

An Investigation into the Impact of Rooting Android Device on User Data Integrity

Lutta Pantaleon
Department of Computing
Staffordshire University
Stoke-on-Trent, UK
o026748f@student.staffs.ac.uk

Mohamed Hassan
Department of Computing
Staffordshire University
Stoke-on-Trent, UK
mohamed.hassan@staffs.ac.uk

Abstract—The available commercial and freeware mobile forensics tools heavily rely on a rooted mobile device for them to extract data. The potential effects of rooting the device before extraction could pose a threat to the forensic integrity rendering the acquisition process flawed.

An endeavour was made in compiling of this paper investigating the impact of rooting android mobile devices on user data integrity. The research examines and analyses data from an android Samsung phone. A framework has been developed to illustrate measures and steps to be observed in the extraction of data from mobile devices.

Keywords—*Android; rooting; forensic; data integrity;*

I. INTRODUCTION

Due to the ubiquitous nature of mobile devices, it is increasingly becoming easier to communicate and to an extent create a 'virtual village'.

The enormous growth of android smartphones' usage currently cannot be ignored. The convenience it creates for people brings with it challenges like crime and information security breaches. These criminal activities bring about the need for mobile forensics and digital investigations for law enforcers.

The available and mostly used mobile forensic software tools like XRY, EnCase and Cellebrite can extract more data if the devices being investigated are rooted.

Lessard and Kessler (2010) note that imaging the phone memory is essential in mobile forensics as the memory contains additional information and passwords; this, therefore, can only be accessed if the phone is rooted. The authors go on and note that changing data in this manner is not forensically sound and therefore would not be advisable to be done in an investigation. They continue and argue that even the process of gaining root access requires that the examiner installs a third party to the phone which could make the evidence not admissible in a court of law.

Understanding and investigating the impact this rooting process causes to the device data is very important to the mobile forensic exercise.

II. RELATED WORK

Vidas et al. (2011) have researched on the process of data collection of android devices. The authors claim that their process intends to obtain a close to 'exact copy', this even though they admit that in the interaction with the device, they alter its state in a way.

The authors suggested a methodology based on data collection through recovery image. The technique involves obtaining a recovery image which is then flashed to the device with the help of device specific instructions.

The authors, (Vidas et al., 2011) have discouraged rooting a device for forensic purposes and have argued for the following reasons:

- That the rooting process leads to a software flaw and leverages on the software versioning in some models. They go on and state that if the device is locked then the investigator may find it hard to reveal the software version running on the device which may lead to damage of the data collected. This reason seems to be remote given the advancement of the rooting applications and this may be dependent on the type of the rooting process used. Although it may sound right, it is not true that it may cause damage and bring data integrity issues.
- That the rooting process may alter some partitions of the device that may store user data. Indeed, this has some weight because if the process is not done right, then some data may be changed leading to integrity issues.
- That due to easy escalation brought by rooting, the android security model may be compromised. This is also a contentious issue because it all comes down to the process and the tools used.

Another related work is that done by (Son et al., 2013); "A study of user data integrity during acquisition of Android devices". The study proposes to use the JTAG (Joint Test Action Group). The authors admit that to their knowledge no studies have been conducted to determine if the JTAG method guarantees data integrity or not.

A related work of Votipka et al., (2013) has described a general methodology to for data acquisition in android devices. This is done by a re-purposing a special android boot mode for comprehensive extraction preserving data integrity. The authors however note that the recovery mode in their study involved was gained through a combination of special keys of the device and thereby circumventing the normal boot process.

III. RESEARCH MOTIVATION

On the key findings from these methodologies suggested by these authors, it can be noted that even though they have designed “excellent” frameworks, methodologies or process; they do not do a proper data analysis of the data that is collected. A good analysis is therefore needed to verify the integrity of the data collected or the lack of it. As stated by (Do et al., 2015), the lack of adequate analysis of the collected data may lead to some relevant evidence being omitted.

IV. EXPERIMENTS

A sound and very well managed and controlled forensic environment is essential and proves crucial in any type of forensic investigation being carried out. A forensically sterile environment which has a solid prevention of any potential cross contamination, blocks out unwanted data and is essentially free from malware and viruses is desirable for a forensically sound investigation.

