

# **Mobile Cloud Computing: Implications to Smartphone Forensic Procedures and Methodologies.**

Meng Zhu (Monica)  
BSc. (UoA, NZ)

A thesis submitted to the graduate faculty of design and creative technologies  
Auckland University of Technology  
in partial fulfilment of the  
requirements for the degree of  
Master of Forensic Information Technology

School of Computing and Mathematical Sciences

Auckland, New Zealand  
2011

## **Declaration**

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....

Signature

## Acknowledgements

This thesis was completed at the Faculty of Design and Creative Technologies in the School of Computing and Mathematical Sciences at Auckland University of Technology, New Zealand. During the time of writing this thesis, lots of support was received from many people. It is my pleasure to take this opportunity to thank all of you, without any of you, I would not have gone this far.

First of all, I would like to thank my family and Devonport Christian Family Church for the continuous prayers and blessings. I especially want to thank my beloved mother and wonderful dad who all provided amazing support and encouragement during the course of this thesis project, as well as at every stage of my life.

Huge thanks to my thesis supervisor Professor Ajit Narayanan, who gave me the freedom to choose my thesis topic and has given exceptional support throughout this time. Professor Ajit Narayanan provided ongoing inspiration, encouragement, excellent guidance, creative suggestions, and critical comments that have greatly contributed to this thesis. It has been a wonderful experience to be supervised by Professor Ajit Narayanan. My vision has greatly expanded with the astonishingly wide range of knowledge he has shared with me.

I would like to thank Dr. Brian Cusack for all the useful advice and support given for these two full years of Masters study. Dr. Brian Cusack has been a great mentor to me. He has not only given me support in my Masters study but also like a father, taught me many important lessons in life, for that I am very grateful. A big thanks also must be given to my colleagues especially Paul Black and Jason Forsyth for providing an excellent environment and advance knowledge in the real world of digital forensic procedures to ground my academic perspective.

I would also like to thank David Levis and Micro Systemation (MSAB) for lending me the mobile forensic tools XRYv5.2 to perform the research experiments. A deep appreciation to Craig S. Wright and Steve Whalen for providing useful information on this research in mobile Cloud forensic methodologies and techniques especially as there has been so little academic writing in this field.

## **Abstract**

The Smartphone is a powerful miniature computer that has phone capabilities and has been sold globally to billions of people, because of its flexibility for work and entertainment. Third party applications are the reason why the Smartphone is so popular, and Cloud computing is the driving force for the growth of these applications. The combination of Smartphone and Cloud computing technology has also led to many predictions. The forecast of Allied Business Intelligence (ABI) is that by 2014 mobile Cloud computing will become the leading mobile application development and deployment strategy (ABI, 2009). Gartner (2010) predicts that 90% of companies will support corporate applications on personal mobile devices by 2014. Gartner (2010) also predicts a huge increase in both mobile and Cloud computing, with an expected US\$6.2 billion to be spent on mobile applications and US\$68.3 billion on Cloud Computing services. However, it must also be remembered that, “the more popular the technology, the more opportunity exists for its misuse” (Turnbull & Slay, 2008, p.1355). Motivated by potential financial gain, Smartphone viruses have already been implemented through the utilization of Cloud computing technology to cause huge global economic damage.

There is a growing understanding of how to conduct digital forensic analysis on mobile devices. However, there is little understanding of how to apply digital forensic methodologies in Cloud computing, and even less understanding in how to apply forensic methodologies in mobile Cloud investigation. The aim of this thesis is to identify the impact of Cloud computing on Smartphone forensics and to test current mobile forensic tools, methodologies and procedures in different mobile Cloud forensic scenarios. Furthermore, the aim of this thesis is to provide recommendations in conducting forensic investigation in mobile Cloud computing. Future research direction within this research topic area will also be identified.

## Table of Contents

Declaration .....	ii
Acknowledgement .....	iii
Abstract .....	iv
Table of Contents .....	v
Appendix .....	ix
List of Tables .....	x
List of Figures .....	xi
Abbreviations .....	xii

## Chapter 1 – Introduction

1.0 BACKGROUND.....	1
1.1 MOTIVATION .....	2
1.2 THESIS STRUCTURE .....	6

## Chapter 2 – Literature Review

2.0 INTRODUCTION.....	9
2.1 MOBILE.....	10
2.1.1 Mobile Networks .....	11
2.1.2 Mobile Forensics .....	13
2.1.3 Mobile Forensics Evidence.....	13
2.1.4 Extraction Methods .....	13
2.1.5 Tools and Capabilities .....	16
2.1.6 Issues and Challenges.....	17
2.2 CLOUD COMPUTING.....	18
2.2.1 Essential Characteristics of Cloud Computing .....	19
2.2.2 Cloud Service Model.....	20
2.2.2.1 SaaS .....	21
2.2.2.2 PaaS.....	21
2.2.2.3 IaaS.....	22
2.2.3 Deployment Models .....	23
2.2.4 Core Technologies of Cloud Computing .....	23
2.2.5 Cloud Forensics.....	24
2.2.5.1 Preservation Phase .....	25
2.2.5.2 Acquisition Phase.....	26
2.2.5.3 Examination Phase .....	27
2.2.5.4 Reporting Phase .....	27
2.2.5.5 Benefits.....	27
2.2.5.6 Limitation / Challenges .....	28

2.3 MOBILE CLOUD COMPUTING .....	29
2.3.1 Mobile Cloud Architecture .....	30
2.3.2 Mobile Cloud Forensics.....	32
2.4 FORENSICS INVESTIGATION PROCEDURE.....	33
2.4.1 Preservation .....	34
2.4.2 Acquisition.....	35
2.4.3 Examination .....	37
2.4.4 Reporting .....	38
2.5 SUMMARY OF ISSUES AND PROBLEMS .....	38
2.6 CONCLUSION .....	39

### **Chapter 3 – Research Methodology**

3.0 INTRODUCTION.....	41
3.1 RESEARCH DESIGN.....	42
3.1.1 Questions and Hypotheses .....	42
3.1.2 Research Methodology .....	44
3.1.3 The Research Model.....	45
3.2 DATA REQUIREMENTS .....	47
3.2.1 Data Collection .....	49
3.2.2 Data Processing.....	50
3.2.3 Data Analysis .....	51
3.2.4 Data Presentation .....	52
3.3 EXPERIMENTAL CASE SENARIOS .....	54
3.3.1 Third Party Virus Application Investigation.....	54
3.3.2 Terrorists Utilise Mobile Cloud in a Criminal Act.....	55
3.3.3 Workplace Misconduct - Dropbox Incident .....	57
3.4 REVIEW OF SIMILAR CASE STUDIES .....	58
3.4.1 Internal Forensic Acquisition for Mobile Equipment.....	58
3.4.2 Android Forensics .....	59
3.4.3 Third party Application Acquisition .....	61
3.4.4 Forensic Information Acquisition in Mobile Networks.....	62
3.4.5 Cloud Computing Forensics .....	63
3.5 LIMITATIONS OF THE RESEARCH.....	64
3.6 CONCLUSION .....	65

