ACQUISITION OF CLOUD DATA REMNANTS IN
ANDROID SMART PHONES

BY
FAITH REHEMA MWENI

UNITED STATES INTERNATIONAL
UNIVERSITY-AFRICA

SUMMER 2016
ACQUISITION OF CLOUD DATA REMNANTS IN ANDROID SMART PHONES

BY
FAITH REHEMA MWENI

A Project Report Submitted to the School of Science and Technology in Partial Fulfillment of the Requirement for the Award of the Degree of Master of Science in Information Systems and Technology

UNITED STATES INTERNATIONAL UNIVERSITY-AFRICA

SUMMER 2016
STUDENT’S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University in Nairobi for academic credit.

Signed: ___________________________ Date: ______________

Faith Rehema Mweni (ID No 608184)

This project has been presented for examination with my approval as the appointed supervisor.

Signed: ___________________________ Date: ______________

Prof. Gerald Chege

Signed: ___________________________ Date: ______________

Dean, School of Science and Technology
COPY RIGHT

All rights reserved. No part of this project may be photocopied, recorded or otherwise reproduced, stored in retrieval system or transmitted in any electronic or mechanical means without prior permission of USIU-A or the author.

Faith Rehema © 2016
Abstract

Smart phones are powerful minicomputers characterized by high performance, large memory capacity and enhanced applications that enable various ways of communication. They are widely used for other purposes besides making phone calls, for instance browsing the internet, reading and responding to emails, road navigation, editing documents, video conferencing, playing music, taking videos and photo, to mention but a few.

The problem at hand is that forensic investigators often encounter difficulty in identifying service providers, accounts credentials like username and passwords and cloud data remnants. This can be provided by the seizure and analysis of data contained in smart phones such as Android devices. There is an emerging trend where criminals use cloud computing to propagate and perform acts of crime like child pornography, which puts into perspective the importance of the study in acquisition of sound forensic tools and techniques that will ensure evidence is admissible before a court of law.

The project was intended at expounding on the following research questions. Firstly, what were the cloud data remnants on a smart phone and where are they located in current Android versions? Secondly, how can these cloud data remnants be forensically acquired from a smart phone? The third question looks into the forensic implication of accessing and downloading cloud data from Google Drive™, Dropbox™ and One Drive® on a Smart phone.

The project explored ways of collecting data from cloud storage accounts with the help of browsers and client software, the use of forensics software thereafter performing a comparison with the original evidence files with the use of a digital forensics framework.

The key findings from the acquisition included log files, the downloaded files and memory captures of some files resident on the clients.

In conclusion, the experiments established that no modifications were made during the process. Notable though was the change of timestamps which should be considered in the assumptions of creation, modification and access times associated with files downloaded via client software.
Recommendations are that the relevant organs in Kenya should gazette laws for the utilization of digital forensics tools for the admissibility of evidence in court of laws. The current evidence act (Republic of Kenya, 2014) does not clearly define the method of acquiring digital evidence or the open source and licensed tools to be utilized, though it explicitly states that electronic records are admissible court.

Future studies can incorporate use of licensed forensics software to retrieve evidential data from new Android versions like Marshmallow. The national government should also initiate activities for the drafting of national mobile forensic guidelines to govern the acquisition of data remnants with the use of approved software.
ACKNOWLEDGEMENT

This project was completed at the Faculty of Information Systems and Technology in the School of Science and Technology at the United States International University – Nairobi. The research and writing of this project has been one of the most significant academic challenges I have encountered. In the absence of support and guidance of the following people, this study would not have been completed. It is to them that I owe my deepest gratitude.

First and foremost, I would like to express my deepest gratitude to God for the strength, knowledge, wisdom, patience and perseverance during the entire Masters program, and indeed throughout my life. Indeed “I can do all things through Christ who strengthens me” (Philippians 4:13)

I would like to thank my husband - Gidi - for the support, encouragement, patience and great sacrifice accorded in order to attain this milestone in my life. To my children - Chaka and Mupa - for their support and unwavering love during my absence and spending many nights without my total attention. Your attitude towards my studies helped me push till the very end.

I especially want to thank my loving mother and ambitious dad who all provided amazing support and encouragement during the course of this program, as well as at every stage of my life.

Heartfelt gratitude to my Life Group - O.P.E.G (Ordinary people, Extra Ordinary God) for their unwavering support and continuous prayers during the entire project.

I would sincerely like to thank my supervisor, Prof. Gerald Chege for giving me the opportunity to conduct this project under his guidance.

I am thankful for support accorded throughout the entire course by the MIST, USIU pioneer class 2014, may God bless you abundantly in your endeavors.

Thanks also to all friends and workmates I have not already mentioned, many of whom stimulated and encouraged me along the way, providing me with new insights and ideas every single time.
# Table of Contents

Abstract ................................................................................................................................. iv

List of Tables .......................................................................................................................... ix

List of Figures ........................................................................................................................ x

**CHAPTER ONE** .................................................................................................................. 1

1.0 INTRODUCTION .............................................................................................................. 1

1.1 Background ....................................................................................................................... 1

1.2 Statement of the Problem ................................................................................................. 2

1.3 Purpose of the Study ......................................................................................................... 3

1.4 Research Questions ......................................................................................................... 3

1.5 Rationale of the Study ..................................................................................................... 4

1.6 Scope of the Study ........................................................................................................... 4

1.7 Definition of Terms ........................................................................................................ 4

1.8 Chapter Summary ........................................................................................................... 5

**CHAPTER TWO** ............................................................................................................... 6

2.0 LITERATURE REVIEW .................................................................................................. 6

2.1 Introduction ...................................................................................................................... 6

2.2 Smart Phone Cloud Data Remnants and Their Locations ............................................. 7

2.3 Acquisition of Cloud Data Remnants ............................................................................ 13

2.4 Implications of the Cloud Data Remnants in Smart Phone Forensics ....................... 17

2.5 Chapter Summary .......................................................................................................... 19

**CHAPTER THREE** .......................................................................................................... 20

3.0 METHODOLOGY ............................................................................................................ 20

3.1 Introduction ..................................................................................................................... 20

3.2 Research Design ............................................................................................................ 20

3.3 Data collection methods ............................................................................................... 22

3.4 Research Procedures ..................................................................................................... 23

3.5 Data Analysis Methods ................................................................................................. 24

3.6 Research Equipment ..................................................................................................... 25

3.7 Research Limitations ..................................................................................................... 25

3.8 Chapter Summary .......................................................................................................... 26

**CHAPTER FOUR** ............................................................................................................. 27
List of Tables
Table 1: File Manipulation Table ............................................................................................................. 24
Table 2: Device specifications used ........................................................................................................... 25
Table 3: Software versions used ............................................................................................................... 26
Table 4: Applying the framework ............................................................................................................ 34
Table 5: Cloud Data Remnant Locations ............................................................................................... 56
Table 6: Date and Time Stamps .............................................................................................................. 62
List of Figures

Figure 1: Android Architecture ............................................................................................. 9
Figure 2: Mobile Device Tool Classification System ............................................................... 14
Figure 3: Block diagram of Research scope ........................................................................... 21
Figure 4: The Digital Forensics Framework ............................................................................ 29
Figure 5: Samples Created on Windows 7 Machine ............................................................... 35
Figure 6: Possible locations for both the Samsung and Huawei devices ............................... 36
Figure 7: The Inception of the Analysis of Samsung A5 ......................................................... 37
Figure 8: The Inception of the Analysis of Huawei D200 ...................................................... 38
Figure 9: Analysis via the Client ............................................................................................ 38
Figure 10: Analysis via a Client in the Scratch Folder .......................................................... 39
Figure 11: Samples created on Windows 7 Machine ............................................................. 42
Figure 12: Possible locations for both the Samsung and Huawei Devices ......................... 43
Figure 13: Location of Evidence Files in Dropbox – Samsung A5 ....................................... 43
Figure 14: The Inception of the Analysis of Samsung A5 ...................................................... 45
Figure 15: The inception of the analysis of Huawei D200 ..................................................... 45
Figure 16: Synchronized Files in the Dropbox Client ............................................................ 46
Figure 17: Downloads Folder in Huawei D200 ................................................................... 47
Figure 18: Samples Created on Windows 7 Machine ............................................................. 49
Figure 19: Possible Locations for Both the Samsung and Huawei Devices ........................... 50
Figure 20: The Inception of the Analysis of Samsung A5 ...................................................... 51
Figure 21: The inception of the analysis of Huawei D200 ..................................................... 52
Figure 22: Location of Cloud Data Remnants ...................................................................... 52
Figure 23: File Path in the OneDrive Folder ....................................................................... 53
Figure 24: Download Folder in Samsung A5 ....................................................................... 53
Figure 25: No Thumbnails in Huawei D200 ....................................................................... 57
Figure 26: Thumbnails in Samsung A5 ................................................................................. 57
Figure 27: Files Contained in the Scratch Folder ................................................................. 58
Figure 28: The Samsung Connection .................................................................................... 58
Figure 29: The Huawei Connection ...................................................................................... 59
Figure 30: The Logical Copy ................................................................................................. 59
Figure 31: The Hashing Process Using MD5 ........................................................................ 60
Figure 32: The Files and Folder Present in the Dropbox Account ......................................... 61
Figure 33: Files and the Date Modified ................................................................................ 61
CHAPTER ONE

1.0 INTRODUCTION

1.1 Background
Cloud computing introduced a paradigm shift in the access of computer resources over a network, in an intranet of over the internet. Essentially it is the hosting of electronic data in remote infrastructure as compared to storing it locally on computing device. NIST defines cloud computing as a computing model for enabling ubiquitous convenient, on demand network access to a shared pool of configurable computing resources (e.g., network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction Mell and Grance (2011).

It is projected that cloud computing will be fully incorporated into business operations to enhance growth, widen the scope and maximize on the potential of existing infrastructure and resource maintenance (Vidalis, 2010). Thus cloud computing and the respective storage options are deeply intertwined in smart phones and other mobile devices alike. Despite the advantages with mobile devices and respective cloud storage, there is rising concern of acquiring digital evidence from remote, distributed and virtualized cloud obstructs (Glisson, 2012).

Indeed it is an arduous task to use traditional forensic tools in the retrieval and investigation of data located on smart phones. Never the less, there is a probability of accessing these artifacts located on a smart phone during mobile forensics investigation using current and robust forensics tools. There exists a wide range of cloud storage services such as Google Drive™, OneDrive and Dropbox™. These services can be accessed using a web browser or client software installed on the smart phone

Unfortunately Kenya does not have Mobile Device Forensics guidelines for guidance but NIST provides that interaction with identified data should be done in accordance with certain procedures to ensure admissibility of evidence in a court of law (Jansen, Ayers, & Brothers, 2014). Despite passing the Data Protection Bill 2012, which regulates the collection, processing, storing, use and disclosure of information relating to individuals that is processed through automated or manual means and for connected purposes ( Laws Of Kenya, 2012),
Kenya has not instituted any procedures, standards and toolkits for presentation of digital evidence in a court of law. On the other hand, Kenyan laws offer provisions for the admissibility of electronic evidence in a court of law under the proposed Security Laws Amendment Bill (Republic Of Kenya, 2014). Timely seizure of the cloud data remnants is of essence due to the volatile nature of cloud data artifacts which can be moved or modified with frequent access to the Internet.

1.2 Statement of the Problem

Data located on the cloud may be virtualized, sparsely distributed across the world and majorly transient thus posing a technical and jurisdictional dilemma to digital forensic investigators in the identification, acquisition and seizure of forensic evidence within a stipulated timeframe (Taylor, Haggerty, Gresty, & Hegarty, 2010). Forensic investigators often encounter difficulty in identifying service providers and accounts credential like username and passwords. This can be provided by the seizure and analysis of data contained in smart phones such as Android, iOS, Symbian and Blackberry devices.

Acquisition of admissible evidence located in smart phones offers a new challenge as there are new ways of protecting smart phones from forensic investigations with the use of anti-forensic software, leaving forensic investigators with inappropriate tools to perform thorough investigations. There is an emerging trend where criminals use cloud computing to propagate and perform acts of crime like child pornography, which necessitates for the acquisition of sound forensic tools and techniques that will ensure evidence is admissible before a court of law.

Due to the remote aspect of evidence, absence of physical mobile contact, and trust to uphold confidentiality, integrity and authenticity, cloud computing changes the perspective and scope of traditional forensics. Law enforcers and investigation units are concerned about the timely acquisition of evidence stored in a Smartphone. Timely seizure of the cloud data remnants is of essence due to the volatile nature of cloud data artifacts which can be moved or modified with frequent access to the Internet.
1.3 Purpose of the Study
Data located in the cloud is available anytime for investigation or for criminals who use crime for personal gain. Cloud computing and the respective services are widely used across different applications which includes web applications and mobile applications. Based on the initial analysis of the research against the cloud based mobile forensics, it is apparent that there are grey areas in literature that focus on aspects like remote data acquisition, examination and analysis where the traditional mobile forensic tools may be inappropriate in offering a comprehensive investigation (Breeuwsma, 2013).