The environment involved in this research was set up as illustrated and explained below:

A. Software Tools

All the software being used in this investigation are licensed and valid for use by Staffordshire University students.

The following are the software tools involved:

Software	Version
Microsoft Windows	10 and 7 Professional
Linux	Ubuntu 16.04
VirtualBox	Version 5.1.18
Samsung Kies	2.6.4.16113_3
EnCase	V8.0.1.01
XRY	7.1 64-bit
MOBILedit Forensic Express	4.0.0.8613 (Demo)
XRY XAMN	1.1.1 Beta (64 bit)
XRY Reader	6.18.0
ODIN	V3.09

Fig1: Software Tools

B. Hardware Tools

The following hardware tools were used in the acquisition and analysis of the data.

Hardware Tool	Specification
HP Pavilion Notebook	Intel Core i5, 2.4GHz, 8192MB
Samsung Note II	GT-N1700
USB Cable	Micro USB3
HP Compaq Elite 8300 SFF Desktop	Intel Core i5, 3.20GHz, 32768MB
XRY Code Meter Dongle	

SIM Card	Nano Simcard
Flash Drive	HP 8GB

Fig2: Hardware Tools

C. Forensic Environment Setup

On the local personal computer running Microsoft Windows 10 Operating System, a virtualbox was installed.

Two machines were set up on the virtualbox; one running Microsoft Windows 7 Operating System and one running Linux Ubuntu 16.04 Operating System.

Both the virtual machines were installed with essential functional capabilities like the memory, disk capacity and other necessary functionalities.

On the virtual machine running windows operating system, the following software tools were installed, Android SDK Toolkit, Samsung phone drivers and other open source/freeware forensic tools.

The android phone used for the tests was a Samsung Note II Model Number: GT-N7100.

To be able to access the mobile phone data on the computer the ADB (Android Debug Bridge) was enabled. ADB is a program that enables the access of the device from a Personal Computer. The USB PC connection protocol enabled on the phone for communication was the Media Transfer Protocol (MTP).

D. Data Acquisition

The methods of data acquisition used were both logical and physical extraction of data. First, the logical data extraction was done using XRY, EnCase and finally MOBILEdit Forensic Express. The physical extraction was done by MOBILEdit Forensic Express and the dd command on Linux. Before we start data acquisition, the mobile device needs to be rooted. The device has been rooted using Odin (an application developed by Samsung for flashing images or custom recovery firmware). The process employed for rooting the device was adapted from steps developed by Pirvu, B. (2017).

E. Physical Extraction Using dd Command

A physical image of the device memory was also obtained using the dd command.

This was done on an Ubuntu Linux; the process and steps followed were derived from Lohrum (2014)

F. The Unrooting Process

For the purposes of variety of experiments and wider range of data collection, the phone was unrooted and rooted again with TowelRoot and KingRoot tools.

A physical extraction of data redone. The unrooting process adopted from Martin (2013)

V. ANALYSIS OF DATA COLLECTED

The SMS messages and Images were analysed.

The mode of the analysis was to randomly pick a instance of the above categories from a logical extraction report and compare that particular instance with the report from a physical extraction.

Another aspect that was considered in this analysis was in relation to different rooting methods used. The analysis factored in the rooting method used in the extraction and in some instances compared two extractions performed by the same tool but the device rooted with different methods.

A. Comparative Analysis of Images.

A sample image from both logical and physical extraction reports from MOBILEdit and XRY and EnCase are shown below:


1544 9e3d2da3bc9d4be9397a029aa54b22ca.jpg	
	Path phone/raw3/WhatsApp/Media/Statuses/9e3d2da3bc9d4be9397a029aa54b22ca.jpg
	Size 29.4 kB
	Created 2017-04-22 12:41:14 (UTC+1)
	Modified 2017-04-22 12:41:14 (UTC+1)
	Accessed 2017-04-22 12:41:14 (UTC+1)
	Width 720 px
	Height 720 px

Fig3: Image from MOBILEdit Logical Extraction Report


Data	
File Name	9e3d2da3bc9d4be9397a029aa54b22ca.jpg
Type	Jpeg
File Size	28,70 KB
MetaData (Full)	Orientation: 1 ExifColorSpace: 1 ExifPixelDim: 720 ExifPixelDim: 720
Path	\\mnt\shell\emulated\0\WhatsApp\Media\Statuses\
Storage	Device
Modified	22/04/2017 11:41:14 UTC (Device)
Hash (SHA1)	b3ee645e3c0f287cb7fca53892d65bd32c8d267
MetaData	
Orientation	None