### **Chapter 4 – Research Findings and Analysis**

4.0 INTRODUCTION.....	66
4.1 EXPERIMENTAL CASE SENARIO ONE.....	66
4.1.1 Stage One - Case Scenario Implementation.....	67
4.1.1.1 Pre-case simulation processing .....	67

4.1.1.2	Expected Outcome .....	69
4.1.2	Act - Apply Forensic Procedures and Methodologies.....	69
4.1.2.1	Preservation .....	69
4.1.2.2	Acquisition .....	70
4.1.2.3	Examination.....	71
4.1.2.4	Using other forensics methodologies to obtain missing evidence .....	74
4.2	EXPERIMENTAL CASE SENARIO TWO .....	77
4.2.1	Stage one - Case Scenario Implementation .....	77
4.2.1.1	Pre-case simulation processing.....	77
4.2.1.2	Expected Outcome .....	78
4.2.2	Act – Apply Forensics Methodologies and Procedures.....	79
4.2.2.1	Preservation .....	79
4.2.2.2	Acquisition .....	79
4.2.2.3	Examination.....	83
4.3	EXPERIMENTAL CASE SENARIO THREE.....	92
4.3.1	Stage one – Experimental Case Scenario Implementation.....	92
4.3.1.1	Pre-case simulation processing.....	92
4.3.1.2	Expected Outcome .....	93
4.3.2	Act – Apply Proposed Forensics Methodologies and Procedures.....	93
4.3.2.1	Preservation .....	93
4.3.2.2	Acquisition .....	94
4.3.2.3	Examination.....	95
4.4	CONCLUSTION.....	97

## **Chapter 5 – Discussion of Findings and Recommendation**

5.0	INTRODUCTION.....	98
5.1	DISCUSSION OF RESEARCH FINDING.....	99
5.1.1	Experimental Case Scenario One .....	99
5.1.2	Experimental Case Scenario Two .....	101
5.1.3	Experimental Case Scenario Three .....	104
5.1.4	Discussion Summary .....	105
5.2	RESEARCH LIMITATIONS .....	105
5.3	RESERARCH QUESTIONS AND HYPOTHESES .....	106
5.3.1	Research Question.....	106
5.3.2	Sub-Question .....	107
5.3.2.1	Sub-Question one.....	107
5.3.2.2	Sub-Question Two .....	107
5.3.2.3	Sub-Question Three .....	108
5.3.3	Sub-Question Answers .....	108
5.3.4	Hypotheses.....	109
5.3.5	Falsifying the Null Hypothesis .....	109

5.4 RECOMMENDED MOBILE INVESTIGATION PROCEDURES AND METHODOLOGIES.....	110
5.5 UPDATE THE FORENSICS INVESTIGATION METHODOLOGIES AND PROCEDURES.....	112
5.5.1 Preservation .....	113
5.5.2 Acquisition.....	114
5.5.3 Examination .....	116
5.6 CONCLUSION .....	116

## **Chapter 6 – Conclusion and Future Research**

6.0 INTRODUCTION.....	118
6.1 SUMMARY OF FINDINGS .....	119
6.2 LIMITATION OF THE RESEARCH.....	124
6.3 FUTURE RESEARCH.....	125
 <b>Publications</b> .....	 127
 <b>References</b> .....	 128



**Appendix**

Appendix A: Motorola Milestone XRY Extraction Logs .....	138
Appendix B: Motorola Milestone Rooting Procédures .....	153
Appendix C: Motorola Milestone XRY Extraction Logs after Rooting.....	156
Appendix D: SIM Card Extraction Logs .....	208
Appendix E: WiFi Connection Report.....	214

## List of Tables

Table 2.1: New Zealand Network Service Providers, Their protocols and Band frequency.....	12
Table 2.2: Overall Ranking.....	17
Table 2.3: Comparison of Computer Forensics and Cloud Forensics during the Preservation Phase.....	25
Table 2.4: Comparison of Computer Forensics and Cloud Forensics the during Acquisition Phase.....	26
Table 2.5: Comparison of Computer Forensics and Cloud Forensics during Examination.....	27
Table 4.1: Android Device Specification .....	67
Table 4.2: Motorola Milestone Preservation Procedures and Actions .....	69
Table 4.3: Motorola Milestone Acquisition Procedures and Actions .....	70
Table 4.4: Motorola Milestone Examination Procedures and Actions .....	71
Table 4.5: Evidence Comparison Table A.....	73
Table 4.6: Evidence Comparison Table B.....	76
Table 4.7: iPhone Specifications.....	78
Table 4.8: iPhone Preservation Procedures and Actions. ....	79
Table 4.9: iPhone Acquisition Procedures and Actions .....	79
Table 4.10: Comparison of Data Extraction by XRY and Oxygen.....	83
Table 4.11: Photos and Corresponding Location Overview .....	84
Table 4.12: Comparison Table of Data Extraction from Third Party Application by XRY and Oxygen.....	90
Table 4.13: Evidence Required and Evidence Found Comparison Table A .....	90
Table 4.14: Evidence Required and Evidence Found Comparison Table B.....	92
Table 4.15: iPhone 4 Technical Specifications.....	92
Table 4.16: Preservation Procedures and Actions Taken .....	93
Table 4.17: Acquisition Procedures and Actions .....	94
Table 4.18: Evidence Required and Evidence Found Comparison Table A .....	96
Table 4.19: Evidence Required and Evidence Found Comparison Table B.....	96

## List of Figures

Figure 1.1: Mobile Virus Growth from 2005 to 2010 .....	4
Figure 1.2: Virus Spreading Methods .....	5
Figure 2.1: Tool Analysis Pyramid .....	14
Figure 2.2: NIST Visual Model of Cloud Computing Definition .....	20
Figure 2.3: Cloud Reference Model .....	22
Figure 2.4: Network as a Service .....	30
Figure 2.5: Mobile Cloud Infrastructure .....	32
Figure 2.6: Mobile Cloud Computing .....	33
Figure 2.7: Preservation Flow Chart .....	35
Figure 2.8: Acquisition Flow Chart.....	36
Figure 2.9: Examination Flow Chart.....	37
Figure 3.1: CRM Framework.....	44
Figure 3.2: Action Research Cycle.....	45
Figure 3.3: Research Model.....	48
Figure 3.4: Data Map .....	53
Figure 3.4: Data Collection Workflow .....	59
Figure 3.5: Protocol Stack for Forensic Information Acquisition of a Mobile Device in a Wireless Network .....	63
Figure 4.1: Online Virus Scan Result.....	68
Figure 4.2: XRY features for Motorola Milestone.....	72
Figure 4.3: Wireless Traffic Capture Set up .....	75
Figure 4.4: TCP Stream Captured by Wireshark Showing that The User's Data is Transferred.....	76
Figure 4.5: SIM Card Information .....	81
Figure 4.6: XRY Features for Apple iPhone 3G.....	82
Figure 4.7: Oxygen Features for Apple iPhone 3G.....	82
Figure 4.8: Wi-Fi Connections .....	85
Figure 4.9: Locations Where Henry Connected to the Wireless Network. ....	85
Figure 4.10: Locations Where Henry Has Been .....	86
Figure 4.11: Skype Account Information .....	87
Figure 4.12: Skype Account Contact Information .....	87
Figure 4.13: Skype Chatting History.....	88
Figure 4.14: Skype Account Calls .....	88
Figure 4.15: Skype Call Contact Extracted by XRY.....	88
Figure 4.16: Messages Read by SkypeLogView .....	89
Figure 4.17: Skype Account Contact Information .....	89
Figure 4.18: Viber Contacts Data .....	89
Figure 4.19: Dropbox Application Information.....	91
Figure 4.20: Viber Call History .....	92
Figure 5.1: XRY Forensics Method and Device Supported .....	111