User or company data is managed and maintained over a remote location across the cloud storage models and the respective security architecture and policies are imposed to ensure the data integrity, reachability and reliability. With the dynamic nature of anti forensics there is a need to conduct comprehensive tests on current tools on their ability to recover data artifacts in a sound manner to be admissible in a court of law. The purpose of this project was to demonstrate the timely forensic identification, preservation, analysis and presentation of cloud data remnants in smart phones using robust forensics software.

1.4 Research Questions

The project focused on the retrieval of cloud data remnants on smart phones and incorporated a computer running Windows 7, a Samsung A5 running 5.0.2 (Lollipop) and a Huawei D200 running 4.1.2 (Jelly Bean). Very few investigations have been conducted on recent releases of JellyBean and Lollipop. In order to guide the investigation procedures, it is important to adopt a framework that can be applied by forensic investigators to fulfill their obligations. For this to be attained, the project dwelt on the following research questions:

1. What were the cloud data remnants on a smart phone and where are they located in current Android versions?
2. How can these cloud data remnants be forensically acquired from a smart phone?
3. What was the forensic implication of accessing and downloading cloud data from Google Drive™, Dropbox™ and One Drive® on a Smartphone?
1.5 **Rationale of the Study**

The rationale of this study was to propose for the use of appropriate mobile forensic tools to produce relevant evidence from smart phones. It charted a path for the acquisition of evidence admissible before a court of law and proposed for the drafting of national mobile forensic guidelines to govern the acquisition of data remnants. It also presented the types of cloud data artifacts available from a smart phone and their inherent roles in smart phone forensics.

1.6 **Scope of the Study**

The project concentrated on cloud data remnant acquisition from Android smart phones which access and download information from Google Drive™, Dropbox™ and One Drive®. The versatility of cloud computing gives criminals opportunities to commit crimes and immediately delete any incriminating evidence, such circumstances will not be considered in this project. Peer to peer cloud computing as experienced by Bit Sync™ was not be part of the study as integrity features cannot be applied on the evidence as compared to the client server architecture of the selected cloud computing services. Anti forensics is a wide subject which was not be part of this project, the project concentrated the consequence of using Google Incognito mode.

1.7 **Definition of Terms**

**Acquisition** – A process by which digital evidence is duplicated, copied, or imaged (Ayers, Brothers, & Jansen, 2014).

**Analysis** - The examination of acquired data for its significance and probative value to the case (Ayers et al., 2014)

**Chain of Custody** – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for any transfers (Ayers et al., 2014)

**Cloud computing** - is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage,
applications and services) that can be rapidly provisioned and released with minimal management (Mell & Grance, 2011).

**Deleted File** – A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data (Ayers et al., 2014).

**EEPROM** - Electrically Erasable Programmable Read-Only Memory is user-modifiable read-only memory (ROM) that can be erased and reprogrammed (written to) repeatedly through the application of higher than normal electrical voltage (Rouse, 2010).

**File System** – A software mechanism that defines the way that files are named, stored, organized, and accessed on logical volumes of partitioned memory (Ayers et al., 2014)

**Hashing** – The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data (Ayers et al., 2014)

**Smart phone** – It is a mobile phone with highly advanced features with a high-resolution touch screen display, WiFi connectivity, Web browsing capabilities, and the ability to accept sophisticated applications (Techopedia, 2016).

### 1.8 Chapter Summary

The chapter introduced the basic concept of the project, the importance of the topic, the rationale and objectives. Research questions are also included. The following chapter provided a detailed literature review on cloud computing in relation to smart phone forensics.
CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

Literature provides that cloud forensics is complex, tedious and unpredictable as compared to traditional digital forensics. Cloud storage services have the potential of being misused by criminals to propagate heinous crimes. This poses a challenge in the identification and acquisition of evidence when different cloud services are used. Cloud forensics can be defined as the science of gathering, analyzing and documenting evidence of data from a cloud environment in a sound and secure manner to be admissible before a court of law. Literature provides that investigation of cloud computing environments is increasingly becoming complex as compared to traditional digital forensics.

There exists a wide range of cloud storage services such as Google Drive™, One Drive® and Dropbox™. These services can be accessed using a web browser or client software installed on the Smart phone. Unfortunately smart phones can be exploited by criminals to propagate all manner of crimes ranging from child exploitation material, terrorism related information and drug trafficking material. It offers an avenue for criminals to evade investigations by law enforcers and presents a difficulty in pointing out ownership of illegal data (Biggs & Vidalis, 2009).

Smart phones have revolutionized traditional desktops and laptops where connectivity to either public or private cloud services is achieved via connectivity to the Internet. Traditional computer forensics tools are considered ineffective and inefficient in performing forensics of crimes propagated in the cloud environment, therefore new approaches and techniques need to considered (Muhammad, Tahar, & Nhien A, 2012). The complexity of cloud forensics is compounded by the need to create sound forensic images during the retrieval of the meta-data from the cloud. The following sections outline research work related to this study with respect to cloud data remnants and their locations, retrieval of these remnants on a smart phone, and its implication in admissibility in a court of law.
2.2 Smart Phone Cloud Data Remnants and Their Locations

Smartphone forensics is a subset of a discipline known as digital forensics which focuses on the investigation and acquisition of evidential artifacts in digital devices. This discipline involves the forensic investigation five sections namely data recovery, data analysis, extraction of evidence and subsequent preservation and presentation of evidence (Carrier & Spafford, 2003). Smartphone forensics involves the extraction of evidence from the internal memory of a mobile phone through logical extraction or obtaining a full image of the mobile phone through physical extraction. It is also known as mobile phone forensics. This specific branch emanated from the need to acquire different tools with the ability of extracting forensic data from small embedded devices (Mislan, 2008). This is achieved with the help of various tools for the retrieval and analysis of smart phone data, which are especially important in the extraction of evidence to be admissible in a court of law.

Smart phone forensics is still at it infancy stages, with the forensics tools and techniques grappling to keep abreast to the ever changing device capabilities and operating systems enhancements. It is very important for forensic investigators to recover data on smart phones or its associated accessories before any modifications take place. Therefore time and expertise is essential as each operating system presents unique challenges to forensics investigators. Forensics tools and software should be subject to frequent updates to ensure compatibility with upgraded operating systems versions - which is an expensive and arduous task. This is further complicated by the restrictions put in place to deter access to a device’s memory; this is illustrated by use of the standard UNIX User (UID) and (GID) file permissions for applications thereby restricting access to root (Cardwell, 2011).

This chapter focused on location of cloud data remnants and their location on a smart phone depending on the model and android version in use. Some methods discussed violate NIST’s forensic principles which emphasize that any action made on the original evidence should avoid alteration of the device (Ayers et al., 2014). According to the United Kingdom Association of Chief Police Officers Guidelines (ACPO, 2012), there are four principles for forensics computer analysis; no action should alter data, when access to the original data is warranted, it should be done by a competent authorized investigator, all processes should be
recorded and the investigator should ensure the guidelines are strictly observed. Kenya does not have its own set of principles to follow but adopts the international procedures prescribed.

2.2.1 The Android OS

Android is an open source mobile operating system that runs in over 400 million devices worldwide. It was first unveiled on November 5th 2007 by the Open Handset Alliance with the aim of fostering innovation on mobile devices and giving consumers a far better user experience than what was available on other mobile platforms (Schonfeld, 2007). This Alliance consists of more than 50 mobile technology companies ranging from handset manufactures and service providers to semiconductor manufacturers and software developers, including Acer, ARM, Google, eBay, HTC, Intel, LG Electronics, Qualcomm, Sprint, and T-Mobile. It was based on the Linux 2.6 kernel, with a proven driver model, existing drivers, memory and process management, networking support along with other core operating systems services.

The software architecture (Figure 1) is divided into five layers: Applications, Application Framework, Libraries, Runtime and the Linux Kernel (Maia, Noguiera, & Phino, 2010). Applications, is the uppermost layer and provides access to a set of core applications. The Application Framework layer implements a software framework that reassembles functions used by existing applications. All available libraries are written in C/C++ and called through a Java interface. The runtime consists of a set of core libraries and a Dalvik virtual machine. The Linux kernel is the bottommost layer is, which allows for interaction between the upper layers by means of device drivers (Maia, Noguiera, & Phino, 2010).
Numerous smart phones used Yet Another Flash File System 2 (YAFFS2) until the release of version 2.2 (Froyo), (Zimmermann, Spreitzenbarth, Schmitt, & Freiling, 2012). YAFFS2 was developed in 2004 to accommodate larger sized AND (Not-AND) flash devices (Lessard & Kessler, 2010). There was a big switch from YAFFS2 to Fourth Extended (EXT4) file system with the release of version 2.3 (Gingerbread) (Zimmermann, Spreitzenbarth, Schmitt, & Freiling, 2012). Multi core chipsets would have experienced setbacks with YAFFS2, whose design was single threaded. The EXT4 file system is currently the most utilized file systems in Linux, with no limitations and is robust on multi-core devices. The disk space of the EXT4 file system is divided into logical blocks, which reduces management overhead and improves throughput (Kim & Kim, 2012). The EXT4 file systems experiences reduced management overhead due to division of the disk space into logical blocks (Kim & Kim, 2012). These core features of the EXT4 file system endorse the development of advanced applications and functionalities.
The Android architecture regularly improves to support more robust applications. It is therefore imperative to keep abreast with changes and be in touch with current research.

2.2.2 Cloud Data Remnants and Their Location

The popularity of smart phones has seen exponential growth in recent years which is directly proportional to the amount of evidence stored in these devices propagated by both cyber and traditional criminals. Smart phones have numerous types of evidential information including phone call logs, cookies, GPS location, photos, videos, notes, web artifacts, user names and passwords, documents, logs and cloud client application data. The extraction of these forensics artifacts is common place, but there has been great interest in data contained in third party cloud applications installed on smart phones. This is attributed to the fact that cloud applications store potential data that can be used during a criminal investigation and eventually in a court of law as evidence.

Koppen, Gent, Bryan, DiPippo and Kramer (2012) identified numerous key locations that cloud data remnants can reside in namely; cached websites, web history, cookies, installed files and registry entries and modified files. They also identified cloud data remnant sets in installed or accessed cloud application files and used software to analyze these files and extracted particular data of relevance for building a case.

According to Thakur (2013) Android applications store data and its remnants in two major locations, namely: external and internal storage. Data is stored and managed in any given location in the external storage (SD card), on the other hand Android APIs control the storage of data in internal storage. In installed applications data is stored in the applications’ subdirectories for instance /data/data/com/Dropbox which further contain various subdirectories. Common subdirectories are lib, files, cache and databases which can all be controlled by the application developers. Cloud data remnants can also be located in the particular browser used.

Applications request for various permissions for acceptance before installation can be performed on a smart phone. These permissions may request access to external storage, the camera, the internet and the phone book. For these resources to be accessed, the developer should explicitly state so in the application’s “Manifest.xml” file located in the Application Package (Martini & Kim-Kwang, 2015). Java is generally the programming language used in writing applications which is then converted to a (DEX) format with the virtual machine used
in the operating system, commonly referred to as Dalvik Virtual Machine (Dalvik). These multiple applications can run concurrently as each application is its own separate VM. Libraries are the main focus during forensics examinations with special interest in the SQLite databases, with most evidential data crucial to an investigation located here. Files can be stored on either the device's storage or on the removable secure digital (SD) memory card (Lessard & Kessler, 2010).

In addition to permissions granted to normal applications installed in the “/data/app” directory, where “app” is the installed application e.g Dropbox. There are also system level permissions which can be used by applications installed in the “/system/app” directory and signed with the developer key which is used to sign the device’s OS. These applications are known as system applications. The “data” and “system” directories, along with several others, are mountpoints for partitions that are used in order to further compartmentalize the system (Martini & Kim-Kwang, 2015).

A typical device has the following partitions:
- System—Contains system files, system apps, device frameworks
- Data—Contains user installed apps, user data, and Dalvik cache
- cache—Stores temporary system data (such as when installing apps)
- boot—Boot partition, used for normal booting of the device
- Recovery—Recovery mode partition which the device can alternatively boot to

According to Hoog (2011), data resident on Android devices can be divided into two groups: Data at rest and Data in Transit. Data at rest has five locations: NAND-FlashMemory (nonvolatile memory), memory cards such as SD cards, the Embedded MultiMediaCard (eMMC), the SIM card and Android data backups. Data in transit has three locations: Network Service Provider, Physical RAM (volatile RAM) and the Cloud.