Fig4: Image from XRY Logical Extraction Report

Pictures of Interest

Name	Logical Item	Signature	File Type
	Size, Type	Analysis	
1 9e3d2da3bc9d4be9397a029aa54b22ca.jpg	29,386 Entry	Match	JPEG Image Standard

1) 9e3d2da3bc9d4be9397a029aa54b22ca.jpg

Item Path	Disk Image\data\media\0\WhatsApp\Media\Statuses\9e3d2da3bc9d4be9397a029aa54b22ca.jpg
File Created	
Last Written	22/04/17 12:41:14
Last Accessed	22/04/17 12:41:14
MD5	1691a668aa7c9e9086a011da41cef6
Comment	



Fig5: Image from EnCase Physical Extraction Report

1) Discussion Points from the images

From both the logical and physical extraction reports, it can be noted that the image retains its shape and identity, the name of the image is maintained and the physical path of the image is also maintained. However, XRY is using SHA1 to compute the hash values of the image. Whereas EnCase uses the MD5 hash values.

To get a better comparison of the hash values, the image was browsed on the EnCase Evidence browser as shown in the figure below:

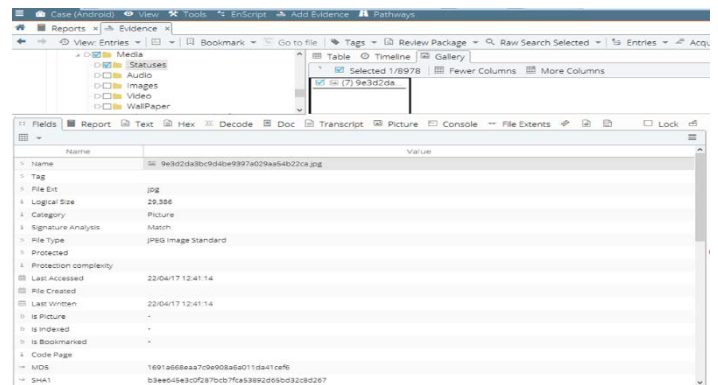


Fig6: EnCase Evidence Browser

The SHA1 hash value shown on this physically extracted evidence, is the same one on the XRY logically extracted data report.

B. Comparative Analysis of Images

Type	Remote Number	Date	Text
Read	AARHEALTH	20/04/17 13:04:29	Quality & affordable healthcare is coming soon to Buru Buru, 1st Fl...

Phone: AARHEALTH
Date: 20/04/17 13:04:29
Text:
Quality & affordable healthcare is coming soon to Buru Buru, 1st Floor Mesora Center next to Kenol Petrol Station, Nairobi. Call us on 0730655000/0780888234.
Folder: Inbox
Status: read
Smsc Number: +254722500166
Status Text: Read
Parent Folder: Inbox

Comparative Analysis of SMS Message Fig7: SMS from EnCase Logical Extraction Report

1 AARHEALTH	
Last Activity	2017-04-20 13:04:29 (UTC+1)
Participants	AARHEALTH.me
AARHEALTH	Quality & affordable healthcare is coming soon to Buru Buru, 1st Floor Mesora Center next to Kenol Petrol Station, Nairobi. Call us on 0730655000/0780888234. 2017-04-20 13:04:29 (UTC+1)

Fig8: SMS Message from MOBILEdit Physical Extraction Report

1) Discussion Points from the SMS Messages

It can be clearly noted that the time, date, sender and the contents of the SMS message are not changed.

C. Key Points from the whole Analysis

The results from the above analysis indicate that no data change occurred when rooting was done on the phone and subsequent physical extractions done.

Even though the hash values changed in all the extractions performed, it was expected to be so because the phone memory keeps on running; a case in point for this is that the time of the device changes even if the phone is put on airplane mode and write blockers (if possible) used as expected by the ACPO guidelines.

It is also of interest to point that while rooting, the tools install third party tools on the device. These tools however, as analysed from the above analysis, have no effect on the final user data retrieved.