### **List of Abbreviations**

API	Application Programming Interface
ASP	Application Service Provider
ATM	Automated Teller Machine
CF	Compact Flash Card
CPU	Central Processing Unit
DD	Disk Dump
DNA	Deoxyribonucleic Acid
EEPROM	Electrically Erasable Programmable Read-Only Memory
FTK	Forensic Tool Kit
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IaaS	Infrastructure as a Service
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MD5	Message Digest
MMC	Multi Media Card
MMS	Multimedia Messaging Service
NaaS	Network as a Service
NIST	National Institute of Standards and Technology
NSP	Network Service Provider
OS	Operating System
PaaS	Platform as a Service
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PLIST	Property List
URL	Uniform Resource Locator
RAM	Random Access Memory
SaaS	Software as a Service
SD	Secure Digital

SHA1	Secure Hash Algorithms
SIM	Subscriber Identity Module
SMS	Short Message Service
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VM	Virtual Machine
WAP	Wireless Application Protocol
XML	Extensible Mark-up Language

# **Chapter 1**

## **INTRODUCTION**

### **1.0 BACKGROUND**

The chosen topic areas for this thesis consist of an overlap of two new growing information technology areas. The first is Smartphone forensics and the other is Cloud computing. Background information for both chosen topic areas of this research will be introduced. Furthermore, specific consideration in the thesis will be given to Smartphone forensics procedures and methodologies. The literature review evaluation includes Cloud computing technology and mobile forensics tools, methodologies and procedures.

Smartphones are widely used mobile devices that have been sold to people globally. Android, iPhone, and Blackberry are the three most popular Smartphones on the mobile market. Beyond just making phone calls, Smartphones offer a wide range of features, such as: browsing the internet, checking E-mails, road navigation, editing documents, video conferencing, playing music, and so on. These features make Smartphones much more popular than other mobile phones. The constraints on the mobile of weight, size, battery life and heat dissipation greatly reduce the capability for the range of applications that can run on these mobile devices. However, the new growing technology of Cloud computing could help mobiles overcome these current constraints by running and storing applications outside the mobile device. The key driving forces behind mobile Cloud computing are the ubiquitous wireless network, “falling storage costs, and progressive improvements in internet computing software” (Dikaiakos, Katsaros, Mehra, Pallis, & Vakali, 2010, p. 11).

Third party applications contain vast amounts of data that could be of interest in forensics investigations. A wide range of data can be obtained, such as the social activities of the user, and the places the user has been. Currently the Apple applications store has more than 350,000 applications available for downloading. Last year, 12 million Americans actively used mobile-banking

services, and this year it is expected to soar to 18 million, with the real growth being driven by Smartphones according to Red Gillen, an analyst for the financial services research firm Celent (Ante, 2010). “With Smartphone usage increasing exponentially, financially-motivated Trojans will be targeting this pool of potential victims,” and the threat “will continue to grow since the level of user awareness is low and there are not too many security features currently on the phone and platforms” (Thia, 2010, p.1). Andrew Hong, Chief investigative officer for ViaForensics tested five new mobile Cloud applications: Groupon, Kik Messenger, Facebook, Dropbox, and Mint.com. “All the applications failed to securely store username and application data” (NetQin, 2010a, p. 1). Four applications including the Groupon Android, the Kik Messenger iPhone and Android, and the Mint.com Android were storing passwords as plain text. Thus credential information could be easily obtained from these Smartphones.

Mobile forensics is still in its infancy and Smartphone forensics is facing many challenges in finding forensically sound methods for acquiring and preserving data. With the involvement of Cloud computing, obtaining data without altering the device is a very hard task. Currently, mobile forensics investigation methodologies remain unsophisticated. Logical extraction of Smartphones to retrieve deleted data is difficult. An iPhone needs to be jail-broken and an Android needs to be rooted to enable the extraction of a physical copy of the device. Keeping the investigation forensically sound is very difficult, when endeavoring to obtain all the data needed for a Smartphone investigation using current mobile forensics investigation methodologies.

The main research question for this thesis is to identify whether or not existing mobile forensics tools, methodologies and procedures are effective at investigating the mobile Cloud, and if so whether it is possible to perform sound mobile Cloud forensics investigations.

## **1.1 MOTIVATION**

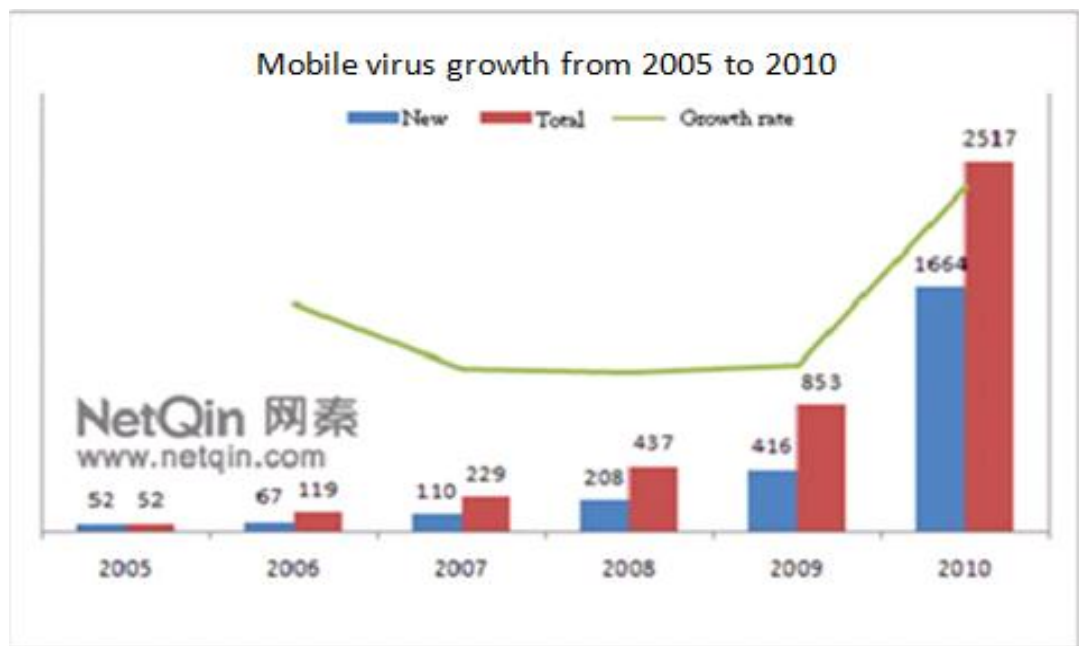
The motivation for researching forensics in mobile Cloud computing can be summarised in three main points. Cloud computing is being widely used across all IT areas. The tremendous changes Cloud computing brings place pressure on IT