Mutawa, Baggili, and Marrington (2012) recommended a technique for the analysis of social networking data artifacts in several smart phones. Once again, for a logical copy to be obtained by the authors, access to user data was gained after rooting the device. Usernames, passwords, profile pictures, and chat messages were retrieved.
Research by Kim, Park and Lee (2012) discussed a technique of analyzing a user’s smart phone usage behavior by taking advantage of ext4 journal logs used by the OS to provide fault tolerance. A logical copy of the data partition of the device was obtained by rooting it and there after running the “dd” command. The authors traced the actions the user performed (such as accessing or deleting a file) by using the journal logs and recovered certain deleted files.

An investigation conducted by Spreitzenbarth, Schmitt and Freiling (2012) also revealed sources of location data on mobile devices and established that the cache stores a huge amount of data from systems applications. The techniques employed by the authors for the acquisition of user data once again required rooting the device in order to gain access to the device.

Researchers, Barghouthy, Marrington and Baggili (2013) demonstrated an approach to retrieve private browsing session information from a smart phone without rooting the device. They established that no private web browsing history was accessible. The device’s user browser history and login credentials were found after rooting the device.

According to Andriotis, Oikonomou and Tryfonas (2012) there is a possibility of obtaining evidential information such as files transferred via Bluetooth and visited wireless networks, from a small buffer which stores this information. The implication therefore is that the viability of this information heavily relies on timely seizure of the device. The device should be rooted in order to access this information and to obtain a logical copy.

Chung, Park, Lee and Kang (2012) researched on the extraction of useful information from smart phones related to applications and application data. They established that a device has to be rooted in order to retrieve evidential data like app access keys and secret keys.

In a research conducted by Grispos, Glisson and Storer (2015) Dropbox™ files were recovered from two locations in the SD card namely, the cache and the files subfolder in the Dropbox™ application folder. They identified thumb nails of JPEG images and saved offline files and documents. Further analysis of unallocated space revealed deleted documents which were still resident in the SD card while viewed and undeleted documents were also
recovered. Meta data was recovered from the internal memory of the smart phone which consisted of two SQLite databases and a transaction log. They also established that clearing the cache did not delete viewed files from the smart phone, rather were still physically stored on the SD card.

2.3 Acquisition of Cloud Data Remnants

There are various forensics techniques and software in the market which have to be updated regularly in order to stay current with Android market trends. Extraction of evidence from a smart phone requires connection to the examination computer via a cable, infrared or Bluetooth. The methods of choice are dependent on the case, time availability, the investigator’s expertise, availability of tools and model of the phone. A card reader can be introduced to make a copy of the suspect’s SIM card as a significant amount of deleted evidence is stored in such locations.

A classification system was conjured by Brothers (2009) who based it on the depth of the examiner or forensic software’s ability to acquire data from the device. The author related this classification to iPhone but it has been widely adopted in the classification of other smart phones, tablets and GPS devices with software developers using it to develop forensics tools. The author offers five levels of extraction from mobile devices as provided in Figure 2. Manual Acquisition (the bottom layer) requires the least amount of expertise yet is the least forensically sound. Micro Read (top layer) on the other hand is the most complex and requires technical expertise s well as offers the most forensically sound approach.
Zhu (2011) provided that manual acquisition involves manually browsing the phone through the user interface via the keypad or touch pad. Despite being simple to perform, it is time consuming, is prone to errors and cannot retrieve deleted files. It is commonly used in emergency cases and where the integrity of data is not of essence. Since it is difficult to prove that the evidence obtained by this method is uncontaminated, it is inadmissible in a court of law, given that the investigation is performed on the original handset. Physical and logical extractions are discussed at length in the next sections.

2.3.1 Physical Extraction

Physical extraction is the bit by bit copy of the entire physical storage, and allows forensics tools to retrieve remnants of deleted data (Grispos, Storer, & Glisson, 2011). This technique requires direct access to the file system of the smart phone. Methods such as carving are incorporated in order to recover deleted data from the disk.

Brothers (2009) provides three physical extraction methods namely, Hex Dump, Chip Off and Micro Read. Hex Dump extraction is achieved by either removing chips from the circuit board and dumping its content or using specialized software on a computer connected to smart phone via a cable. According to the author, Hex Dump is commonly used, despite the fact that data obtained is in its rawest form which is a challenge during interpretation. The
chip off method incorporates an EEPROM reader after the physical removal of the flash chip from the device. This is very intrusive and can permanently damage the evidence or hardware components, despite being classified as forensically sound. The Micro Read method offers a physical view of the electronic circuitry of the smart phone with the help of a high powered microscope, which requires highly specialized expertise. It also extracts evidence from damaged chips and is also classified as forensically sound. It is preferred for the retrieval of data from extremely valued devices or damaged chips with essential evidence.

In physical extraction the use of specialized software, may require rooting the device which may interfere with the evidence thus going against the ACPO principles which state that in any given case data stored in a smart phone should not be modified (ACPO, 2012). Rooting basically means escalating the current rights on the Android device to root access rights, this allows access to the root directory (Kessler & Lessard, 2010). The technical process of rooting an Android smart phone is beyond the scope of this project. And if this cannot be observed the investigator should document all procedures and give the relevance and implications of the actions taken. Although the rooting process differs with different device models, it alters data stored on the device and exploits security vulnerabilities (Tapaswi & Srivastava, 2015).

According to Martini & Kim-Kwang (2015), physical extraction of data offers thorough analysis of data stored in the device’s flash memory by ensuring all files are collected, which includes file signature verification, and header/keyword search using current forensics tools which can read the ext4 format utilized by modern Android smart phones.

A study by Tajuddin and Manaf (2015), revealed that a huge amount of data artifacts can be physically extracted from a smart phone with very minimal loss of data. The researchers used Celebrite’s UFED which is renowned for comprehensive smart phone acquisition hence retrieving chats, calendar information, audio and video files, documents and images, including deleted data. This was done without tampering with the evidence which is a requirement for the admissibility of evidence in a court of law. In numerous cases physical extraction can bypass and retrieve security hurdles presented on a smart phone.
2.3.2 Logical Extraction

Logical extraction is the extraction of allocated data and is achieved by accessing the file systems. Hoog (2011) defines allocated data as the data that has not been deleted and is accessible on the file system but this definition has an exception to it, as some files like the SQLite database can be allocated and still contain deleted records. It refers to the extraction of logical storage artifacts resident in a smart phone e.g directories and files. In contrast, in SQLite built platforms like Android, some database files marked as deleted may not be overwritten, which is particularly useful for forensic investigators. The deleted information can be recovered if the device gives permission for file systems access through its synchronization interface. File system extraction is instrumental in the understanding of the file structure, application usage or web history as well as provide the ability to use traditional computer forensics tools for analysis.

There are numerous methods and tools for performing logical acquisitions on smart phones, in this project I discussed the Oxygen Forensics Detective®, which acts as a benchmark for understanding the logical solutions available in the market. There are vast logical acquisition tools in the forensic industry which are challenged by the ever evolving products of Android versions. The NIST Computer Forensics Tool Testing Program conducts tests on forensic tools on various aspects like data object extraction and data integrity. It then publishes a final report with a brief of the test results and projects the failures of the, which are then communicated to the vendors to provide patches.

Katz, Leberfinger and Halsky (2013) conducted a research on the logical acquisition of smart phones with the use of Cellebrite and MicroSystemation’s XRY Complete and concluded that it is not possible to acquire data deleted data types like original videos and photos but certain data like cookies, book marks and emails could be recovered using file system extraction.

Logical data can be obtained using a custom recovery image which contains basic binaries for booting the device into recovery mode. Extra features and root permissions can be found in CyanogenMod and TeamWin which make custom recovery images for mobile devices (Tapaswi & Srivastava, 2015). The authors successfully built and installed the custom
recovery image of the device using a tool they designed. They dumped specific partitions of memory, thereafter booting into default recovery mode and selecting the SD Card option to apply updates.

Quick and Choo (2013a), Quick and Choo (2013b), Quick and Choo (2014) undertook three different studies on data remnants from Dropbox™, Google Drive™ and OneDrive which involved a Windows 7 PC emulating virtual machines and an Apple 3G iPhone, widely used web browser and cloud storage client applications. Their findings revealed various evidential information including user names, passwords, file names, their content as well as date and times of access. It is worth noting that the content of the files stored in the cloud were not recovered from the iPhone. The authors recommended physical acquisition of the iPhone for their future research in order to ascertain the presence of these files on the device.

2.4 Implications of the Cloud Data Remnants in Smart Phone Forensics

As indicated earlier cloud storage has the potential for being exploited by criminals in propagating criminal activities. At the time of writing this project, Kenya did not have publicly documented cases of criminal activities involving cloud computing and smartphone devices, but a good example occurred in Australia. According to R vs Paul James (2011), Mr. James’ gmail, yahoo and hotmail accounts which contained child pornography material were seized by the police together with two computers in his possession. Performing a link analysis of evidential data on physical media and that residing on the cloud has become a touchy issue in investigations. In this case it was established that due to the high rate of duplication between the email accounts and the two computers, the total number of images was much higher. It is therefore paramount to accurately compare file contents and establish whether cloud storage alters the content of files.

Law enforcement agencies and digital forensic investigators highly regard the timely acquisition and preservation of evidential from exhibits like cloud storage and mobile devices. Some jurisdictions like Australia have legal provisions that allow for the search and seizure of evidential data at the time of serving a warrant device, which drastically reduces the time and processes involved in accessing an account to collect the data. Using three popular public cloud storage providers (Dropbox™, Google Drive™, and OneDrive®) as
case studies, this section focuses on file contents and time implications of cloud data remnants downloaded using a browser and client software. The original data and resulting data will be compared for a comprehensive analysis.

### 2.4.1 File Content

Hash sets are frequently used for ensuring integrity of files from points of origin to the final destination of download using numerous tools in the market for instance the Volcano Hash Tool. Differences in the compared hash sets point out those modifications were made while the files were in transit from the point of origin to the final destination. (Koppen et al., 2012) further reiterated that monitoring tools can also be incorporated to solidify the resultant findings to ascertain their significance to the signature of an application.

A research conducted by Quick and Choo (2013c) established that there were no changes made to data during the uploading storage and downloading process after analyzing the MD5 and SHA1 values. Neither did the method of downloading change the contents of the file, as the MD5 and SHA1 values of downloaded files were similar to the files in the cloud storage accounts. There was a slight change of time stamp information when the files were moved from one location to another, but the hash values remained constant. As highlighted above this is a crucial aspect during an investigation.

### 2.4.2 Date and Time

Time and date are often aspects that are significant in forensic investigations with both positive and negative implications, therefore the need to document the correct findings and fully comprehend the circumstances related to the time stamps on cloud data remnants.

Times and dates affect the outcome of a court case when associated with electronic evidence like in the case of R vs Edmonds (2011) where the forensic specialist was put to task to explain information that was related to hotmail printouts, but in the end the timings on the headers was considered in the delivery of a judgment (Australia, 2011). At first glance of the headers, they looked different, and this would have led to false conclusions if the time zones were not considered. It was later established that the disparity emanated from the different time zone offsets between South Australia and Greenwich Meridian. As a consequence, it
was provided that the ‘text of the emails was identical’ which clarified the inquiries on the content of the emails.

According to Quick and Choo (2013c), the analysis of evidential data from the collected cloud storage accounts in relation to the time and dates associated to the downloaded files showed changes depending on the service and the method used for downloading the data. The research also revealed that that the last written time was similar to the one on the original file when the client cloud software was used. i.e files accessed and downloaded from Dropbox™ and One Drive® from the client software showed constant values of Last Accessed, Files created and Time Modified with the original files. In contrast when a browser was used, differences were observed; the last written time and the entry modified time of the downloaded files was the recorded unzipping time. No file dates and times matched the original file time and date in the cloud storage service. It is worth noting that for all files downloaded, the file stamps were the downloaded time recorded. All browsers recorded similar results. NIST provides that the date and time of files and their content can be very useful in an investigation to be admitted in a court of law (Jansen, Ayers, & Brothers, 2014).

2.5 Chapter Summary

The popularity of cloud storage services has experienced exponential growth especially with the known limitations of smart phones in the storage of huge amounts of data. The ubiquitous nature of smart phones attracts users to store files, pictures, videos, documents and other data on virtual storage services. This chapter expounded on existing literature on cloud data remnants, their location, the acquisition of these cloud data remnants and the implications they may have during a forensic investigation. The next chapter discusses the methodology used in answering the research questions proposed and discussed in chapter 1 and 2 respectively.
CHAPTER THREE

3.0 METHODOLOGY

3.1 Introduction

This chapter focused on the research method undertaken to address the research questions posited in chapter one. The literature review in chapter two informed the main research questions for the project, and partially answered some of the questions. Limitations of the project research were then highlighted and a chapter summary provided.

3.2 Research Design

The first step was to carry out literature research to identify relevant techniques relating to smart phone forensic analysis. This was carried out and whilst some information attempted to answer the research sub questions, the overall aim of the project was not answered in published literature.

