



**BUSITEMA
UNIVERSITY**
Pursuing Excellence

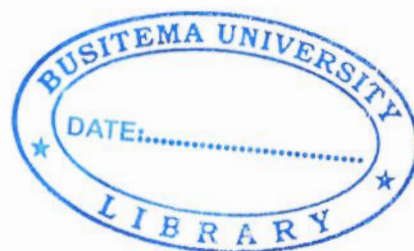
**FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTER ENGINEERING**

**FRAMEWORK FOR FORENSIC ANALYSIS OF EVIDENCE FROM NAVIGATION
DEVICES POWERED BY ANDROID OPERATING SYSTEM**

BY

HALONGO GODFREY

BU/GS16/MCF/2



A Dissertation Submitted to the Directorate of Research, Graduate Studies and Innovation in
Partial Fulfillment of the Requirements for the Award of the Degree of Master of Computer
Forensics of Busitema University

September 2019

DECLARATION

I hereby declare that, except where quotations have clearly been acknowledged, this Dissertation is my original work and has not yet been submitted before for the award of any university degree.

Signature:  Date: 10/09/2019

Halongo Godfrey

BU/GS16/MCF/002




APPROVAL


This is to certify that the following Dissertation has been prepared by Halongo Godfrey under the title:

**“FRAMEWORK FOR FORENSIC ANALYSIS OF EVIDENCE FROM NAVIGATION
DEVICES POWERED BY ANDROID OPERATING SYSTEM”**

Supervisors:

Signature:  Date: 11/09/2019

Dr. Semwogerere Twaibu
Faculty of Engineering
Busitema University,
P.O Box 226,
Busia.

Signature:  Date: 11/09/2019

Mr. Bwire Felix
Faculty of Engineering
Busitema University,
P.O Box 226,

Busia.

DEDICATION

I dedicate this work to my beloved parents Mr. Asobola Patrick, Mrs. Phoebe Nafula Asobola, my lovely wife Nahigo Manjeri and my children Martha, Othniel and Nathanael.

ACKNOWLEDGEMENTS

I thank the Almighty God who has given me wisdom, favor and good health to carrying out this Project.

I thank in an exceptional way my supervisor Dr. Semwogerere Twaibu for his invaluable guidance and patience throughout this dissertation. I appreciate your facilitation during this study.

I will not forget about the advice and guidance offered to me by my second supervisor, Mr. Bwire Felix. I remember when I came to a standstill at the time of research designing; the guidance you offered to me gave me a break through.

I want to remember the guidance and encouragement given by Mr. Ocen Gilbert thanks for sacrificing your valuable time.

I recognize Mr. Ogwang Nixon thanks for the help and contribution during the time of data collection. My appreciation goes to my classmates who supported me in one way or the other to see that the objectives of this study are achieved. They include: Ms. Ikwap Agatha, Mr. Nafuye Ivan and Mr. Kitembo Moses.

I may not mention all but my prayer is that God may bless even all those whose contribution deserves recognition.

TABLE OF CONTENTS

DECLARATION	i
APPROVAL	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
TABLE OF CONTENTS	v
LIST OF FIGURES	viii
LIST OF TABLES	ix
LIST OF ACRONYMS	x
ABSTRACT	xi
CHAPTER ONE	1
INTRODUCTION	1
1.1 Back ground	1
1.2 Problem statement	3
1.3 Main objective	3
1.3.1 Specific objectives	3
1.3.2 Research questions	3
1.4 Significance of study	4
1.5 Scope	4
CHAPTER TWO	5
LITERATURE REVIEW	5
2.1 Introduction	5
2.2 Navigation Devices	5
2.2.1 Standalone navigation devices	5
2.2.2 Assisted GPS navigation devices	6
2.3 Android devices	7
2.3.1 Android OS architecture	7
2.3.2 File system and partitions	9
2.4 Data extraction methods	9
2.5 Android forensic tools	11
2.6 Challenges for android forensics	12