VI. PROPOSED FRAMEWORK

The proposed framework by this research is based on the best measures and steps coupled with methodologies to be followed for a forensically sound physical extraction of android devices. The research adopted the forensically sound adversary model for mobile devices proposed by Do et al. (2015). The model illuminates some key features that are to be observed during the rooting process and ensuring integrity of the data thereof after a physical extraction is performed.

The framework therefore as exhibited by these authors intends to be forensically sound by satisfying the following key criteria:

a) *Meaning*

The collected evidence/data must maintain its originality and interpretation. No change of the user data should occur in any form that corrupts or makes the data lose its original meaning.

b) *Errors*

This refers to the identification of errors and when they do occur and be able to have an explanation for justification that the errors have not affected the validity of the data. This also includes the installation of third party tools like the rooting tools on the target device. A clear explanation should be made and explicitly documented to show that indeed these application software tools do not in any way change the user data.

c) *Transparency and trustworthy*

This highlights the need for a court of law to validate the integrity by undertaking an oversight that is independent of the forensic process used. This would ensure that if a second opinion is sought by the court, the device on which the physical extraction was carried on should produce the same results.

d) *Experience*

The person undertaking the forensic investigation must have the necessary qualifications and experience so that the findings presented can be relied upon.

The capabilities of the framework are as follows:

- *Exploit*

The target device is exploited by using an exploit either by script or a software application. The forensic soundness is maintained as the capability is restricted to functions that do not lead to the introduction of errors.

- *Forensic Copy*

A physical image of the target device is made. The capability reserves the forensic soundness by avoiding errors.

- *Forensic Examination*

Analysis of the data collected is examined and the true meaning of the data examined is maintained.

- *Inject*

A piece of code is infiltrated on the target device and forensic soundness is maintained by avoiding any introduction of errors.

- *Modify*

A modification of an application execution on the target device. This is however done in a forensically sound way that no introduction of errors occurs and that the transparency and trustworthiness of the data are maintained.

A. *Implementation of the Framework*

The framework process flow is based as seen in the process flow diagram below:

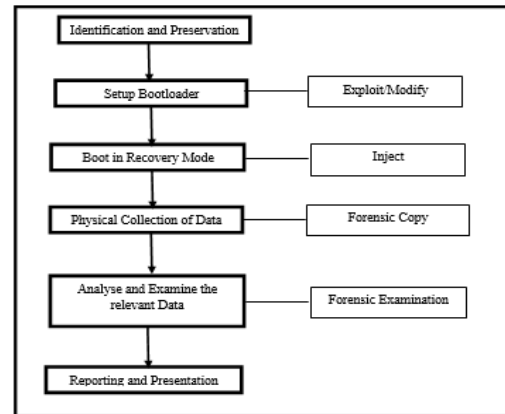


Fig9: Framework Process Flow

Upon completion of the identification and preservation of the mobile device, the data collection is commenced.

The process begins with the configuration of the bootloader. The bootloader must be set up to enable booting of in the download mode of the device.

The booting of the recovery image is used to collect the physical image of the partitions of the device.

The collected physical image is now processed for analysis of the relevant data or information under investigation.

The investigator is now able to prepare a forensic report including all the procedures undertaken and then it is presented.

VII. RECOMMENDATIONS

The following are recommendations that should be observed during physical acquisition of data from mobile devices;

i) *Adherence to standards and guidelines*

To preserve the integrity of the data and the whole forensic process, it is important that all the standards and guidelines provided for digital forensics are followed and observed.

These are the ISO standards like the ISO/IEC 27041:2015 which provides for the good practice methods and processes

for evidence acquisition and the investigation of the captured digital evidence.

ii) *Trained examiner*

As required by the ACPO principles of digital evidence, principle 2 directs that only competent personnel should be allowed to have access to the original evidence. This means that the forensic process should be carried out by a qualified person who understands the process and who is able to document all the processes they have undertaken in the acquisition of the data including all the actions undertaken.

iii) *Type and model of the device*

The NIST guidelines as published by Ayers et al. (2017) provide that mobile identification is key to the success and integrity of the mobile forensic process. As this research has revealed, most of the tools used in the rooting process depends on the device. If a device is not well identified, a wrong rooting tool may be used on it and this may brick the phone rendering it useless and thereby losing all the evidence.

iv) *The type of rooting process to use*

There are quite several rooting processes available. Some can be downloaded directly on the google app store and some can be injected during the booting process.