3.2.1 Research Question 1 Experiment Process

To answer Research Question 1, a quasi-experimental nonrandomized research method was used. It is a quasi-experimental process as the nature of cloud storage means the devices are connected to the Internet to gather data and establish the circumstances for review, which can lead to changes to the devices outside the scope of the experiment (Shadish & Cook, 2002). Hence the results may not be repeatable within the exact same parameters in future, depending on changes to the websites visited, operating system updates, and other processes not controlled by a user. The experiment is nonrandomized to enable analysis to be undertaken to determine changes to various control circumstances, and the use of randomized samples would increase the scope of the research, therefore known content control media is used and then copied.

A computer was identified during the first stage of the experiment process, and used to provide a pretest set of data for comparison. The experiment is undertaken, and then analysis compares the results with the pretest media, to determine any changes after the experiment. Each process was documented to capture the steps taken. The cloud storage services were
accessed using the client cloud service and Google Chrome’s (incognito mode) installed on the Android smart phones to accommodate various circumstances as illustrated in (Figure 3).

![Figure 3: Block diagram of Research scope (Author’s own illustration)](image)

This process is applied to answer the research questions in relation to the use of cloud storage services; Dropbox™, OneDrive® and Google Drive™.

The project incorporated one forensic tool which is commonly by used law enforcement agencies and the private sector in the forensics field namely, Oxygen Forensics Detective version 8.3.0.95 which was installed on the Windows 7 machine. Hash values (MD5) were used to ensure the forensic integrity of the data. The Digital Volcano Hash tool version 1.1.0.0 was used for calculating hash values.

When assessing the use of cloud service on an Android phone, the following process is undertaken; Android phones were selected which had not been used to access each cloud service previously as the device history and usage was known. Oxygen Forensics ® was used to extract a logical image of the contents, prior to undertaking the research. These extracts were analyzed to confirm there was no service provider related data on the device. Next, the installed client storage services and the selected browser were used to access the cloud storage accounts, install the client storage services was used to access the cloud service user
account created for this research and view the sample files and files stored remotely. A logical extract was then conducted using Oxygen Forensics. The cloud service application was then downloaded and installed to the Android phone. The test user account was then accessed using the application, and the files stored in the account were viewed. A third logical extract with Oxygen Forensics was then conducted and an analysis performed to locate and identify data.

3.2.2 Research Question 2 Experiment Process

To answer Research Question 2, the same experimental process applies. In this process due diligence is observed not to introduce agents to the mobile phone as it will tamper or modify the evidence. A logical acquisition approach was adopted where the allocated data is acquired by accessing the file systems.

3.2.3 Research Question 3 Experiment Process

To answer Research Question 3, the analysis of file data extends to the hash values generated by Digital Volcano hash tool and time stamps produced against the original files.

3.3 Data collection methods

A quasi-experimental nonrandomized research method was used. It is a quasi-experimental process as the nature of cloud storage means the devices are connected to the Internet to gather data and establish the circumstances for review, which can lead to changes to the devices outside the scope of the experiment (Shadish & Cook, 2002). Hence the results may not be repeatable within the exact same parameters in future, depending on changes to the websites visited, operating system updates, and other processes not controlled by a user. The experiment was nonrandomized to enable analysis to be undertaken to determine changes to various control circumstances, and the use of randomized samples would increase the scope of the research, therefore known content control media is used and then copied.

The project incorporated one forensic tool which is commonly by used law enforcement agencies and the private sector in the forensics field namely, Oxygen Forensics Detective version 8.3.0.95 which was installed on the Windows 7 machine. Hash values (MD5) were
used to ensure the forensic integrity of the data. The Digital Volcano Hash tool version 1.1.0.0 was used for calculating hash values.

Android phones were selected which had not been used to access each cloud service previously as the device history and usage was known. Oxygen Forensics ® was used to extract a logical image of the contents, prior to undertaking the research. These extracts were analyzed to confirm there was no service provider related data on the device. Next, the installed client storage services and the selected browser were used to access the cloud storage accounts, install the client storage services was used to access the cloud service user

3.4 Research Procedures

The following steps were taken:

1. Preparation of the smart phones by performing a ‘reset’ to restore to default factory settings.
2. Connecting the phone to a wireless network for internet access and downloaded the cloud storage application via Google App Store
3. Execution of the cloud storage application, creation of a new user account using a predefined email address and a password.
4. Connection to the cloud storage provider through the application, using the test account in order to download the samples.
5. A personal computer running Windows 7 was used to access the test account created in Step 3 and the samples were uploaded to the cloud storage provider using a web browser. Hash values were generated using MD5 then the date and time of upload the cloud storage provider documented. Synchronization was done between the smart phone and the cloud storage provider in order to access the samples on the installed applications
6. Once they could be seen, manipulation on the files were done to imitate the various scenarios that make be encountered in the real world. The manipulation included:
   • viewed or played;
   • viewed or played then saved for later use or saved for offline use;
   • viewed or played then deleted from the cloud storage application;
• neither opened/played nor deleted (no operation)

This is shown in (Table 1).

<table>
<thead>
<tr>
<th>File</th>
<th>Size (bytes)</th>
<th>Manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>101.docx</td>
<td>13KB</td>
<td>Viewed</td>
</tr>
<tr>
<td>102.docx</td>
<td>13KB</td>
<td>Viewed and saved for later use</td>
</tr>
<tr>
<td>103.docx</td>
<td>13KB</td>
<td>Viewed and deleted</td>
</tr>
<tr>
<td>104.docx</td>
<td>13KB</td>
<td>No operation</td>
</tr>
<tr>
<td>101.pdf</td>
<td>81KB</td>
<td>Viewed</td>
</tr>
<tr>
<td>102.pdf</td>
<td>81KB</td>
<td>Viewed and saved for later use</td>
</tr>
<tr>
<td>103.pdf</td>
<td>81KB</td>
<td>Viewed and deleted</td>
</tr>
<tr>
<td>104.pdf</td>
<td>81KB</td>
<td>No operation</td>
</tr>
<tr>
<td>105.jpeg</td>
<td>4KB</td>
<td>Viewed</td>
</tr>
<tr>
<td>106.jpeg</td>
<td>5KB</td>
<td>Viewed and saved for later use</td>
</tr>
<tr>
<td>107.jpeg</td>
<td>3KB</td>
<td>Viewed and deleted</td>
</tr>
<tr>
<td>108.jpeg</td>
<td>3KB</td>
<td>No operation</td>
</tr>
<tr>
<td>113.mp3</td>
<td>8218KB</td>
<td>Viewed/played</td>
</tr>
<tr>
<td>114.mp3</td>
<td>4018KB</td>
<td>Viewed/played and saved for later use</td>
</tr>
<tr>
<td>115.mp3</td>
<td>4730KB</td>
<td>Viewed/played and deleted</td>
</tr>
<tr>
<td>116.mp3</td>
<td>6141KB</td>
<td>No operation</td>
</tr>
</tbody>
</table>

3.5 Data Analysis Methods

Data analysis of the collected evidence was performed using the inbuilt analysis tool in Oxygen Forensics which provided an overview of the entire logical acquisition. A comparison was performed on the original data artifacts against the downloaded data in the various cloud service applications installed on the smart phones. This also followed
procedures given by the ACPO (2012), which give steps on handling evidence. The hash values and timestamps were noted and documented for further analysis.

3.6 Research Equipment

The details of the host computer system, and smart phone specifications are outlined in (Table 2). In relation to the host computer, there was Windows 7 on a 1 TB hard drive with 8 GB RAM allocated. Handwritten notes were made, as per common forensic practice, at each stage of the experiments. These proved to be invaluable, and were referred to numerous times whilst undertaking the research.

Table 2: Device specifications used

<table>
<thead>
<tr>
<th>Device</th>
<th>Generic Personal Computer Tower (PC)</th>
<th>Huawei D200</th>
<th>Samsung A5</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Windows® 7 SP1</td>
<td>Android 4.1.2 (Jelly Bean)</td>
<td>Android 5.0.2(Lollipop)</td>
</tr>
<tr>
<td>Processor</td>
<td>Intel® Core i7 3.0 GHz</td>
<td>Quad-core 1.5 GHz</td>
<td>1200Mhz 64bits Quad-Core</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB RAM</td>
<td>2 GB RAM</td>
<td>2 GB RAM61</td>
</tr>
<tr>
<td>Storage</td>
<td>1 TB</td>
<td>32 GB</td>
<td>16 GB</td>
</tr>
</tbody>
</table>

3.7 Research Limitations

Version dependence: The outcomes of the experiment are in tandem with the software versions present during the project which emphasizes its quasi-experimental nature. Previous or future software versions may yield totally different results. (Table 3) shows the software versions used.
Table 3: Software versions used

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oxygen forensics</td>
<td>8.3.0.95 (released 24\textsuperscript{th} Mar, 2016)</td>
</tr>
<tr>
<td>Digital volcano hash tool</td>
<td>1.1.0.0 (released 16\textsuperscript{th} Jan, 2011)</td>
</tr>
<tr>
<td>Android Kitkat</td>
<td>4.1.2 (released 9\textsuperscript{th} July, 2012)</td>
</tr>
<tr>
<td>Android Lollipop</td>
<td>5.0.2 (released 19\textsuperscript{th} Dec, 2014)</td>
</tr>
</tbody>
</table>

Operating system dependent: The project was conducted while taking into consideration any alteration of files running in Windows 7 and the NTFS file system. Other operating systems, such as Windows 10, Microsoft Vista, Apple Mac OSX, or Linux, may all result in different data remnants. This also includes other file systems, such as HFS+ or EXT3. Therefore if NTFS or Windows 7 are not incorporated, different results may be recorded to answer the research questions.

Hardware dependent: The project was limited to non-rooted Android smart phones running versions 4.1.2 and 5.0.2 respectively therefore other versions may provide different information and a rooted device may provide additional information. Additionally, iPhones and other mobile device operating systems and hardware may result in other data remnants and implications.

3.8 Chapter Summary

This chapter expounded on the methodology used to undertake experiments related to the research questions. The equipment used to in the project was described and limitations of the project finally pointed out. The next chapter implemented a proposed a digital forensic framework which dealt with various characteristics in an investigation as elucidated in the literature review. This offered a glimpse in mobile cloud forensics which may require the identification of data during the analysis stage of an investigation, therefore requiring retracing steps to preserve data.
CHAPTER FOUR

4.0 IMPLEMENTATION

4.1 Introduction

There is a need for a framework which can accommodate future providers offering new services and technologies. In order to ensure information sources are identified and appropriately preserved, any suggested framework requires inclusivity of any common circumstances and services that may be encountered during an investigation. According to Slay, Lin, TurnBull, Beckett and Lin (2009) numerous digital forensics models have been identified. Conversely, these existing digital forensics procedures are not sufficient for investigations in modern cloud computing environments (Birk 2011). As indicated by ACPO, (2012), Mukasey, Sedgwick and Hagy (2008) there are standards, rules and procedures that digital forensic investigators and law enforcers follow.

According to Mckemmish (1999) there are four stages in a forensic computing investigation: ‘identification, preservation, analysis, and presentation. The analysis of digital evidence may be an outcome of the identification and preservation when performing investigations in cloud services. This framework was instrumental in the implementation of the project.

4.2 The Digital Forensic Framework

According to Mckemmish (1999) there are four stages in a forensic computing investigation: ‘identification, preservation, analysis, and presentation. According to Ratcliffe (2003) data capture in relation to forensics has metamorphosed over the years with given that it is an ongoing process that involves a continuous cycle of tasking, collecting, collation, analysis, dissemination and feedback. The analysis of digital evidence may be an outcome of the identification and preservation when performing investigations. For instance, an investigator should be prudent enough to continue analyzing captured evidence as he/she awaits data stored in the cloud to be availed for the investigation. These cloud data remnants will be included for analysis as the investigator continues analyzing the data at hand. Additional cloud data remnants may be identified for analysis therefore the digital forensic process can be termed as cyclic.
Additionally, there are other supplementary steps which can be derived from the intelligence cycle; tasking and feedback. The proposed framework as shown in (Figure 4) is based on the intelligence analysis cycle and the process of forensic analysis, and consists of the following steps: Define the scope, Prepare and act appropriately, Identify and Collect, Preserve, Analysis, Presentation, Feedback and Closure. This framework is derived from research conducted by Quick, Martini and Choo (2014).

