora of Cyber Forensics. International Journal of Advanced Computer Science and Applications, 2011, 2(11), 110 – 114.

[9] Sindhu K K, and Meshram B B. Digital Forensic Investigation Tools and Procedures. International Journal of Computer Network and Information Security, 2012, 4, 39-48, doi: 10.5815/ijcnis.2012.04.05.

[10] Vishal R A, and Meshram B B. Digital Forensic Tools. IOSR Journal of Engineering, 2012, 2(3), 392-398.

[11] Umale M N, Deshmukh A B, and Tambhakhe M D. Mobile Phone Forensics Challenges and Tools Classification: A Review. International Journal on Recent and Innovation Trends in Computing and Communication, 2014, 2(3), 622 – 626.

[12] Casey E, and Turnbull B. Digital evidence on mobile devices. Eoghan Casey, Digital Evidence and Computer Crime. Third Edition. Forensic Science, Computers, and the Internet, Academic Pres (2011).

[13] Willassen S Y. Forensic analysis of mobile phone internal memory. Advances in Digital Forensics. Springer US, 2005. 191-204.

[14] Mokhonoana P M, and Olivier M S. Acquisition of a Symbian Smartphone's Content with an On-Phone Forensic Tool. In Proceedings of the Southern African Telecommunication Networks and Applications Conference, 2007, 8. Retrieved from mo.co.za/open/symbianfor.pdf.

[15] Brothers S., Cell Phone and GPS Forensic Tool Classification System. 2009, Retrieved from http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhoneandGPSForensicToolClassificationSystem.pdf.

[16] Ahmed R, and Dharaskar R V. Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective. 6th International Conference on E-Governance (ICEG), Emerging Technologies in E-Government, M-Government, 2008, 312 – 323 (2008).

[17] Lutes K D, and Mislan R P. Challenges in Mobile Phone Forensics. Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems, and Applications (2008).

[18] Distefano A, and Me G. An overall assessment of Mobile Internal Acquisition Tool. Digital Investigation, 2008, 5, 121 – 127.

[19] Mohtasebi S H, Dehghantanha A, and Broujerdi H G. Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone. International Journal of Digital Information and Wireless Communications, 2011, 1(3), 651 – 655.

[20] Pooters I. Full User Data Acquisition from Symbian Smart Phones. Digital Investigation, 2010, 6, 125 – 135.

[21] Lessard J, and Kessler G C. Android Forensics: Simplifying Cell Phone Examinations. Small Scale Digital Device Forensics Journal, 2010, 4(1), 1 – 12.

[22] Sack S, Kroger K, and Creutzburg R. Overview of Potential analysis of an Android Smartphone. IS&T/SPIE Electronic Imaging, pp. 83040M-83040M. International

Society for Optics and Photonics, 2012. doi:10.1117/12.909657.
[23] Mubarak A, and Ali A. Smartphone Forensics Analysis: A Case Study. International Journal of Computer and electronic Engineering, 2013, 5(6), 576 – 580.
[24] Al Mutawa N, Baggili I, and Marrington A. Forensic Analysis of Social Networking Applications on mobile devices. Digital Investigation, 2012, 9, 24 – 33.
[25] Schwamm R, and Rowe N C. Effects of the factory reset on mobile devices. Journal of Digital Forensics, Security and Law, 2014, 9(2), 205-220.
[26] Williamson B, Apeldoorn P, Cheam B, and McDonald M. Forensic Analysis of the contents of Nokia Mobile Phones. 4th Australian Digital Forensics conference, 2006, 36.
[27] Casey E, Bann M, and Doyle J. Introduction to Windows Mobile Forensics. Digital Investigation, 2010, 6, 136 – 146.
[28] Jonkers K. The Forensic Use of Mobile Phone Flasher Boxes. Digital Investigation, 2010, 6, 168 – 178.
[29] www.samsung.com
[30] GSMArena. http://www.gsmarena.com/compare.php3?idPhone1=4612&idPhone2=5666#results
[31] http://www.mobiledit.com/phones?MANUFACTURER_ID=315
[32] http://www.mobiledit.com/phones?MANUFACTURER_ID=7

Authors' Profiles

Oluwafemi Osho is currently a lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. He holds an M.Tech. degree in Mathematics, and a B.Tech. degree in Mathematics/Computer Science. Before joining the institution, he served as Head of the IT Department of one of the leading mortgage banks in Nigeria. His current research interests include cybersecurity, mobile security, and security analysis. Oluwafemi is a Certified Ethical Hacker (CEH), and a member of the Cyber Security Experts Association of Nigeria (CSEAN), and a host of other professional associations.

Sefiyat Oyiza Ohida is currently undertaking a Masters degree in Computer Science at the African University of Science and Technology, Nigeria. She holds a B.Tech degree in Computer Science (Cyber Security).

How to cite this paper: Oluwafemi Osho, Sefiyat Oyiza Ohida,"Comparative Evaluation of Mobile Forensic Tools", International Journal of Information Technology and Computer Science(IJITCS), Vol.8, No.1, pp.74-83, 2016. DOI: 10.5815/ijitcs.2016.01.09