2.7 Existing frameworks.....	13
2.8 ACPO guidelines and NIST publications.....	16
2.9 The concept from McKemmish model (1999)	16
CHAPTER THREE	18
METHODOLOGY	18
3.1 Introduction.....	18
3.2 Research methods.....	18
3.3 Research strategy.....	18
3.3.1 Design Science.....	18
3.3.1.1 Environment	20
3.3.1.2 IS research	20
3.3.1.3 Knowledge base.....	21
3.4 Ethical considerations.....	22
CHAPTER FOUR	24
THE FINDINGS FROM THE FIELD STUDY	24
4.1 Introduction.....	24
4.2 The field study and the Descriptive Statistics.....	24
4.2.1 Respondent background.....	25
4.2.2 Awareness and usage of operating systems and mapping applications.....	27
4.2.3 Barriers to forensic analysis of android navigation devices.....	29
4.2.4 Geo-data extraction.....	30
4.2.5 Recovery and analysis of historical locational data.....	30
4.2.6 Current location of the android navigation device user.....	33
4.3 Summary of the constructs to the framework.....	37
CHAPTER FIVE	39
A frame work for forensic analysis of android navigation device.....	39
5.1 Introduction.....	39
5.2 Theoretical Contribution from McKemmish model	40
5.3 Contribution from field survey Analysis	41
5.4 Framework Evaluation.....	41
CHAPTER SIX.....	44
Discussion of findings, recommendations and conclusions	44

6.1 Introduction.....	44
6.2 Discussion of Findings	44
6.2.1 State of android navigation devices and barriers to their forensic analysis.....	45
6.2.2 Scope of locational data available from android navigation devices that can be used to discern between destinations only searched for and those actually traveled to	46
6.2.3 The framework for forensic analysis of android navigation devices.....	46
6.3 Summary of Contributions: Meeting Research Objectives	47
6.4 Recommendations.....	47
6.5 Conclusion	48
References.....	49
Appendices	53

LIST OF FIGURES

Figure 2.1: Android Os architecture.....	8
Figure 2.2: Maus framework.....	14
Figure 3.1: Information system research framework.....	19
Figure 5.1: The framework for forensic analysis of android navigation devices.....	40

LIST OF TABLES

Table 2.1: Comparison of android device GPS analysis frameworks	15
Table 3.1: sample size.....	22
Table 4.1: Reliability Statistics of the questionnaire	25
Table 4.2: Respondents background.....	26
Table 4.3: Use of operating systems.....	27
Table 4.4: Type of mapping applications used.....	28
Table 4.5: Preference of data extraction technique.....	28
Table 4.6: Explanation for preferred technique.....	29
Table 4.7: Barriers to forensic analysis of android navigation devices	29
Table 4.8: Explanation for the necessity of OS geo-data.....	30
Table 4.9: Technique likely to recover historical locational data.....	31
Table 4.10: Type of tool likely to recover historical locational data.....	31
Table 4.11: Information likely to be retrieved from an android navigation device.....	32
Table 4.12: Possibility of identifying an android navigation user in motion from historical locational data.....	32
Table 4.13: Information which can be retrieved from an android navigation device for a user in motion.....	33
Table 4.14: Possibility of retrieving current location of the android navigation device from historical location data.....	34
Table 4.15: Relevant datasets in retrieving the current location of the android navigation device user.....	34
Table 4.16: The possibility of identifying the given information from historical locational data of an android navigation device.....	35
Table 4.17: Possibility of being able to distinguish between locations searched for and or traveled to by the android navigation device user.....	36
Table 4.18: Description of how locations only searched for can be distinguished from locations searched for then traveled to.....	37
Table 5.1: Reliability Statistics of the evaluation questionnaire.....	42
Table 5.2: Evaluation questionnaire responses.....	42

LIST OF ACRONYMS

ACPO	Association of chief police officers
ADB	Android debugging bridge
CSV format	comma-separated values
GPS	Global positioning system
HTCI	High Tech Crime Investigation
JTAG	Joint Test Action Group (named after)
NIST	National Institute of Standards and Technology
OS	Operating System
SD Card	Secure Digital card
AGPS	Assisted global positioning system