The processes in this proposed framework are repetitive and iterative as the forensic investigator may regularly go back or refer to previous steps during an investigation. For instance, during the analyzing stage, an investigator may discover valuable evidence linked to the data stored with a particular cloud storage provider. This may prompt the investigator to retrace their steps to stages like ‘Prepare and Act appropriately’ or ‘Identify and Collect’ and consider actions to locate, identify, and collect the newly identified evidence using existing lawful procedures. This will not impede the process of collecting other forensic evidence but rather promote an understanding of the evidence being gathered. This new data will then be considered for preservation through obtaining a forensic copy and carefully analyzed while accommodating the scope of the investigation.
Figure 4: The Digital Forensics Framework (Quick & Choo, 2013c)
4.2.1 Define the Scope

It is imperative for every investigation to commence with an outline detailing the scope, nature and background of the investigation. According to Taylor, Haggerty, Gresty and Lamb (2011) it is essential that the intention of a digital forensic investigation is comprehensively defined so that the complete scope of the investigatory process can be decided. The intricacies of an investigation need to be understood in order to establish the limits of an investigation. Since examiners and investigators will use it as a point of reference during the examination process, proper documentation should be done.

The scope would include the persons involved, any data or evidence already seized keyword terms, any urgent timeframes, and other relevant information. At the commencement of the investigation, the scope may be vague, but may take shape and clarity of purpose as it gathers momentum. In this project, the scope focused on the research question about the types of cloud data remnants and their location on the smart phone when accessed by the cloud service application and the browser.

4.2.2 Prepare and Act Appropriately

Once the scope is determined, the next step of any investigation, criminal or civil, is to understand the requirements and ensure that the correct equipment and information is available. Preparation can include training and equipment acquisition. There is a need for an examiner to have the appropriate skills, as per ACPO Principle 2 (ACPO, 2012) of ‘competency’ and this can be addressed by undertaking the appropriate training prior to undertaking an examination.

Advances in ICT such as the cloud computing environments will require ongoing training and research in digital forensics, which may include general ICT professionals. The latter is becoming more actively involved in the investigation and prosecution of cybercrime. For example, ICT professionals may be called upon to help facilitate compliance with legal obligations, developing and operating secure computer and cloud computing systems to ensure the privacy of protected information is not compromised. Training would equip ICT professionals with a working knowledge of key legal challenges and issues they are likely to encounter in the course of professional activities.
Preparation can also include research and development undertaken to gain an understanding of a particular issue or aspect of an investigation. For example, if the scope of an investigation relates to a particular cloud storage service, an examiner can conduct research using virtual computers or available equipment to gain an understanding prior to an investigation commencing. This can also occur during an investigation if cloud storage becomes an aspect of an investigation. Inferences can be outlined and tested in a controlled environment to determine outcomes, which can then be applied to an investigation to answer particular questions, or gain an understanding of the presence of data or information, and form hypotheses.

Preparation also includes other aspects of an investigation, such as timely response, timeframe, personnel, duties, and locations of interest. An investigation plan can outline the various issues that need to be considered and addressed. The investigation scope would be outlined to the relevant people, and the appropriate equipment organized and available. Additional expertise can be sought to ensure the process can flow in a timely manner, or an examiner can undertake research to ensure they have the requisite knowledge to undertake an examination. The project prepares for the investigation by gathering sufficient and relevant knowledge on the locations of data remnants, the types of remnants expected and the types of acquisitions recommended for admissibility of evidence in court.

4.2.3 Identify and Collect

The collect and identify phase involves adopting a predefined plan for proper documentation and accountability of actions. It will ensure all relevant evidence is procedurally identified and preserved well for analysis and eventual conclusion of the case. This predefined plan may consist of documentation, guided timelines, probable locations, equipment and software required, chain of custody and expertise required.

Essentially this stage is geared at collecting and identifying any important evidential artifacts. Some service providers can be contacted for further and proper identification and collection of evidential data, unfortunately this is time consuming and may lead to the loss or expiration of essential evidence. The evidential copies should be collected and stored in appropriate media that cannot not be damaged or tampered with easily and hash values applied to ensure integrity.
4.2.4  Preserve

Digital forensics proffers that investigation should be conducted on the forensic copy instead of working on the original copy, which may, tamper with the evidence ACPO (2012). It is at this stage that details are documented, e.g the mobile make and model numbers, the external memory details etc. The data in the device is then forensically copied using the right procedures, with the possibility of right protection to avoid accidental tampering. A bit-by-bit copy is created and a hash algorithm applied to ensure validity.

It is useful to involve the service provider in case the court case involves data stored in the cloud, who may be instrumental in retrieval and preservation of cloud data; this is beyond the scope of this project. This particular stage attempts to answer RQ2 which dwells on the suitable acquisition method of cloud data remnants that be accepted in court.

4.2.5  Analysis

This stage is undertaken to examine the investigation’s evidence gathered against any theories that may have been provided by the prosecution. This may consider numerous procedures to address the issues at hand being pointed out during an investigation. Other sources of data may be identified during this stage which may point back to the previous step of ‘Prepare and Respond’.

This will however not stop the analysis process but rather offer a new aspect of evidence to be incorporated when available. It is also important to include experts from various fields who will inform the whole process. Analysis should be done to the downloaded file properties against the original files uploaded to the cloud service. This stage is significant to RQ3 which dwelt on the significance of date/time and content of cloud data remnants in Android smart phones.

4.2.6  Presentation

This stage elucidates evidence provided in court in an understandable manner to all officials without using heavy digital forensics terms which may impede the reasonable judgment of the case. It is of utmost importance to have the analysis reported aptly in a lawful manner to prevent wrong decisions and ensure clarity throughout. According to Mckemmish (1999), the
analysis should be thorough, highlighting any setbacks and systems utilized while also considering verbal or written communication.

The entire sequence of events should be recorded, which can act as reference for informing discussions during the court proceedings. Collecting data from various sources like the memory, network snapshots, and cloud storage account can concretize the case at hand.

A spreadsheet timeline of events can be created using data and information from the various sources, which can assist to explain the course of events. Merging the information from the acquisitions may also be of assistance during the analysis process to gain an understanding of the sequence of events.

4.2.7 Feedback

Feedback is basically providing information from the evidence gathered and validating it to the analysis and findings discovered. This is borrowed from Baryamureeba & Tushabe (2006) who adds a final step he terms as ‘Review’. Feedback is included in the ‘Review’ process to ensure that the right scope was defined, the right answers are given to the issues at hand, the right procedures were observed, all areas of analysis were exhausted and finally that these procedures and steps can inform, be adopted and applied in future investigations.

4.2.8 Closure

This is the conclusion stage of an investigation where a verdict is given on whether further analysis is required, founded on the feedback provided by the investigating officers. It also considers the initial parameters at the definition scope, which may lead to the reconsideration of previous stages like the ‘Prepare and Act appropriately’. In the event that it was conclusive, the case can be closed, documented and stored or archived for future use. All this should be conducted in a procedural manner to avoid tampering of evidence as court cases can drag on for numerous years which may require for the representation of evidence once again.

4.3 Applying the Framework

This proposed framework offers steps that are repetitive and iterative since forensic investigators may be required to retrace their steps during an investigation in order to give
undisputed evidence. A good example is when an investigator goes to a previous step like preserve to ensure all hash values and preservation procedures were followed and may prompt further action into proper identification and collection of evidence lawfully. This turn of events will require the investigators expertise in creating a forensic copy and add this newly found evidence into the scope defined earlier.

The framework can be mapped to the research questions in (Table 4):

**Table 4: Applying the framework**

<table>
<thead>
<tr>
<th>Research questions</th>
<th>Steps in the framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>RQ1</td>
<td>Scope definition</td>
</tr>
<tr>
<td>RQ2</td>
<td>Scope definition and, Prepare and Act appropriately, Identify and collect, Preserve</td>
</tr>
<tr>
<td>RQ3</td>
<td>Analysis, Closure</td>
</tr>
</tbody>
</table>

4.4 **Google Drive™ Analysis: Samsung A7 and Huawei D200**

Android smart phones were used to access Google Drive™ cloud storage either using the built in the Google Chrome browser (incognito mode), or installing the Google Drive™ application. Analysis of mobile devices is a growing area for forensic practitioners, and there are hardware and software solutions to assist this process, such as Oxygen Forensics Detective. In the scope of this project, it is relevant to consider what information can be determined from a smart phone in relation to the use of Google Drive™. This will also assist in assessing the suitability of the framework being implemented in various scenarios.

4.4.1 **Definition of the scope**

The scope of this part of the research was to examine the data remnants on Samsung A7 and Huawei D200, Android versions 5.0.2 and 4.1.2 respectively which were used to access Google Drive™, via a browser or Google Drive’s client application. Analysis also sought to determine if there were any remnants prior to accessing Google Drive™ on the android devices. These two access methods were utilized in the determination of any differences in
the logical acquisition of data remnants. The focus is on remnants like filenames, date/time, or even the presence of log files on the cloud client software.

4.4.2 Prepare

The Android devices were reset in order to clear previous activity for access to Google Drive™ previously. Since the device usage was known, Oxygen Forensics version 8.3.0.95 was used to extract a logical image of the contents, prior to accessing Google Drive™. The phones were hard reset and extracts analyzed to confirm there was no Google Drive™ related data on the device prior to undertaking the experiment. The Google cloud client and Google Chrome’s browser were then identified to enable access to the Google Drive™ user account created for this project. Logical extracts were then conducted. A Windows 7 machine was also used to create the files as indicated in (Figure 5)

The following software and tools were used for the purposes of this research:

- Google Drive
- Google Chrome
- Digital Volcano Hash tool
- Oxygen Forensics Detective

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>4/12/2016 3:06 PM</td>
<td>Microsoft Word Document</td>
<td>13 KB</td>
</tr>
<tr>
<td>102</td>
<td>4/12/2016 3:06 PM</td>
<td>Microsoft Word Document</td>
<td>13 KB</td>
</tr>
<tr>
<td>103</td>
<td>4/12/2016 3:07 PM</td>
<td>Microsoft Word Document</td>
<td>13 KB</td>
</tr>
<tr>
<td>104</td>
<td>4/12/2016 3:07 PM</td>
<td>Microsoft Word Document</td>
<td>13 KB</td>
</tr>
<tr>
<td>105</td>
<td>4/12/2016 3:08 PM</td>
<td>PDF File</td>
<td>81 KB</td>
</tr>
<tr>
<td>106</td>
<td>4/12/2016 3:08 PM</td>
<td>PDF File</td>
<td>81 KB</td>
</tr>
<tr>
<td>107</td>
<td>4/12/2016 3:09 PM</td>
<td>PDF File</td>
<td>81 KB</td>
</tr>
<tr>
<td>108</td>
<td>4/12/2016 3:09 PM</td>
<td>PDF File</td>
<td>81 KB</td>
</tr>
<tr>
<td>109</td>
<td>4/10/2016 1:29 PM</td>
<td>JPEG image</td>
<td>4 KB</td>
</tr>
<tr>
<td>110</td>
<td>4/10/2016 1:29 PM</td>
<td>JPEG image</td>
<td>5 KB</td>
</tr>
<tr>
<td>111</td>
<td>4/10/2016 1:29 PM</td>
<td>JPEG image</td>
<td>3 KB</td>
</tr>
<tr>
<td>112</td>
<td>4/10/2016 1:29 PM</td>
<td>JPEG image</td>
<td>3 KB</td>
</tr>
<tr>
<td>113</td>
<td>7/14/2009 8:32 AM</td>
<td>VLC media file (mp3)</td>
<td>8,218 KB</td>
</tr>
<tr>
<td>114</td>
<td>7/14/2009 8:32 AM</td>
<td>VLC media file (mp3)</td>
<td>4,018 KB</td>
</tr>
<tr>
<td>115</td>
<td>7/14/2009 8:32 AM</td>
<td>VLC media file (mp3)</td>
<td>4,730 KB</td>
</tr>
<tr>
<td>116</td>
<td>4/12/2016 2:54 PM</td>
<td>VLC media file (mp3)</td>
<td>6,141 KB</td>
</tr>
</tbody>
</table>

Figure 5: Samples Created on Windows 7 Machine
4.4.3 Identify and Collect

To fulfill the aims of the research question 2, folders which contained relevant information were identified which, in this instance being the Oxygen extract files and the output of these tools, including PDF reports and the files exported. This is shown in (Figure 6). These were identified for each of the extracts from the Client Software. The exhibits were word documents (101, 102, 103, 104), pdf files (105, 106, 107, 108), jpeg photos (109, 110, 111, 112) and audio files (113, 114, 115, 116).

![Possible locations for both the Samsung and Huawei devices](image)

4.4.4 Preservation

In adherence to the principles of forensic computer analysis ACPO (2012), a forensic copy was made of the Oxygen Forensics extract files, the file output, and the reports. As these were logical files, this was done in the Oxygen Forensics format (odf). MD5 hash values were used to ensure the forensic integrity of the data. The exhibit below gives the hash values before they were uploaded to the various cloud services.