and businesses, as there are high demands in building Smartphone and tablet business core applications. If such applications are not developed, the businesses will most likely lose ground to their competitors (NetQin, 2011a). Allied Business Intelligence (ABI) forecasts that by 2014 mobile Cloud computing will become the leading mobile application development and deployment strategy (ABI, 2009). According to a recent survey by the software testing firm AppLabs, 30% of companies in the Forbes Global 2000 were already using Cloud applications, with a further 20% planning to move to Cloud computing in the next 12 months (Frowen, 2011). Gartner (2010) also predicted a huge increase in both mobile and Cloud computing, with about US\$6.2 billion to be spent on mobile applications and US\$68.3 billion in Cloud computing services. Cloud computing is fast becoming the dominant technology in which mobile applications will operate and communicate.

The IT market research and analysis organization IDC has noted that those selling Android devices are experiencing the highest growth in sales among Smartphone manufactures. There is an expectation of a corresponding rise in the amount of malware that will target that platform as a result, according to Denis Maslennikov, Mobile research Group Manager at Kaspersky lab (Tanwar, 2010). With the advent of WIFI and the 3G cellular networks, mobiles now receive better internet connection and faster data transferring speed. The ease of use of the internet for checking E-mail and playing online games is making the mobile internet very popular, especially with the great capabilities offered by Smartphones. Most of the mobile applications distributed in recent years use Cloud computing technology; Facebook and Google Mail being good examples. Recent Smartphone threats include Trojans which are targeting iPhones, and fake Android banking applications. There are also Trojans targeting SMS messages to steal one-time passwords (Thia, 2010). The United States is not the only one to have had experiences of mobile virus attacks. Since the introduction in 2008 of 3G and the WIFI networks, China has also experienced a huge number of mobile virus attacks. According to the NetQin Cloud Safe Data Analysis Centre in China, by November 2010 mobile viruses had reached 2,357 and approximately 800 million mobile phones had been infected (NetQin, 2010b). Figure 1.1 is a bar graph based on China's mobile virus growth from 2005 to 2010 (NetQin, 2010b).



The bar graph shows a significant increased growth rate and 1,664 new viruses from 2009 to 2010.

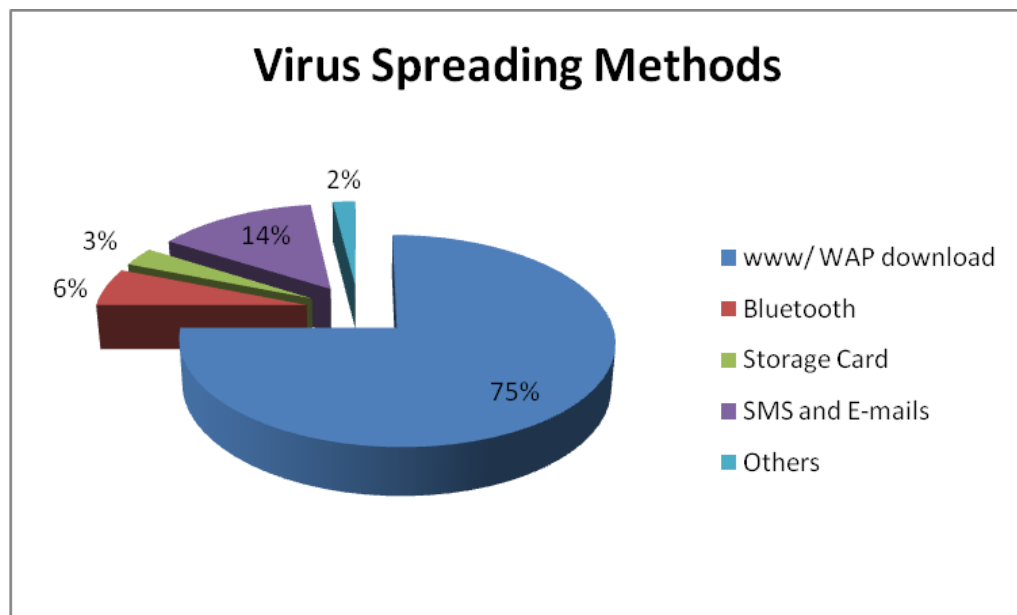


**Figure 1.1: Mobile Virus Growth from 2005 to 2010 (NetQin, 2010b, p. 4)**

Even though New Zealand has not yet been significantly affected by mobile viruses, there is no doubt mobile viruses will soon strike the mobile market, as people are starting to use mobiles more often for tasks that are financially related, such as mobile banking and mobile internet shopping. Google's vice-president for commerce and payments, Stephanie Tilenius (2010), states that Google have joined with leaders in the industry to build the next generation of mobile commerce (as cited in Shukla, 2011). The Google Wallet application has now been launched and this application enables customers to pay using their Smartphones. Currently 70% of mobiles do not have encrypted username and passwords, but store these credentials in plain text (NetQin, 2010c). Thus, there is expected to be an increase in the number of viruses being generated, due to the poor security measures of Smartphones, the richness of their stored information and the potential for large financial gain (NetQin, 2010c).

Viruses can infect mobiles in many different ways, including the internet Wireless *Application* Protocol (WAP) application downloads, SMS messages, E-mails, instant messengers, Bluetooth, and storage cards. WAP downloads are

responsible for 75% overall, making them the most popular way to spread viruses, as shown in Figure 1.2 below.



**Figure 1.2: Virus Spreading Methods (CCTV13News, 2010, p. 1)**

A very recent publicly known Android virus, *GeiNiMi*, launched an attack in 2009 within China and infected over 150 million mobiles. *GeiNiMi* caused damage to the economy estimated at \$300,000 US dollars, or 2 million RMB a day. The *GeiNiMi* virus infected mobiles after they installed a third party application that harboured a malicious code.