ABSTRACT

The use of hand-held dedicated GPS (Global positioning system) devices for navigation such as Garmin, Tom-Tom, Mio Technology, Navman, and Magellan has been reducing while the use of Smartphones as navigation devices has increased where by the navigation application system has been integrated into the Smartphone itself. Conducting GPS routing using a smartphone phone is convenient as there would be no need to have another device for GPS navigation devices. The use of this technology is associated with certain crimes, forensic analysis of android navigation devices (android smartphone) is necessary. This study aimed at developing a framework for forensic analysis of forensic data originating from android navigation devices. A descriptive field study using a questionnaire was carried out to find out constructs important for the design of a framework for forensic analysis of android navigation devices. The designed framework was evaluated in a questionnaire based field study and the results showed that; the use of logical technique for data extraction of data as is easy to understand and work with allowing innovation and facilitates direct communication with operating system of the device, analysis of mapping application dataset complemented with operating system dataset gains additional information and also improve on the accuracy of information gained and reconstruction of traces of geo-data like last selected destination and home location coupled with timestamps such as start time of the journey and end time of the journey can be used for reconstruction of the motion of the android navigation device user to enable a digital forensic expert to discern between locations only searched for and locations traveled to by the android navigation device user.

CHAPTER ONE

INTRODUCTION

1.1 Back ground

GPS technology has substituted the use of printed folding maps for navigation. GPS is a network of 24 satellites placed in a geostationary orbit about twenty thousand kilometers from earth with enabled Synchronized atomic clocks to transmit the accurate time and position in space[1][2]. A GPS receiver device's function is to locate four or more of these satellites, find out the distance to each satellites and use this information to come up with its own location[3][4]. GPS was originally developed as a tool for the military by the United States Department of Defense in 1970. It then became selectively available to the civilians in 1980s and full availability was in 2000, thereby increasing its accuracy[5][6].

The accuracy and reliability of navigation systems are highly dependent on the amount of tracked satellites and the satellite geometry[6], which can be degraded in low satellite visibility areas. To operate properly, the GPS receivers need signals from at least four satellites of the 24 and clear views of the sky. The system is based on using the clear line of sight hence there can be errors and inconsistencies when signals pass through obstacles such as buildings and clouds.

There two main categories of GPS receivers that is; built-in and mobile, the built-in devices are those that are permanently placed in a specific area for operation and the use of the GPS technology is focused on a specific task, mobile units are available that allow GPS functionality built into a small units including those that fit on the wrist, and others which can be hung around the neck[7]. The use of hand-held GPS devices such as Garmins, Tom Tom, Mio Technology, Navman, and Magellan has been reducing while the use of Smartphones as navigation devices has increased where the navigation application system has been integrated into the Smartphone itself[4][8][9]. Most cellular vendors are now offering phones and data plans that support the use of GPS and they work very similar to the smaller vehicle units used to obtain routing information and input addresses of interest. Conducting GPS routing using a smartphone phone is extremely convenient as it eliminates the need to have another device devoted to GPS navigation[7]. Smartphones for GPS navigation has now become a handy tool incorporated inside a device that many people have with them at all times.