This research recommends rooting the device during the boot process. This is because, the ACPO principle 1 states that no actions taken by the examiner on the device should change any data. Installing rooting tools through google app store requires that one logs in with a google account and downloads the application then installs it. This is a threat to the integrity of the data as the phone must be connected to the internet to enable the download. Data wiping through cloud computing may also be possible once the phone connects to the internet thereby losing evidence. The NIST guidelines for the acquisition of mobile devices require that the phone is put on an airplane mode so that all communication is lost.

The custom recovery images used for rooting should also be carefully selected. This is because if a wrong image is selected for a wrong device, it may brick the phone and render it useless leading to lose of the evidence.

v) *Selection of the acquisition tools*

The selection of the acquisition tool determines how much data you will collect. Different tools have different capabilities of how much data they can collect by also recovering deleted data and reconstructing the recovered data for meaningful reporting.

The NIST guidelines for mobile forensics propose that a good acquisition tool has the following characteristics.

- a. *Usability*: ability to present data that is useful and meaningful to the examiner
- b. *Comprehensive*: ability for the data to be presented in a way that is easy to understand to enable isolation and sorting
- c. *Accuracy*: ability to verify the quality of the data output of the tool

- d. *Deterministic*: ability for the same results to be obtained under the same circumstances

vi) *Analysis of the Data (Check for Data Integrity)*

In most cases, the tool used for data acquisition would be the appropriate tool for analysis. Tools like XRY can only analyse data acquired by itself. However, a dd image can be analysed on FTK Imager, EnCase and MOBILEdit as evident in this research.

Maintaining the integrity of the original data is the desirable feature for any acquisition process. Whereas digital forensics experts employ the write blockers and hash functions in acquisition of data, it is very hard and almost impossible to do this in mobile forensics. This is because mobile data is ever changing from the clock to internal updates of the applications. A back to back acquisition of the same device will have a slightly different hash value.

The way to go about this is to check the hash values of a selected set of items from the data. As this research revealed, documents, images and directories in the phone data are hashed and they should be matched with the original data to check any inconsistencies that may arise on upon acquisition.

vii) *Reporting and Presentation*

This should include a detailed summary of all steps taken in the acquisition and analysis of the data. The conclusion of the of the investigation should also be noted down.

Of interest to the forensic integrity is to state the reasons as to why some third-party tools for rooting the device before physical acquisition was carried out. This should state that the installed applications have in no way affected the final data collected and this should be evidenced in the analysis of the investigation to affirm that the applications only aided in retrieving data.

viii) *Restore the device to original state*

It is important and a requirement that the phone is restored back to its original state. This research showed that indeed third-party applications are installed on the device either through ADB or normal installation.

Tools like XRY, Cellebrite and MOBILEdit install their third-party tools through ADB. Some of these tools like MOBILEdit has the capability uninstalling the application automatically.

However, for those that cannot be uninstalled through ADB, they must be uninstalled manually to preserve the originality of the phone.

This should be documented clearly in the report.

VIII. CONCLUSIONS

The use of mobile devices worldwide is growing a spontaneous faster rate. This rapid growth is also has led to these devices being misused for criminal activities.

As the use of mobile device and subsequent usage for criminal activities continues so must the mobile forensics help the law enforcement agencies to prosecute criminals.

The collection of evidential data from mobile devices must adhere to the laid down standard procedures by law.

Forensic soundness is in some way vague as argued by Casey et al. (2011) when they stated that: "Setting an absolute standard that dictates 'preserve everything but change nothing' is not only inconsistent with other forensic disciplines but also is dangerous in a legal context. Conforming to such a standard may be impossible in some circumstances and, therefore, postulating this standard as the 'best practice' only opens digital evidence to criticisms that have no bearing on the issues under investigation."

Rooting mobile devices for physical acquisition of data requires altering the device data, however, documentation of the processes and careful avoidance of any unnecessary changes to the user data is desired.

This research has carried out investigations to try and find any data integrity issues relating to user data when a device is rooted before the data acquisition. The investigations revealed that indeed no change is observed in the user data when the root access is enabled.

The research has proposed a framework that can be followed during the physical acquisition of data from mobile devices to preserve data integrity.