“The more popular the technology, the more opportunity exists for its misuse” (Turnbull & Slay, 2008, p. 1355). Gartner predicts that 90% of companies will support corporate applications on personal mobile devices by 2014 (NetQin, 2011b). This trend has led toward users having both corporate information and personal information on a single mobile device. A company has very little control over its mobile phones, thus any misuse may be difficult to track. An example could be of a confidential file being mistakenly or purposely uploaded onto Facebook. Cybercriminals and terrorists are likely to take advantage of any new technology to commit crimes. Cloud computing technology can be used to propagate a terrorist ideology, disseminate information, facilitate communication, or for an attack against someone’s digital information, computer systems, and/or computer programs. How to conduct forensics investigations in

Cloud and mobile Cloud environments under a global acceptance of Cloud services have become an emergent need, and a challenge for traditional digital forensics. However, at this stage Cloud computing forensics is only in its infancy. The full impact that the Cloud model will have on the digital forensic community is unknown (Biggs & Vidalis, 2009). Thus, it is important to understand the impact of Cloud computing on Smartphone forensics, and how existing mobile forensics investigation techniques, tools and methodologies would cope in mobile Cloud scenarios.

The aim of this thesis is to identify the impact of Cloud computing on mobile forensics in terms of tools, methodologies and procedures. In order to answer the research aim, research must first be undertaken into whether current forensic processes and procedures are still applicable to Cloud based mobile forensic investigation. It is currently not known whether digital forensic processes and procedures devised for mobile phones will continue to be effective in dealing with crime performed in a Cloud environment on a Smartphone device.

## **1.2 THESIS STRUCTURE**

This thesis starts with an introductory section, followed by six chapters set in a logical manner. In the introductory section, the thesis abstract, an acknowledgement, a table of contents, the list of the abbreviations, as well as the figures and tables used in this thesis are presented.

Chapter one briefly presents the background information of the chosen areas: Cloud computing, Smartphones and mobile forensics. The motivation for initially researching, and then conducting, such a thesis project is also introduced, and the structure of the entire thesis is also presented.

Chapter two provides an extensive literature review of the chosen areas of research and is divided into four main sections. The first section is Smartphone computing and forensics. First, the types of data that can be extracted and used as forensics evidence from a Smartphone are identified. This is followed by the identification of the tools and techniques that can be used to extract the data from the Smartphone for a forensics investigation. The challenges and limitations of

performing forensics work on a Smartphone, using existing forensics tools and techniques, will also be outlined.

In the second section, as Cloud computing is a relatively new area of computing and the concepts of Cloud computing are yet to be consolidated, the existing concepts of Cloud computing are researched, compared, summarised, and then presented. The possible impact of Cloud computing on forensics practices is also discussed. Furthermore, a comparison between traditional forensics and Cloud forensics will be presented. In the third section mobile Cloud computing is introduced, along with literature reviews of proposed mobile Cloud computing infrastructure from several scholars. Lastly, the issues regarding Mobile Cloud computing forensics are outlined. The last section of chapter two contains an introduction to the current US National Institute of Standards and Technology (NIST) standard mobile forensic procedures and methodologies for conducting an investigation. The literature on existing tools and techniques used to forensically extract data are reviewed and compared.

In chapter three, the proposed research methodologies for this thesis project are critically evaluated. In chapter three the research questions and hypotheses are formed. The Null hypothesis of this thesis is formed based on the literature review conducted in chapter two. The proposed research methodologies and research models are then constructed to help answer the research questions. Four testing phases are established and the data requirements of the research model that the testing will follow are investigated. Data generation, collection, analysis and reporting methodologies required for each of the testing phases are then outlined. Three Cloud based experimental case scenarios are then introduced to perform the experiments on. The experimental case scenarios are based on real cases. Five similar case studies relevant to the thesis topic areas are reviewed to help to identify better methodology to conduct investigation. The chosen studies, which range from academic sources to news articles, are: *Internal Forensic Acquisition for Mobile Equipment*, *Android Forensics*, *Third Party Application Acquisition*, *Forensic Information Acquisition in Mobile Networks*, and *Cloud Computing Forensics*. The limitations of the research are also described.

Chapter four reports the results of the research findings throughout each research testing phase, based on the three Cloud scenarios prepared in chapter three. Chapter four will examine the existing mobile forensics procedures, tools and methodologies on all three case scenarios to test if current mobile forensic procedures, tools and methodologies are still applicable to Cloud based mobile experimental scenarios, and the types of data they can and can not extract. Evaluation of the existing procedures, tools and techniques of each scenario will be given for the purpose of identifying problems in current mobile forensic procedures and methodologies. The research limitations are also presented in this chapter.

Chapter five first discusses and evaluates the results generated in chapter four. Based on the analysis of the data, the impact of Cloud computing on Smartphone forensics investigation will be discussed in depth. Investigation procedures, tools and methodologies used to generate these results will also be outlined to help answer the research questions and hypotheses. The research questions and corrected hypotheses will be presented based on the results generated from chapter four. If there are possible ways of falsifying a Null hypothesis in this thesis project, they will also be commented on. Finally, recommended Smartphone forensics investigation procedures to be adopted while investigating Cloud based Smartphone scenarios will be proposed. The revised mobile forensic procedures will in future provide a benchmark for Cloud based Smartphone forensics, assuming the Null hypothesis is correct.

Chapter six, the final chapter, will conclude the whole thesis and give future research directions for the problems in the chosen area. A summary of the findings will cover both the lessons learned from this research, and the limitations of the conducted research. To complete the chapter the research questions will be answered and areas for future research will also be outlined, based on the experiments conducted and the literature reviewed. Following on from this thesis a possible step could be research into the need for the deriving of forensically sound methodologies for other mobile devices such as tablets, which have numerous features in common with Smartphones and also contain rich data for evidence in an investigation.

## **Chapter 2**

### **LITERATURE REVIEW**

#### **2.0 INTRODUCTION**

Mobiles are a very powerful, fast growing and popular technology, especially with the recent integration of Cloud computing. As Smartphone technology improves, especially in memory storage, computational power and energy efficiency, there may come a time when they will be able to perform the same tasks that a PC is capable of, with greater portability. In order to build a better understanding in the chosen knowledge domain, the literary review is divided into four main domains: mobile computing, Cloud computing, mobile Cloud computing, and mobile forensics procedures.

The first selected literary topic is mobile computing. The literature on mobile devices helps to identify where, and what type of data can be obtained from the Smartphone handset for a forensics investigation. Mobile cellular networks often store forensics rich data that can only be provided by the cellular service providers. Furthermore, extraction methods for both the handset and SIM are introduced. Brothers (2009) outline five different extraction methods for mobile handsets, and discussion on the advantages and disadvantages of each method will be described in section 2.1.4. Evaluation of existing mobile forensics tools and their capabilities will be presented in section 2.1.5.