<table>
<thead>
<tr>
<th>Hash Value</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>2ec613a48ff8935ad99038a62dca852</td>
<td>C:\Users\Administrator\Desktop\Forensics\Test\101.docx</td>
</tr>
<tr>
<td>4c373ef7b4ee055b6b41f4bab5adfd7</td>
<td>C:\Users\Administrator\Desktop\Forensics\Test\102.docx</td>
</tr>
<tr>
<td>f7ae846fe61c8593ed9dd60ff33f80d</td>
<td>C:\Users\Administrator\Desktop\Forensics\Test\103.docx</td>
</tr>
<tr>
<td>2f415f0a2588972df6c60f9f808848b1c</td>
<td>C:\Users\Administrator\Desktop\Forensics\Test\104.docx</td>
</tr>
<tr>
<td>7cc5791259352c7902513bd087accbf6</td>
<td>C:\Users\Administrator\Desktop\Forensics\Test\105.pdf</td>
</tr>
</tbody>
</table>
4.4.5 Analysis

For this research, each of the forensic logical files and their contents were examined using Oxygen Forensic Detective which has an inbuilt analysis tool for each target location e.g. file browser, key evidence, reports and device information as shown in (Figure 7) for the Samsung A5.

![Figure 7: The inception of the analysis of Samsung A5](image-url)
(Figure 8) shows the commencement of the study for the Huawei D200 for each target location.

![Figure 8: The inception of the analysis of Huawei D200](image)

4.4.5.1 Google Drive™ accessed via the Client Software

The presence of cloud data remnants were found in the Google Drive™ application which was installed in the internal memory of both phones. The path for this particular pinned document for offline use was as shown in (Figure 9).

```
InternalMemory/Android/data/com.google.android.apps.docs/files/pinned_docs_files_do_not_edit/00fb1b0c2d324e6be89ff5cc5ab6e0fe/
```

![Figure 9: Analysis via the Client](image)
The downloaded files were also located in the internal memory of the smart phones specifically in the download folder. There was also evidence present in the cache and files/scratch folder as shown in (Figure 10).

Figure 10: Analysis via a Client in the Scratch Folder

4.4.5.2 Google Drive™ accessed via the Chrome browser

The evidence of access to Google Drive™ via Google Chrome (incognito mode) could not be traced, apart from the intentionally downloaded files on to the smart phones’ Download folder. This information could not be extracted by the inbuilt Oxygen Forensics Detective, Demo Version. The text from the test files could be read in the extracts, but locating the user name and password for the Google Drive™ account was not possible in both Android phones.

4.4.6 Presentation

In this research, several data remnants were located when searching for evidence of Google Drive™ used on the Android smart phones. As indicated earlier, the aim of the project was to locate and identify the data remnants by the access to Google Drive™. No traces were found
on the use of the Google Chrome browser apart from the intentional download of sample files.

A report was generated showing the findings of the analysis. The files of interest were then copied to a DVD, together with the related reports for each file, showing access dates and file details. This is shown in the appendices appended to this project report.

4.4.7 Feedback

This research was very successful in the installation of the Google Drive™ application, on the Android phones. Older versions of the Android operating systems may produce errors during installation due to the advancement in the software. On the other hand the extraction of files systems (logical acquisition) by Oxygen Forensics on the Android phones’ did not require rooting. Unfortunately the logical acquisition was not conclusive as the geo mapping and SQLite databases could not be accessed which could be a future research opportunity with a licensed version. Another future research opportunity is to undertake similar research using an Android version 6.0 (Marshmallow), and also widen the devices examined to include other popular mobile device operating systems, such as Apple’s iOS and Microsoft Windows. In addition, the comparison of a physical extract of an Android phone to a logical extract to determine what information is available, and also to compare the process with other Android forensic software and hardware processes.

4.4.8 Closure

In the context of this research, the data created and used may be required in future research opportunities, and hence has been stored in various physical storage facilities be used in the future.

4.5 Dropbox Analysis: Samsung A7 and Huawei D200

4.5.1 Definition of the scope

The scope of this part of the research was to examine the data remnants on Samsung A7 and Huawei D200, Android versions 5.0.2 and 4.1.2 respectively which were used to access Dropbox™ via a browser or Dropbox™ client application. Analysis also sought to determine if there were any remnants prior to accessing Dropbox™ on the android devices. These two
access methods were utilized in the determination of any differences in the logical acquisition of data remnants. The focus is on remnants like filenames, log files, date/time, or even the presence of cloud client software.

4.5.2 Prepare

The Android devices were reset in order to clear previous activity for access to Dropbox™ previously. Since the device usage was known, Oxygen Forensics version 8.3.0.95 was used to extract a logical image of the contents, prior to accessing Dropbox™. The phones were hard reset and extracts analyzed to confirm there was no Dropbox™ related data on the device prior to undertaking the research. The Dropbox™ cloud client and Google Chrome’s browser were then identified to enable access to the Dropbox™ user account created for this research. A Windows 7 machine was also used to create the files as indicated in (Figure 11). Logical extracts were then conducted.

The following software and tools were used for the purposes of this research:

- Dropbox™
- Google Chrome
- Digital Volcano Hash tool
- Oxygen Forensics Detective
4.5.3 Identify and Collect

To fulfill the aims of the research question 2, folders were identified which would contain the information needed to conduct the analysis as shown in (Figure 12), in this instance being the Oxygen extract files and the output of these tools, including PDF reports and the files exported. These were identified for each of the extracts from the Client Software and Browser. The exhibits were word documents (101,102,103,104), pdf files (105, 106, 107, 108), jpeg photos (109, 110, 111, 112) and audio files (113, 114, 115, 116).
Figure 12: Possible locations for both the Samsung and Huawei Devices

The Huawei D200 did not store any files in its client Dropbox application unlike the Samsung A5 which had some remnants in the cache as given in (Figure 13).

Figure 13: Location of Evidence Files in Dropbox – Samsung A5

4.5.4 Preservation

In adherence to the principles of forensic computer analysis ACPO (2012), a forensic copy was made of the Oxygen Forensics extract files, the file output, and the reports. As these were logical files, this was done in the Oxygen Forensics format (odf). MD5 hash values were used to ensure the forensic integrity of the data.
Below are the hash values generated by the Volcano Hash tool before upload to the cloud service.

2ec613a48ff8935ad99038a62dcaf852,C:\Users\Administrator\Desktop\Forensics\Test\101.docx
4c373ef7b4ee055b6b41f4fbaf5adfd7,C:\Users\Administrator\Desktop\Forensics\Test\102.docx
f7ae846fee61c8593ed9dd60ff33f80d,C:\Users\Administrator\Desktop\Forensics\Test\103.docx
2f415f0a2588972df6c609f808848b1c,C:\Users\Administrator\Desktop\Forensics\Test\104.docx
7cc5791259352c7902513bd087acce6f6,C:\Users\Administrator\Desktop\Forensics\Test\105.pdf
8a138f6b0920a19a489aae4888164a7,C:\Users\Administrator\Desktop\Forensics\Test\106.pdf
68dfdf5578cd64d2d224b13fa7b7588d5e,C:\Users\Administrator\Desktop\Forensics\Test\107.pdf
a456c3a54f6295c7c4a03dc51dd6f1a,C:\Users\Administrator\Desktop\Forensics\Test\108.pdf
9ca9be1a76f6ca119e76dd5a7423835a,C:\Users\Administrator\Desktop\Forensics\Test\109.jpg
9e26ec8c14cc7a9e2b46bd64e70812,C:\Users\Administrator\Desktop\Forensics\Test\110.jpg
8066b27e27ca3c5c8b627d4e9a1ae0c,C:\Users\Administrator\Desktop\Forensics\Test\111.jpg
dac959d512b1f0e17e067d5abc87da03,C:\Users\Administrator\Desktop\Forensics\Test\112.jpg
5a9a1184e611dac3f6ed162b8787ce5f,C:\Users\Administrator\Desktop\Forensics\Test\113.mp3
5bacdbda9a42150c27b1a182ba169f8,C:\Users\Administrator\Desktop\Forensics\Test\114.mp3
b8b5bd3ae23d40b5c4a650e272f2e19,C:\Users\Administrator\Desktop\Forensics\Test\115.mp3
c309b379175a3d603346b8674300999d,C:\Users\Administrator\Desktop\Forensics\Test\116.mp3

### 4.5.5 Analysis

For this research, each of the forensic logical files and their contents were examined using Oxygen Forensic Detective which has an inbuilt analysis tool for each target location e.g. file browser, key evidence, reports and device information as shown in (Figure 14).
Figure 14: The Inception of the Analysis of Samsung A5

(Figure 15) shows the beginning of the analysis of the Samsung D200 for each target location e.g. file browser, key evidence, reports and device information.

Figure 15: The inception of the analysis of Huawei D200

Common areas for analysis
4.5.5.1 Dropbox™ accessed via the Client Software

The Dropbox client in Samsung A5 had evidential image files that were synchronized automatically from the test folder in the cloud service as depicted below. The files could be viewed and opened as shown in (Figure 16).

Figure 16: Synchronised Files in the Dropbox Client
4.5.5.2  Dropbox™ accessed via the Chrome Browser

The evidence of access to Dropbox™ via Google Chrome (incognito mode) could not be traced, apart from the intentionally downloaded files on to the smart phones’ Download folder as shown in (Figure 17). This information could not be extracted by the inbuilt Oxygen Forensics Extractor. The text from the test files could be read in of the extracts, but locating the user name and password for the Google Drive™ account was not possible in both Android phones.

![Figure 17: Downloads Folder in Huawei D200](image)

4.5.6  Presentation

In this research, several data remnants were located when searching for evidence of Dropbox™ use on the Android smart phones. As indicated earlier, the aim of the project is to locate and identify the data remnants by the access to Dropbox™. No traces were found on the use of the Google Chrome browser apart from the intentional download of sample files. A report was generated showing the findings of the analysis. The files of interest were then copied to a DVD, together with the related reports for each file, showing access dates and file details. This is shown in the appendices appended to this project report.
4.5.7 Feedback

This research was very successful in the installation of the Google Drive™ Application, on the Android phones. It is worth noting that the Google Chrome browser in the Huawei smart phone download expressly asked for permissions to download the files into a specific folder unlike the Samsung A5 which downloaded all its files into the download folder.

4.5.8 Closure

In the context of this project, the data created and used may be required in future research opportunities, and hence has been stored in numerous physical storage facilities for future use.

4.6 OneDrive Analysis: Samsung A7 and Huawei D200

The Android phone is one such (popular) device that can be used to access OneDrive® cloud storage either using the built in Android browser, or installing the Microsoft OneDrive® application. In the scope of this research, it is relevant to consider what information can be determined from a portable device in relation to the use of OneDrive®. This also serves to further assess the suitability of the framework being applied in a variety of circumstances.

4.6.1 Definition of the Scope

The scope of this part of the research was to examine the data remnants on Samsung A7 and Huawei D200, Android versions 5.0.2 and 4.1.2 respectively which were used to access OneDrive® via a browser or OneDrive® client application. Analysis also sought to determine if there were any remnants prior to accessing OneDrive® on the android devices. These two access methods were utilized in the determination of any differences in the logical acquisition of data remnants. The focus is on remnants like filenames, date/time, or even the presence of cloud client software.

4.6.2 Prepare

The Android devices were reset in order to clear previous activity for access to OneDrive® previously. Since the device usage was known, Oxygen Forensics version 8.3.0.95 was used to extract a logical image of the contents, prior to accessing OneDrive®. The phones were hard reset and extracts analyzed to confirm there was no OneDrive® related data on the
device prior to undertaking the research. The OneDrive® cloud client and Google Chrome’s browser were then identified to enable access to the OneDrive® user account created for this research. Logical extracts were then conducted. A Windows 7 machine was also used to create the files as indicated in (Figure 18). Logical extracts were then conducted.