References

- [1] . P. S., "geo-location based augmented reality application," *Int. J. Res. Eng. Technol.*, vol. 04, no. 07, pp. 495–498, 2015.
- [2] Hannay, P. (2008). Forensic acquisition and analysis of the tomtom one satellite navigation unit. Paper presented at the Proceedings of the 6th Australian Digital Forensics Conference, Perth Western Australia.
- [3] S. P. Umratkar and P. R. Kumar, "SecureChild - Children Tracking Android Application," *Int. J. Sci. Res. Manag.*, vol. 3, no. 3, pp. 2441–2451, 2015.
- [4] P. N. Ramakrishnan, "Forensic Analysis of Navigation System (Gps) A Case Study," *J. Forensic Sci. Crim. Investig.*, vol. 7, no. 4, pp. 1–6, 2018.
- [5] P. Hannay, "Satellite Navigation Forensics Techniques," *Proc. 7th Aust. Digit. Forensics Conf. Ed. Cowan Univ. Perth West. Aust.*, pp. 14–18, 2009.
- [6] B. Chapman, "Utilizing GPS to Track Crime Scene Investigators Within a Crime Scene and Monitoring Their Fatigue Veronica D * Souza," pp. 1–76, 2017.
- [7] C. Strawn, "Expanding the Potential for GPS Evidence Acquisition," *Small scale digital device forensics journal*, vol. 3, no. 1, 2009.
- [8] N. A. Abdullah and N. Mohd Rashid, "acquiring cybercrime evidence on mobile global positioning system (gps): review," *Acta Electron. Malaysia*, vol. 1, no. 2, pp. 17–19, 2018.
- [9] J. Moore, I. Baggili, and F. Breitingner, "Find Me If You Can: Mobile GPS Mapping Applications Forensic Analysis & SNAVP the Open Source, Modular, Extensible Parser," *J. Digit. Forensics, Secur. Law*, vol. 12, no. 1, 2017.
- [10] G. M. Jones, S. G. Winster, and P. Scholar, "Forensics Analysis On Smart Phones Using Mobile Forensics Tools," *Int. J. Comput. Intell. Res. ISSN*, vol. 13, no. 8, pp. 973–1873, 2017.
- [11] Forensic analysis of geodata in android smartphones. In International conference on cybercrime, security and digital forensics, <http://www.schuba.fh-aachen.de/papers/11-cyberforensics.pdf> S.
- [12] Hannay, P. (2008). Forensic acquisition and analysis of the tomtom one satellite navigation unit. Retrieved from <http://ro.ecu.edu.au/adf/45/>

- [13] F. Freiling, S. Schmitt and M. Spreitzenbarth, Forensic analysis of smartphones: The Android Data Extractor Lite (ADEL), presented at the ADFSL Conference on Digital Forensics, Security and Law, 2011
- [14] R. Diepeveen,(2016) "University of Amsterdam MSc System and Network Engineering Computer Crime & Forensics Forensics on mobile travel planner applications,"un-published master's thesis university of Amsterdam, Netherlands.
- [15] Hannay, P. (2007). A Methodology for the forensic acquisition of the TomTom One satellite navigation System—A research in progress. Paper presented at the Proceedings of The 5th Australian Digital Forensics Conference.
- [16] P. Hannay and P. Hannay, "Forensic Acquisition and Analysis of the TomTom One Satellite Navigation Unit," 2008.
- [17] A. Arbelet, "Garmin satnavs forensic methods and artefacts : An exploratory study School of Computing," no. August, 2014.
- [18] W. T. B. FCC, "Location-Based Services: an overview of opportunities and other considerations," 2012.
- [19] A. E. Stefan Steiniger, Moritz Neun, "Foundations of Location Based Services Lesson 1 CartouCHE 1- Lecture Notes on LBS," vol. 1.0, pp. 1–28, 2005.
- [20] A. Thach, Elizabeth C., Thompson, Karen J., Morris, "A fresh look at followership: A model for matching Followership and leadership styles," *J. Behav. Appl. Manag.*, vol. 91, no. 1, pp. 1–5, 2006.
- [21] Z. Jovanovic, "Android Forensic Techniques," p. 20, 2012.
- [22] M. Quick, Darren Alzaabi, "Forensic analysis of the android file system YAFFS2," *Proc. 9th Aust. Digit. Forensics Conf. Ed. Cowan Univ. Perth West. Aust.*, vol. 8, no. 2, pp. 101–109, 2011.
- [23] A. Mahajan, M. S. Dahiya, and H. P. Sanghvi, "Forensic Analysis of Instant Messenger Applications on Android Devices," *Int. J. Comput. Appl.*, vol. 68, no. 8, pp. 38–44, 2013.
- [24] G. Madhuri and R. Sheth, "Mobile Device Forensics: Extracting Data from Unallocated Space," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 6, no. 6, pp. 1046–1049, 2017.
- [25] A. Mitra, "Social Forensics in Mobile Phones - Analysis of the temporal dimension of Evidence

Storage," no. January, 2015.