The second literary area selected is within Cloud Computing. A good understanding of Cloud computing technology is very important for mobile Cloud computing, as mobile Cloud computing is a process that utilises the Cloud services to the maximum in a mobile computing environment (Liu, Jian, Hu, Zhao, & Zhang, 2009). Cloud computing is believed to be one of the most transformative technologies in the history of computing, as it has made huge changes to existing IT infrastructure and, as will be shown later in this literature review, to traditional forensics investigations (Ruan, Carthy, Kechadi, & Crosbie, 2011). A comparison of traditional forensics and Cloud forensics will be

discussed in section 2.2.5, along with the Cloud forensics benefits and challenges, based on the literature reviewed. This leads to the third section, mobile Cloud computing.

In the mobile Cloud computing section, the literature reviewed will be on different proposed mobile Cloud computing infrastructure. Each of the infrastructures will be introduced in detail. Furthermore, the issues regarding mobile Cloud computing forensics will be outlined in section 2.3.2.

In section 2.4 the literature on existing standard mobile forensics procedures will be reviewed. The four domains of forensics investigation, including preservation, acquisition, examination and reporting will be discussed in detail, as associated with mobile forensics. Challenges and issues in each domain will be outlined and evaluated. Overall, the aim of the literature review will be to give a good overview of the background knowledge and problem areas of the chosen domain. Finally, research limitations in terms of literature cited in this thesis are explained in section 2.5

## **2.1 MOBILE**

Mobile phones can be defined as “handheld portable, battery-operated devices that are becoming increasingly sophisticated and incorporate features found in many other electronic devices” (Keisler, Daley, & Hagy, 2007, p. 30). Mobiles are a fast growing technology which is significantly changing the way people communicate. Initially, mobile phones were only designed to call and send short messages, hence the name Short Message Service (SMS). More and more features and functionalities were integrated into the mobiles to make them easier to use. The convenience offered by mobiles made them very popular and crucial to our everyday life. There are many different mobile models being manufactured each day by different vendors, such as Nokia, Apple and Samsung. With all the different kinds of mobile, Smartphones are leading in the market share. By the end of 2009, 46.3% of mobile phones in the United States were Smartphones, according to AdMob (2010). Smartphones offer a wide range of features beyond those of the standard cell phone, such as: mobile banking, mobile internet, document editing, video conferencing using third party applications, and will

eventually be able to perform all the tasks that a computer is capable of. The portability and flexibility offered by mobile computing make Smartphones very popular and also significant in making changes to everyday life.

“The massive penetration of Smartphones is driving a rapid wave of transformation around how we pay, bank, buy and sell things” (Botsman, 2011, p. 12). In March 2011, 68% of Australians planned to be using their mobile device for transactions and payments in the near future, according to a study conducted by the Nielsen Company (Botsman, 2011). Mobile commerce is a new innovation for Smartphones. AFR Boss Magazine (Botsman, 2011) summarised 10 hot mobile commerce trends. One of them, *wave and pay* means the user no longer needs a bank card for payments, as the bill will automatically be paid with a swipe of the mobile. A second trend is the *bump payments* application which, in a restaurant for example, makes splitting bills with friends simple and easy. A third trend, *mobile credit billing* is also simple and easy. The only thing needed to process the transaction is the mobile phone number. For example, to purchase pizza online the mobile number is entered onto the website. A text message will then be received to confirm the payment. The pizza will be purchased once this confirmation text is sent back. Mobile commerce also enables the making of payments using text messages. Just text the desired item's code to the store, which will then debit the person's bank account and mail the purchased product. Another is *location aware* commerce, which helps the user to identify the position of the nearest bank, or the closest ATM. If an *Event Cinemas* application is installed on the Smartphone, it can also help to identify the nearest cinema and the time of the movie that you wish to book. All of these functions are not possible without internet access, Cloud computing and a Smartphone.

### **2.1.1 Mobile Networks**

Mobiles can connect to a network either through a cellular provider network or through a wireless network. There are three cellular network providers in New Zealand: Vodafone, Telecom XT and 2degrees. The 1G cellular system has many deficiencies, such as inferior call quality, spectrum inefficiency and lack of encryption of communication. To overcome these problems the 2G cellular systems was developed. Currently more and more data consuming applications for



mobiles are being developed, with functions ranging from video conference and web browsing, to writing E-mails. Usually these are very bandwidth consuming and 2G systems are inefficient for such applications. “Despite 2G cellular systems’ great success and market acceptance, 2G systems are limited in terms of maximum data rate” (Nicolitidis, Obaidat, Papadimitriou, & Pomportsis, 2003, p. 12). When considering a simple transfer of a 2MB presentation for example, it would take approximately 28 minutes when employing the 9.6 kbps GSM data transmission (Nicolitidis et al., 2003). Thus the 3G cellular system was developed to cope with these current and future mobile market trends. Smart mobile devices such as iPhones and Google phones were designed especially for 3G cellular systems and these phones are the most popular in the market at present. Although 3G networks offer multimedia transmission and global roaming across a cellular or other single type of wireless network, there are still places out of coverage. Thus 4G cellular wireless networks are under development and aim to “support global roaming across multiple wireless and mobile networks” (Varshney & Jain, 2001, p. 94). Presently, GSM and 3G cellular networks are the dominant networks internationally. Table 2.1 below is the list of the networks, protocols and band frequencies for each cellular network provider in New Zealand.

**Table 2.1: New Zealand Network Service Providers, Their Protocols and Band Frequencies.**

Network	Protocol	Band Frequency
Vodafone NZ	GSM	900MHz (2G)
	GSM	1800MHz (2G)
	UMTS/HSDPA	900MHz (3G)
	UMTS/HSDPA	2100MHz (3G)
Telecom XT	UMTS/HSDPA	850MHz (3G)
	UMTS/HSDPA	2100MHz (3G)
2degrees	GSM	900MHz (2G)
	GSM	1800MHz (2G)
	UMTS/HSDPA	2100MHz (3G)

### **2.1.2 Mobile Forensics**

Mobile phone forensics is the “science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods” (Zareen & Baig, 2010, p. 47). Mobile forensics can also be defined as “the process that collected, preserved and analysed of relevant electronic evidence from the SIM cards, phone memories, removable cards and service provider and eventually gains the evidence which can be accepted by the court” (Dai, 2007, p. 100). Like any other digital devices, electronic evidence stored in mobile phones is extremely fragile. Inappropriate handling of the mobile could easily result in the altering, overwriting or deleting of data. Thus, care should be taken throughout the investigation to ensure the integrity of the data so that it is admissible in court.