The following software and tools were used for the purposes of this research:

- OneDrive®
- Google Chrome
- Digital Volcano Hash tool
- Oxygen Forensics Detective

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>4/12/2016 3:06 PM</td>
<td>Microsoft Word Document</td>
<td>13 KB</td>
</tr>
<tr>
<td>102</td>
<td>4/12/2016 3:06 PM</td>
<td>Microsoft Word Document</td>
<td>13 KB</td>
</tr>
<tr>
<td>103</td>
<td>4/12/2016 3:07 PM</td>
<td>Microsoft Word Document</td>
<td>13 KB</td>
</tr>
<tr>
<td>104</td>
<td>4/12/2016 3:07 PM</td>
<td>Microsoft Word Document</td>
<td>13 KB</td>
</tr>
<tr>
<td>105</td>
<td>4/12/2016 3:08 PM</td>
<td>PDF File</td>
<td>81 KB</td>
</tr>
<tr>
<td>106</td>
<td>4/12/2016 3:08 PM</td>
<td>PDF File</td>
<td>81 KB</td>
</tr>
<tr>
<td>107</td>
<td>4/12/2016 3:09 PM</td>
<td>PDF File</td>
<td>81 KB</td>
</tr>
<tr>
<td>108</td>
<td>4/12/2016 3:10 PM</td>
<td>PDF File</td>
<td>81 KB</td>
</tr>
<tr>
<td>109</td>
<td>4/10/2016 1:29 PM</td>
<td>JPEG image</td>
<td>4 KB</td>
</tr>
<tr>
<td>110</td>
<td>4/10/2016 1:29 PM</td>
<td>JPEG image</td>
<td>5 KB</td>
</tr>
<tr>
<td>111</td>
<td>4/10/2016 1:29 PM</td>
<td>JPEG image</td>
<td>3 KB</td>
</tr>
<tr>
<td>112</td>
<td>4/10/2016 1:29 PM</td>
<td>JPEG image</td>
<td>3 KB</td>
</tr>
<tr>
<td>113</td>
<td>7/14/2009 8:32 AM</td>
<td>VLC media file (mp3)</td>
<td>8,218 KB</td>
</tr>
<tr>
<td>114</td>
<td>7/14/2009 8:32 AM</td>
<td>VLC media file (mp3)</td>
<td>4,018 KB</td>
</tr>
<tr>
<td>115</td>
<td>7/14/2009 8:32 AM</td>
<td>VLC media file (mp3)</td>
<td>4,730 KB</td>
</tr>
<tr>
<td>116</td>
<td>4/12/2016 2:54 PM</td>
<td>VLC media file (mp3)</td>
<td>6,141 KB</td>
</tr>
</tbody>
</table>

**Figure 18: Samples Created on Windows 7 Machine**

**4.6.3 Identify and Collect**

To fulfill the aims of the research question 2, possible folders were identified which would contain the information needed to conduct the analysis, in this instance being the Oxygen extract files and the output of these tools, including PDF reports and the files exported. This is shown in (Figure 19). These were identified for each of the extracts from the Client Software and Browser. The exhibits were word documents (101,102,103,104), pdf files (105, 106, 107, 108), jpeg photos (109, 110, 111, 112) and audio files (113, 114, 115, 116).
4.6.4 Preservation

In adherence to the principles of forensic computer analysis ACPO (2012) a forensic copy was made of the Oxygen Forensics extract files, the file output, and the reports. As these were logical files, this was done in the Oxygen Forensics format (odf). MD5 hash values were used to ensure the forensic integrity of the data.

The hash values generated by the software are shown below.

2ec613a48ff8935ad90038a62dca852,C:\Users\Administrator\Desktop\Forensics\Test\101.docx
4c373ef7b4ee955bd64f6b55adfd7,C:\Users\Administrator\Desktop\Forensics\Test\102.docx
f7ae846fe61c8593ed9d60f33f80d,C:\Users\Administrator\Desktop\Forensics\Test\103.docx
2f415f0a2588972df6c609f808848b1c,C:\Users\Administrator\Desktop\Forensics\Test\104.docx
7cc5791259352c7902513bd087accb6,C:\Users\Administrator\Desktop\Forensics\Test\105.pdf
8a138f0b0920a19a489a4a48f81d4a7,C:\Users\Administrator\Desktop\Forensics\Test\106.pdf
68ddf5578c6d4224b13f8b7258d5e,C:\Users\Administrator\Desktop\Forensics\Test\107.pdf
a456c3a54f6295e7c4a03dc51dd6f1a,C:\Users\Administrator\Desktop\Forensics\Test\108.pdf
9ca9be1766ca119e76dd5a7423835a,C:\Users\Administrator\Desktop\Forensics\Test\109.jpg
9e2f668c14cc7a9e246c6d64ec70812,C:\Users\Administrator\Desktop\Forensics\Test\110.jpg
8066b27e27ca3ce8b627c4ef9a1ae0c,C:\Users\Administrator\Desktop\Forensics\Test\111.jpg
For this research, each of the forensic logical files and their contents were examined using Oxygen Forensic Detective which has an inbuilt analysis tool for each target location e.g. file browser, key evidence, reports and device information as shown in (Figure 20).

Figure 20: The Inception of the Analysis of Samsung A5
(Figure 21) shows the inception of the analysis of the Huawei D200.

**Figure 21: The inception of the analysis of Huawei D200**

### 4.6.5.1 OneDrive® accessed via the Client Software

The presence of cloud data remnants were found in the OneDrive® application which was installed in the internal memory in the Huawei phone. This is unlike the previous samples where the Huawei did not have any data remnants in the cloud applications installed. The log file was located in the cache subfolder in the `com.Microsoft.skydrive` folder by the inbuilt Oxygen Forensics Extractor as shown in (Figure 22).

*Figure 22: Location of Cloud Data Remnants*
(Figure 23) shows the file path location of One Drive using the inbuilt Oxygen Forensics Extractor.

![Figure 23: File Path in the OneDrive Folder](image)

4.6.5.2 OneDrive® accessed via the Chrome’s Browser

The evidence of access to OneDrive® via Google Chrome (incognito mode) could not be traced in either phone, apart from the intentionally downloaded files on to the smart phones’ Download folder as shown in (Figure 24).

![Figure 24: Download Folder in Samsung A5](image)
4.6.6 Presentation

In this research, several data remnants were located when searching for evidence of OneDrive® use on the Android smart phones. As indicated earlier, the aim of the project is locate and identify the data remnants by the access to OneDrive®. No traces were found on the use of the Google Chrome browser apart from the intentional download of sample files. A report was generated showing the findings of the analysis. The files of interest were then copied to a DVD, together with the related reports for each file, showing access dates and file details. This is shown in the appendices appended to this project report.

4.6.7 Feedback

This research was very successful in the installation of the OneDrive® Application, on the Android phones. It yielded remnants resident in the OneDrive® client application subfolders in the JellyBean android version. The Android 5.0.1 did not have any remnants recorded.

4.6.8 Closure

In the context of this research, the data created and used may be required in future research opportunities, and hence has been stored in numerous storage facilities for future use.

4.7 Chapter Summary

This chapter offered a glimpse of the proposed framework which contributed to the knowledge of traditional forensic computer analysis with the addition of initial steps like ‘Definition of scope’ and ‘Prepare and act appropriately’ and ‘Feedback’ and ‘Closure’ which are the final steps were clearly accentuated. As provided above the framework is repetitive and iterative, where the investigator can reconsider previous steps during the entire investigation. This emphasized the relevance of general digital forensics frameworks that can be deemed relevant in cloud computing environments, for instance when definition of scope there may arise a need for reconsideration after completing the entire cycle to steer an investigation into the right direction.

The proposed framework was validated in the following chapter which looked in to the implementation of the methodology provided in Chapter 3. It offered guidance throughout all the steps highlighted above and applied in various scenarios that can be adopted by would be
criminals in real investigation scenarios. The framework was used in the analysis of the OneDrive®, Google Drive™ and Dropbox™ cloud storage service in relation to using a Windows 7 computer to access the service via a browser and client software, using an Android smart phone.
CHAPTER FIVE

5.0 RESULTS AND FINDINGS

5.1 Introduction

This chapter focused on expounding the results and findings obtained from the experiments performed in the previous chapter. The outcomes of this project proved to be beneficial for Police investigations as it will guide them in locating cloud data remnants stored on Android smart phones. The identification and location of cloud data remnants was attained after logical extraction of data was performed on the Android smart phones. This had a profound impact in demystifying the misconception that some cloud storage clients have employed encryption techniques on the local host that prevents extraction of any data. The results and findings were categorized according to the three research questions outlined in Chapter 1.

5.2 Cloud Data Remnants and Their Location

The research provided earlier in the literature review highlighted various areas of interesting locations (Internal Storage i.e cache and file folders, SD Card, SIM Card) and the types of remnants to identify, namely; time stamps, GPS coordinates, usernames, password, profile pictures, chat messages, journal logs and browser history. Cloud data remnants (timestamps, logs, cached files and actual downloaded files) were located in the cache and file folders which also had corresponding thumb nails and log files.

Table 5: Cloud Data Remnant Locations

<table>
<thead>
<tr>
<th>Remnants location</th>
<th>Samsung</th>
<th>Huawei</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downloads</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Thumb folder</td>
<td>√</td>
<td>X</td>
</tr>
<tr>
<td>Cache</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Client application folder</td>
<td>√</td>
<td>X</td>
</tr>
<tr>
<td>Logs</td>
<td>X</td>
<td>√</td>
</tr>
</tbody>
</table>

The locations of interest were Downloads, cache for the Microsoft OneDrive application and Sohunewscache logs only as documented above in (Table 5).
The rest of the folders (Dropbox, Google Drive or Google Chrome Browser) did not have any evidential data. (Figure 25) shows that thumbs nails were conspicuously absent in Huawei D200 unlike in the Samsung phone A5.

![Figure 25: No Thumbnails in Huawei D200](image)

The Samsung A5 had numerous thumbnails in the /thumbs/test folder which had the previewed data as seen in the figure below (Figure 26) but the Huawei D200 was devoid of such evidence. The path was Internal memory/Android/data/com.android.providers.media/albumthumbs

![Figure 26: Thumbnails in Samsung A5](image)
The Dropbox client in Samsung A5 had evidential image files that were synchronized automatically from the test folder in the cloud service as depicted below. The files could be viewed and opened as indicated in (Figure 27).

Figure 27: Files Contained in the Scratch Folder

5.3 Acquisition of Cloud Data Remnants

Logical acquisition was the preferred method of extraction as it does not tamper with the evidence by introducing agents, additionally being much faster and very friendly to conduct. According to ACPO (2012), forensics copies of Oxygen Forensics were made in order to avoid altering data on the original evidence exhibits and verified with MD5. The Samsung A5 acquisition was made simple due to the universal drivers and standards that the manufacturers adhere to, unlike the Huawei Chinese chipset which had to be restarted and reconnected numerous times for drivers to detect as shown in (Figure 28).

Figure 28: The Samsung Connection
The details of the smart phones were documented, including make, model and serial number. A successful connection with appropriate drives positively impacts the amount and type of data that will be extracted as shown in (Figure 29).

![The Huawei Connection](image1.png)

Figure 29: The Huawei Connection

Both Samsung A5 and Huawei D200 produced successful outputs of extraction and prompted for final actions from the user, for analysis or storage with the appropriate data formats as shown in (Figure 30).

![The Logical Copy](image2.png)

Figure 30: The Logical Copy
5.4 Implications of the Cloud Data Remnants in Smart Phone Forensics
The implications of the data remnants are demonstrated right from the creation of the documents on the computer before uploading to the cloud storage services. The files were hashed using Volcano Hash tool before upload and were verified after download. The date and time before upload and after downloads on both Android phones via the cloud client or web browser were also noted. In the downloading of files from the Dropbox account through the Google Browser (incognito) mode, the page showed the files and folders present in the account as shown in the (Figure 31).

Figure 31: The Hashing Process Using MD5
Selecting the test folder displayed the files uploaded from the host PC machine indicating the type of the file and the date modified. This was the date and time of upload as shown in the screen shot below in (Figure 32).

(Figure 33) shows the specific sample files uploaded to Dropbox indicating the size, time and date of upload to the cloud service provider.
The hash values are also availed for analysis and comparison to ascertain they are genuine
and match the original created files as shown below.

This scenario was similar for the rest of the cloud storage services, where the hash values
remained constant with a slight variance in the timestamps which reflected the download
time. The dates and timestamps were recorded as shown in (Table 6) below.

Table 6: Date and Time Stamps

<table>
<thead>
<tr>
<th>Oxygen Forensics</th>
<th>File creation on the Windows PC</th>
<th>Upload time to the various cloud storage services</th>
<th>Download timestamps for files download individually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Drive</td>
<td>Google Chrome</td>
<td>Last modified time (EAT)</td>
<td>Date and time at upload</td>
</tr>
<tr>
<td></td>
<td>Google Client</td>
<td>Last modified time (EAT)</td>
<td>Date and time at upload</td>
</tr>
<tr>
<td>Dropbox</td>
<td>Google Chrome</td>
<td>Last modified time (EAT)</td>
<td>Date and time at upload</td>
</tr>
<tr>
<td></td>
<td>Dropbox Client</td>
<td>Last modified time (EAT)</td>
<td>Date and time at upload</td>
</tr>
<tr>
<td>OneDrive</td>
<td>Google Chrome</td>
<td>Last modified time (EAT)</td>
<td>Date and time at upload</td>
</tr>
<tr>
<td></td>
<td>One Drive Client</td>
<td>Last modified time (EAT)</td>
<td>Date and time at upload</td>
</tr>
</tbody>
</table>
5.5 Chapter Summary
This chapter examined the logical process of acquisition and determined the file locations and their data remnants to prove that the contents were not modified in any way during the process of upload, storage download. All these were documented as proof of evidence that an investigation was conducted. It is worth noting that the time stamps of the files were different from those of the original files. This can hamper an investigation if inappropriate assumptions are made based on the recorded timestamp information, which can become a burden of proof. It is therefore paramount to choose an appropriate acquisition method for retrieval of evidential data from the browser and client software.
CHAPTER SIX

6.0 DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter gives a synopsis of the entire project and concluded the research. The first section of this chapter summarized the purpose of the study, research questions, the research methodology and major findings. The applicability, results and implications of the project are discussed and a recap were finally offered at the end.