- [26] V. Rao and A. S., "Survey on Android Forensic Tools and Methodologies," *Int. J. Comput. Appl.*, vol. 154, no. 8, pp. 17–21, 2016.
- [27] L. Chen and H. Zhao, "Forensic Analysis of Cloud Storage on Android Volatile Memory," 2017, pp. 20–26.
- [28] Hoog, A. (2011). *Android Forensics* (Vol. 1st Ed). Waltham, MA, USA: Syngress.
- [29] B. Felix Jeyareuben Chandrakumar, K.-K. Raymond Choo and B. Martini, "An evidence-based Android cache forensics model," 2014.
- [30] Abalenkovs, D., Bondarenko, P., Pathapati, V. K., Nordb, A., Piatkivskyi, D., Rekdal, J. E., & Ruthven, P. B. (2012). *Mobile Forensics: Comparison of extraction and analyzing methods of iOS and Android*.
- [31] C. Paper, S. Hazra, A. V. Vidyapeetham, and P. Mateti, *Advances in Security in Computing and Communications*, vol. 746, no.1 November 2017.
- [32] V. Vijayan, R. Ludwiniak, and G. McCara, "Android Forensic Capability and Evaluation of Extraction Tools," no. 1 April, 2012.
- [33] P. Lindberg, "Challenges in Mobile Phone Antenna Development," in *Design of Ultra Wideband Antenna Matching Networks*, vol. 1, 2008, pp. 45–66.
- [34] T. Edward, A. Barton, and M. A. H. Bin Azhar, "Forensic Analysis of the Recovery of Wickr 's Ephemeral Data on Android Platforms," no. c, pp. 35–40, 2016.
- [35] A. Boztas, A. R. J. Riethoven, and M. Roeloffs, "Smart TV forensics: Digital traces on televisions," *Digit. Investig.*, vol. 12, no. S1, pp. S72–S80, 2015.
- [36] J. Kizza, F. Migga Kizza, J. Kizza, and F. Migga Kizza, "Digital Evidence and Computer Crime," in *Securing the Information Infrastructure*, 2011, pp. 298–317.
- [37] J. F. Molina-Azorin, "Mixed methods research: An opportunity to improve our studies and our research skills," *Eur. J. Manag. Bus. Econ.*, vol. 25, no. 2, pp. 37–38, 2016.
- [38] L. Pavelek, "Approaches for selecting the correct research strategy," in *Proceedings in Scientific Conference*, 2013, no. June 2013, pp. 251–253.

- [39] M. Swamynathan, *Mastering Machine Learning with Python in Six Steps*, vol. 19, no. 2, 2017.
- [40] Hevner, March, Park, and Ram, "Design Science in Information Systems Research," *MIS Q.*, vol. 28, no. 1, p. 75, 2004.
- [41] B. Martini and K. K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*, vol. 9, no. 2. Elsevier Ltd, pp. 71–80, 2012.
- [42] S. Rajasekar *et al.*, "Research Methodology," *J. Math. Behav.*, vol. 68, no. s1, p. 23, 2006.
- [43] R. Heale and A. Twycross, "Validity and reliability in quantitative research Validity and reliability in quantitative studies," no. August, 2015.
- [44] H. Mohajan and H. K. Mohajan, "M P RA Two Criteria for Good Measurements in Research: Validity and Reliability Two Criteria for Good Measurements in Research: Validity and Reliability," *Ann. Spiru Haret Univ.*, vol. 17, no. 3, pp. 58–82, 2017.
- [45] R. McKemmish, "What is forensic computing?," *Trends Issues Crime Crim. Justice*, vol. 118, no. 118, pp. 1–6, 1999.
- [46] Andri P Heriyanto, "Procedures and Tools for Acquisition and Analysis of Volatile Memory on Android Smartphones," pp. 84–95, 2013.