### **2.1.3 Mobile Forensics Evidence**

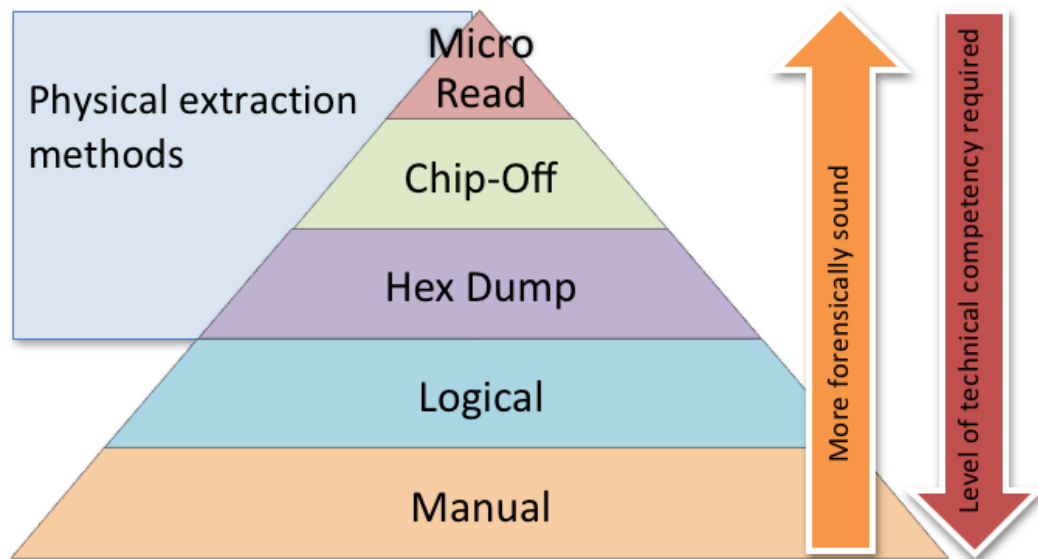
Mobile phones contain vast amounts of information that can be used as evidence (Williamson, Apeldoorn, Cheam, & McDonald, 2006). Mobile data evidence can normally be obtained from the Subscriber Identity Module (SIM), the internal mobile memory, external memory cards and the Network Service Providers. External memory cards may include SIM, SD, MMC, or CF cards. The information that can be found on the handset includes: contacts, call history, SMS messages, internet browsing history, audio files, E-mails, and more. The SIM card stores the raw data from the SIM card manufacturer, fixed information for the phone, short messages, fixed dial up, and the user's phone book. Additional evidence can also be found from network operators including: Subscriber information, location, call logs and SMS information.

### **2.1.4 Extraction Methods**

“Mobile forensic includes both SIM and Phone Memory analysis” (Zareen & Baig, 2010, p. 47). In order to extract information from the handset, the mobile phone needs to be connected to the examination computer by a cable, infrared or Bluetooth. Different methods need to be employed according to the case scenario, time availability and model of the mobile. Using a card reader to make a forensic copy of the SIM memory card is important, as a significant amount of deleted data

can be recovered from memory cards. Logical and physical extractions are the two main extraction methods commonly used by forensics investigators for phone memory acquisition, and both are needed for a complete forensics examination (Zareen & Baig, 2010). Logical extraction methods are faster, easier to use and very reliable, if compared with physical extraction methods. The weakness in logical extraction is that it can not extract all the deleted data from the phone memory. However, physical extraction can extract the complete image of the memory, even deleted data if it has not been overwritten. Physical extraction can also retrieve data without the SIM card being present, and can sometimes bypass and retrieve the security codes of the mobile handset.

Brothers (2009) outlines five levels of extraction from mobile devices shown in Figure 2.1. The bottom layer (Manual Acquisition) is considered to require the least amount of technical expertise but, at the same time, it is the least forensically sound approach. The top layer (Micro Read) is the most complex and requires the most technical knowledge to perform, but it produces the most forensically sound memory images.



**Figure 2.1: Tool Analysis Pyramid (Brothers, 2009, p. 3)**

Manual acquisition browses the phone contents manually through the user interface via the mobile's keypad or touch pad. Manual acquisition is simple to perform and works for almost all mobile phones. However, manual extraction can potentially take a long time, is prone to errors and will not recover deleted files.

Manual acquisition can only be used in situations where integrity of the data is not important, or when there is a life-threatening situation. Otherwise, evidence generated from this method can not be held as trustworthy evidence in court, as the experiments are performed on the original handset and it is very hard to identify whether the data has been contaminated, thus making it inadmissible in court.

The layer above manual extraction is logical acquisition. Logical acquisition involves using forensics software and tools to access and extract the logical files from the mobile handset for analysis. Logical extraction is quick to perform, easy to use and most of the commercially available tools support foreign languages. Westman (2009) views logical acquisition as not being forensically sound, as changes could be made to the data on the device while extracting the files, and logical acquisition also fails to provide access to deleted data (Zareen & Baig, 2010).

Hex Dump, Chip Off and Micro-Read are all classified as physical extraction methods. Physical extractions methods are more forensically sound, as a bit by bit copy of the memory can be extracted, but this requires highly technical expertise. Hex Dump extraction can be performed either by using specific software connected to the mobile through a cable, or by removing chips from the circuit board and 'dumping' the contents (Zareen & Baig, 2010, p. 51). Brothers (2009) states that hex dumping is the fastest growing segment in the cellphone forensic tool marketplace. However, data obtained from Hex Dump extraction is in a 'raw' form, which poses challenges in the interpreting of the data. However, deleted data from the mobile's internal memory and hidden data from the handset menus are able to be extracted.

Chip-off acquisition method involves physically removing the flash chip from the mobile phone and reading it with either an EEPROM reader or another phone, so as to conduct forensic analysis (Zareen & Baig, 2010). The chip-off method is potentially dangerous, as evidence can be permanently damaged or destroyed from de-soldering internal hardware components. The chip-off method however is forensically sound and is able to retrieve all the data on the device.

The final method of extraction is Micro Read, which provides a physical view of the electronic circuitry of the mobile phone's memory by using a high-powered microscope. This method requires the most technical expertise to perform. Micro Read is classified as being forensically sound, and can also work on damaged chips but is very expensive due to the high cost involved with microscopic reading. This method is suited for use on high value devices or on damaged chips.

### **2.1.5 Tools and Capabilities**

There are currently no standard methods for analyzing Smartphone internal memory. There are however many forensic extraction tools; such as XRY, Cellebrite, Oxygen, and FTK. Each forensics extraction product does well in some areas but not so well in others. Hoog and Strzempka (2010) of viaForensics released a white paper on evaluation of various iPhone forensic tools. Their evaluation showed that some of these tools, such as XRY and Oxygen, can extract data from many different phone operating systems and phone models. Table 2.2 shows the individual ranking for every piece of software tested on iPhones by viaForensics. The table evaluates each step of the process, including installation, acquisition, reporting and accuracy, and gives a rating in each individual column. The overall rating is calculated based on the average rating of each evaluation process. The overall average of all software tested is 3.3. Thus, the labelling of 'Below', 'Meet' and 'Exceed' is anything below 3.3, meeting 3.3, or above 3.3, respectively.