6.2 Summary of Findings

The project began with an introduction which expounded on the purpose of the study and highlighted the research questions that would guide the reader’s understanding of the topic’s background. The motivation of the project was equally explained to provide clarity in the objectives to be delivered. The purpose of this project was to demonstrate the timely forensic identification, preservation, analysis and presentation of cloud data remnants in smart phones. This is attributed to the fact that data located in the cloud is unavailable anytime for investigation but available for criminals who use it for personal gain. Cloud computing and the respective services are widely used across different applications which includes web applications and mobile applications.

**Research Question 1:** What are the cloud data remnants on a smart phone and where are they located in current Android versions?

The literature reviews offered gave a detailed background of current locations on Android smart phones and possible locations for forensic investigators to source for evidential data. It greatly contributed and informed the answers to the research question. The cloud data remnants found were: **.doc, jpeg, mp3 and pdf files** in both smart phones and journal logs on the Huawei phone.

**Research Question 2:** How can these cloud data remnants be forensically acquired from a smart phone?

At the initial stages of an investigation it was paramount to adopt a framework which guided the entire acquisition process; therefore I adopted a framework whose validity was examined using the experiments when acquiring the cloud data remnants. The framework in Chapter 4
referred to existing guidelines on digital forensics analysis to offered processes that conform to standard forensics investigations, hence allowing investigators to implement it in their day to day work. The inclusion of the common forensic analysis steps served to ensure the process was applicable in real-world investigations, and that the research was widely applicable to be used in investigations. The additional feedback step proved to be of assistance to ensure findings in relation to the analysis were not forgotten or ignored, and the final step of completion served to ensure the data and findings were archived correctly, and not just discarded. This highlights that the proposed framework has wide application in digital forensic examinations, and the proposed additional steps are important to include in forensic examinations to ensure the whole process guides an investigation through the steps necessary from beginning to end. The cloud data remnants can be acquired through logical acquisition which created logical copy of the file structure of the smart phone. This logical copy was the image that was used for forensic analysis of the smart phone.

**Research Question 3: What is the forensic implication of accessing and downloading cloud data from Google Drive™, Dropbox™ and One Drive® on a Smartphone?**

This research question dwelt on the findings in relation to accessing cloud storage services and the web browser from the smart phone and the inherent forensic implications associated.

The research method adopted did not require rooting of the smart phone and was implemented without any major hiccups. This method took precedence over other types of phones to ensure that relevant data is obtained before the perpetrators get the chance of tampering with evidence. In the real world, an investigator may be required to retrieve data from a criminal’s smart phone before arrest, but ideally safe acquisition methods should be developed to avoid suspicion from the criminal such as the use of the nearest base station. With the wide spread adoption of Android around the world it is paramount to develop robust and non intrusive forensics tools.

6.3 Discussions

6.3.1 Cloud Data Remnants on a Smart Phone and Their Locations

The username and password for all client services and the browser could not be retrieved for all cloud storage services and the web browser. Some remnants were found in the internal
memory of the Android devices and could be recovered from the sub-folder named after the application. The folder name was different for each application installed on the devices. The inability to acquire this evidential data does not support numerous literature reviews that logical acquisitions are efficient in acquiring some data artifacts. The actual files that were downloaded were available in the path: Internal memory/Download, while files in the Dropbox files that were viewed and pinned for offline use could be viewed in the path:

Internal memory/Android/data/com.dropbox.android/files/u554162050/scratch/Samples

OneDrive had some data remnants present in the Jelly Bean Android version (4.1.2) which are very significant in evidence collection. The path was determined as

Path: Internal memory/Android/data/com.microsoft.skydrive/cache/Instrumentationb/{09b8475d-1ee6-4a47-ac34-c90f43a992e9}/

This research retrieved cloud data remnants from the Dropbox folder in the Lollipop Android version. The ability to extract the file contents in relation to the Dropbox application nullifies the findings of Zhu (2011), who was also unable to extract the file contents from the Dropbox application. Oxygen Forensic could not retrieve data remnants from the browser used due to the limited version of the forensic software. It was observed that Google Drive kept records of devices that access and synchronize the account as provided in (Table 7). This information is particularly useful in the determination of evidence related to a case at hand.

Table 7: Summary of locations and cloud data remnants

<table>
<thead>
<tr>
<th>Application Software</th>
<th>Remnants found</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Drive</td>
<td>Thumbnails, logfiles, sample files located in Downloads, Cache</td>
</tr>
<tr>
<td>Dropbox</td>
<td>Sample files, log files</td>
</tr>
<tr>
<td>OneDrive</td>
<td>Sample files, log files in the JellyBean android version (Huawei D200)</td>
</tr>
</tbody>
</table>
The Demo version of Oxygen Forensics did not give the opportunity of locating the deleted files on the smart phones which is a limitation on the Demo version of the software used in the project. It can be concluded that the cloud service provider, android versions and the forensics software used are the determinants of evidential files to be acquired.

6.3.2 Acquisition of Cloud Data Remnants

Android smart phone acquisition is yet to mature with the rapid releases of different version being released cyclically thus rendering digital forensics strides futile in the examination of these devices. This presents challenges of inadequacies that cannot be addressed by the differences in each platform introduced to the market. This section observed ACPO (2012), guidelines of observing procedures that will not alter the original evidence hence choosing the logical acquisition. The process of acquisition was performed with ease providing understandable results within a very short time. Unfortunately major data remnants like GPS coordinates, browsing history, profile pictures, usernames and passwords were visibly absent. This is due to the limited nature of the logical copy acquired by Oxygen Forensics. This is against Quick and Choo (2013a), Quick and Choo (2013b), Quick and Choo (2014) research whose findings revealed various evidential information including user names, passwords, file names, their content as well as date and times of access.

The logical acquisition used in this project tried to capture the evidence available on mobile devices that are highly volatile as compared to standalone computer systems. Mobile devices leave room for intrusion and alteration of evidence files due to existing network connections or any existing malware. Indeed in the forensics arena it is increasingly becoming difficult to acquire evidential data without interfering with the device especially when admissibility of the evidence in a court of law is of essence. As provided in the project findings, logical acquisition is less conclusive as it dwells on the file structure present in the smart phone without performing a detailed acquisition of the entire device as projected by a physical acquisition, which often leads to integrity issues, and trustworthiness of the evidence.

There is a need for defining and adopting sound logical acquisition methods that will bring out possible hurdles during investigations which will enable proper preparations in obtaining a complete set of evidence avoiding possible mishaps and losing/modifying forensic
evidence. This particular method was preferred so that the techniques, procedures and analysis tools used would not interfere with the adopted framework. Consequently as new techniques come up, with new advances in undertaking smart phone acquisitions, such as bypassing access controls, they will be addressed in the approach proposed to offer formidable evidence to be used in court.

Deleted files were not recovered as they reside within the physical memory of smart phones meaning that a bit by bit extraction method should be incorporated but this method is highly likely to be legally challenged. This is in harmony with Katz et al., (2013), who conducted a research on the logical acquisition of smart phones with the use of Cellebrite’s UFED and MicroSystemation’s XRY Complete and concluded that it is not possible to acquire data deleted data types like original videos.

6.3.3 Implication of the Cloud Data Remnants in Smart Phones Forensics

This was demonstrated in the comparison of time stamps and hash values detailed during the findings section. It was found that the process of uploading then downloading the test files did not alter the data content, as the MD5 hash values of the files remained the same. The file date and time stamps were, however different to the original test files, and this needs to be considered when forming conclusions in relation to the times and dates of the files within cloud storage accounts. It is concluded that the process of preservation should be undertaken and strictly observed while incorporating proper documentation. The time recorded on the smart phone reflects the time of download from the cloud storage service.

As outlined above, the process of downloading files did not alter the contents of the files as the hash values were the same as the original files. As the file date and time associated with the downloaded files was altered from the original file, it requires sound judgment of issues at hand. The information observed in the time and date stamps after the files were downloaded from the cloud storage accounts proved to be useful for an investigation, even though the data was different from the original file data, as the different timestamps associated with the different methods of downloading the files provides additional information which may be relevant to an investigation. This conforms to Quick et al., (2014)
research which revealed that timestamps on the downloaded Android devices differed from original timestamps.

Logical acquisition is less conclusive as it dwells on the file structure present in the smart phone without performing a detailed acquisition of the entire device as projected by a physical acquisition, which often leads to integrity issues, and trustworthiness of the evidence.

6.4 Conclusions

6.4.1 Cloud Remnants and their Location

During an investigation, the storage of data using cloud service providers, identification of possible locations with the data remnants types should be done at the commencement of an investigation. This will assure investigators of finding evidential potential locations and their inherent data, thus leading to actions that will secure this data in a timely manner. It was vividly shown that that an investigator can identify cloud storage account use by examining common files and file locations to locate relevant information.

As outlined, there is a wide range of investigation locations for an investigator to determine the use of cloud storage, such as; directory listings, prefetch files, link files, thumbnails, registry, browser history, and memory captures. By determining the data remnants, this project provides a better understanding of the type of artifacts that are likely to remain, and the possible locations to be used during investigations. The Jellybean Android version analysis provided very little evidential data as compared to the popular Lollipop version which may have flaws in the development life cycle of the software.

6.4.2 Acquisition of Cloud Data Remnants

Software forensics vendors should conduct intensive research for robust tools that can acquire data from a smart phone without the need to alter or physically damage smart phones of its inherent data. This will ensure the right judgments are delivered when convicting criminals and the right assumptions made. Logical acquisitions capture evidence available on mobile devices which is highly volatile as compared to standalone computer systems. Mobile devices leave room for intrusion and alteration of evidence files due to existing network
connections or any existing malware. Logical acquisition is less conclusive as it dwells on the file structure present in the smart phone without performing a detailed acquisition of the entire device as projected by a physical acquisition, which often leads to integrity issues, and trustworthiness of the evidence.

Indeed in the forensics arena it is increasingly becoming an arduous task to acquire evidential data without interfering with the device especially when admissibility of the evidence in a court of law is of essence. There is a need for defining and adopting sound logical acquisition methods that will bring out possible hurdles during investigations which will enable proper preparations in obtaining a complete set of evidence avoiding possible mishaps and losing/modifying forensic evidence. Consequently as new techniques come up, with new advances in undertaking smart phone acquisitions, such a bypassing access controls, these will be addressed in the approach proposed to offer formidable evidence to be used in court.

6.4.3 Implications of the Cloud Data Remnants in Smart phone Forensics

The time and date discrepancies are the only changes observed during the upload and download of files when accessing cloud storage. Sound judgment and extra evidential data like hash value can validate the findings. There were no changes to the file content therefore no implications were observed. Most cloud storage services allow the collaboration of documents and other files which is an added value by most providers. Despite the fact that the contents were unaltered, there arises an opportunity for the modification of files while stored in these accounts which can make changes in the originality of the uploaded files. As has been clearly stated, timestamps can be altered and hence change the direction of a case presented in court. It is therefore paramount that full comprehension is made of the timestamps presented with files notwithstanding the method of download chosen when proffering a judgment. Timestamps should not be regarded on face value but scrutinized in order to avoid wrong assumptions especially when an accomplice may offer different values as evidence.
6.5 Recommendations

6.5.1 Recommendations for Improvement

6.5.1.1 Cloud Data Remnants and their Location

Cloud data remnants are crucial for the solidifying of evidence in a case therefore speedy and procedural identification of evidence from the various sources should be of utmost importance. This data should be verifiable for integrity to ensure that it is not contested. This requires expert knowledge of the types of cloud data remnants, their location and methods of ensuring integrity.

6.5.1.2 Acquisition of Cloud Data Remnants

The limited nature of the logical acquisition should prompt massive development and research projects to produce robust and non complex software for law enforcers and leave physical acquisition for military intelligence scenarios. It is important to handle evidence and its exhibits with proper care while observing the APCO guidelines.

6.5.1.3 Implications of the Cloud Data Remnants in Smart Phone Forensics

The use of stronger hashing values should be considered to ensure the validity of the evidence. It will be of great benefit to educate the entire judicial system on the implications of differences in date and time during an investigation in order to proffer better judgments when giving a verdict.

6.5.2 Recommendations for Future Studies

It has been identified that conducting research into logical extracts of data from an Android phone may offer better results if licensed forensics versions are used. In addition, future research opportunities may include conducting research of other cloud storage services such as Bit Sync which use a peer to peer model. This will assist to determine data remnants from other cloud service providers and encompass a methodology that can be used to identify cloud storage providers and any remnants involved.
REFERENCES


R vs Edmonds, SADC 5 (District Court of South Australia February 4th, 2011).

R vs Paul James, 185 (District Court of New South Wales November 4, 2011).