IX. FUTURE WORK

Future work for this project includes similar experiments using another android phone models and compare results.

This research focussed more on the analysis of the user data, and even though the research assumed that if there are any data written or overwritten on the Random Access Memory (RAM) of the phone, then the impact must be evident in the user data retrieved (the research found no evidence), it is also desirable that a research is conducted to analyse what this impact has on the running processes and the application data in general.

Another area of research would be to investigate on iOS phones and establish the impact of jailbreaking on the user data, application data and the phone's Random Access Memory.

REFERENCES

Association of Chief Police Officers. (2014) *Good Practice Guide for Computer-Based Electronic Evidence*. [Online] Available from: [https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guide_lines_computer_evidence\[1\].pdf](https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guide_lines_computer_evidence[1].pdf). [Accessed: 23rd February 2016].

Ayers, R., Brothers, S. & Jansen, W. (2017). *Guidelines on mobile device forensics*. [Online]. 2017. Available from: <http://dx.doi.org/10.6028/NIST.SP.800-101r1>. [Accessed: 19 April 2017]

Casey, E., Fellows, G., Geiger, M. & Stellatos, G. (2011). The growing impact of full disk encryption on digital forensics. *Digital Investigation*. 8 (2). pp. 129-134.

Chen, S., Yang, C. & Liu, C. (2011). Design and Implementation of Live SD Acquisition Tool in Android Smart Phone. *2011 Fifth International Conference on Genetic and Evolutionary Computing*. [Online]. Available from: <http://ieeexplore.ieee.org/document/6042741/>. [Accessed: 5 April 2017].

Do, Q., Martini, B. & Choo, K. (2015). A Forensically Sound Adversary Model for Mobile Devices. *PLOS ONE*. 10 (9). p. e0138449. [Online]. Available from: <http://dx.doi.org/10.1371/journal.pone.0138449>. [Accessed: 5 April 2017].

ISO/IEC 27037. (2012) *Guidelines for identification, collection, acquisition, and preservation of digital evidence* [Online] Available from: <http://www.iso27001security.com/html/27037.html>. [Accessed: 25 March 2017].

Lessard, J. & Kessler, G. (2010). Android Forensics: Simplifying Cell Phone Examinations. *ECU University Publication*. [Online]. Available from: <http://ro.ecu.edu.au/ecuworks/6479/>. [Accessed: 5 April 2017].

Lohrum, M. (2014). *Live imaging an Android device*. [Online]. 2014. [Freeandroidforensics.blogspot.co.uk](http://freeandroidforensics.blogspot.co.uk). Available from: <http://freeandroidforensics.blogspot.co.uk/2014/08/live-imaging-android-device.html>. [Accessed: 1 May 2017].

Martin, A. (2013). *How to restore a Galaxy Note 2 from rooted to factory settings*. [Online]. 2013. CNET. Available from: <https://www.cnet.com/uk/how-to/how-to-restore-a-galaxy-note-2-from-rooted-to-factory-settings/>. [Accessed: 3 May 2017].

Pirvu, B. (2017). *Root Samsung Galaxy Note 2 on Android 4.4.2 KitKat*. [Online]. Available from: <http://www.android.gs/root-samsung-galaxy-note-2-on-android-4-4-2-kitkat/>. [Accessed: 29 April 2017].

Son, N., Lee, Y., Kim, D., James, J., Lee, S. & Lee, K. (2013). A study of user data integrity during acquisition of Android devices. *Digital Investigation*. [Online]. 10. pp. S3-S11. Available from: <http://www.sciencedirect.com/science/article/pii/S1742287613000479>. [Accessed: 3 April 2017].

Vidas, T., Zhang, C. & Christin, N. (2011). Toward a general collection methodology for Android devices. *Digital Investigation*. [Online]. 8. pp. S14-S24. Available from: <http://www.elsevier.com/locate/diin>. [Accessed: 3 April 2017].

Votipka, D., Vidas, T. & Christin, N. (2013). Passe-Partout: A General Collection Methodology for Android Devices. *IEEE Transactions on Information Forensics and Security*. [Online]. 8 (12). pp. 1937-1946. Available from: <http://ieeexplore.ieee.org/document/6628001/>. [Accessed: 3 April 2017].