Zdziarski is a physical acquisition tool, and has the best accuracy and overall rating. FTS iXAM is the 2nd best acquisition tool for iPhone and, like Zdziarski, only works for iPhone operating systems. XRY and Lantern are both equal third. However, unlike other tools, XRY works for many different operating systems. Oxygen Forensics Suite and XRY are both commercially available tools, but only XRY can perform physical extractions on iPhones among all the commercially available tools.

**Table 2.2: Overall Ranking (Hoog & Strzempka, 2010, p. 1)**

Software	Installation	Acquisition	Reporting	Accuracy	Overall
Cellebrite	5.0	4.0	2.5	3.0	3.4 (Exceed)
FTS iXAM	3.0	3.0	3.0	4.2	3.9 (Exceed)
Oxygen Forensic Suite	5.0	4.0	3.0	3.1	3.5 (Exceed)
XRY	5.0	5.0	4.0	3.2	3.7 (Exceed)
Lantern	5.0	5.0	4.0	3.2	3.7 (Exceed)
MacLockPick	3.0	3.0	1.0	1.3	1.9 (Below)
Mobilyze	5.0	5.0	3.5	2.9	3.4 (Exceed)
Zdziarski	5.0	3.5	2.0	4.2	4.1 (Exceed)
Paraben	3.0	2.5	2.5	2.9	3.0 (Below)
Mobile Sync Browser	4.5	5.0	3.0	3.1	3.5 (Exceed)
CellIDEK	4.0	3.5	3.0	2.7	2.9 (Below)
EnCase Neutrino	4.5	4.5	3.0	2.9	3.3 (Meet)

### 2.1.6 Issues and Challenges

Mobile forensics is currently facing a number of issues and challenges. Mobile phones are a fast developing technology, with different manufactures storing their data differently. The lack of standardized methods of data extraction and the huge number of existing mobile operating systems available pose big challenges to the forensics field. There is a continual need to develop new forensics tools and techniques to keep up with the fast growth in mobile technology and different operating systems that are being continually implemented. Most commercially available tools do not provide solutions for physically damaged mobile phones and forensic examiners must be trained and equipped to handle such situations (Zareen & Baig, 2010). The lack of a conversational write-blocking mechanism

poses issues, as the extracted data may become less forensically sound, because data on an active mobile phone can be contaminated very easily during acquisition. There are also various methods available to remotely destroy or alter data on a mobile phone, although a shielded lab environment will help to solve this. However, if a phone network connection is not properly avoided during transportation by the phone being sealed in a radio isolation container, or by the use of another method such as enabling 'airplane mode', the data could then be easily contaminated, thus making the extracted data inadmissible in court. Sealing the mobile in radio isolated container while it is turned on also poses issues, as it can deplete the battery. Power consumption is increased as the mobile tries to connect to a network by raising its signal strength to the maximum (Jansen & Ayers, 2007).

## **2.2 CLOUD COMPUTING**

Cloud computing is the rapidly developing era of computing. Although there are many formal definitions proposed by both academia and industry, there is still no standard definition of Cloud computing. IBM defines Cloud computing as a “flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet” (Buecker, Lodewijckx, Moss, Skapinetz, & Waidner, 2009, p. 1). Oracle (2009) defines Cloud computing as “the convergence and evolution of several concepts from virtualization, distributed application design, grid and enterprise IT management to enable a more flexible approach for deploying and scaling applications” (p. 4). U.S. NIST (National Institute of Standard and Technology) defines “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 effort or service provider interaction.” (Mell & Grance, 2009, p. 1). Cloud computing enables everything that can be done on computers and/or servers, and beyond, to be performed on a small device such as a Smartphone. Regardless of the user location and the device used, all Cloud resources such as services, applications and processes can be rapidly deployed, scaled and provisioned, on demand.

The Cloud model provided by NIST consists of five essential characteristics, three service models and four deployment models. The key components are shown in Figure 2.2 and a detailed explanation is also provided below.

### **2.2.1 Essential Characteristics of Cloud Computing**

The five essential characteristics of Cloud computing are shown in Figure 2.2: broad network access, rapid elasticity, measured service, on demand self-service and resource pooling. These five essential characteristics demonstrate how Cloud computing relates to, or is different from other traditional computing approaches.

- **Resource Pooling:**

Computing resources like storage, processing, memory, network bandwidth, and virtual machines are pooled together to serve multiple customers using a multi-tenant model. Different physical and virtual resources are assigned and reassigned to the customers according to their demands during the day. Customers have no knowledge of the exact location of the provided resources. However, customers might be able to be informed of the higher levels of abstraction, like the country or the data centres where the resources are stored.

- **Broad Network Access:**

The broad network access enables thick or thin clients, like computers and mobile phones, to access the Cloud services via the network. The Cloud services include standard mechanisms, and other traditional or Cloud based software services.

- **Rapid Elasticity:**

The rapid elasticity provides flexible and easily scalable resources (e.g., Servers, applications, storage). Such characteristics enable customers to scale up and down the resource on demand, rapidly and elastically at any time.

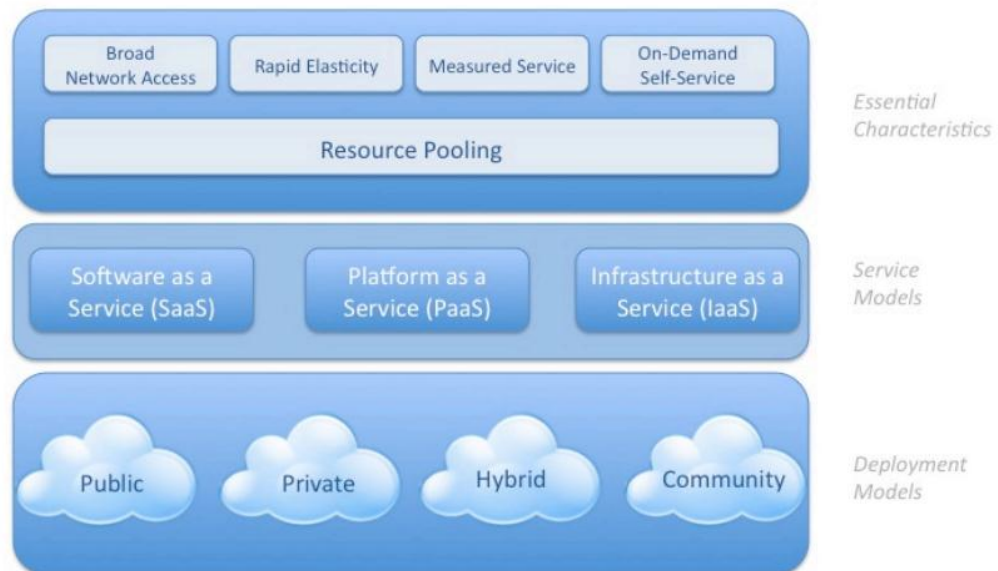


- **Measured Service:**

The Cloud resources usage is constantly monitored by leveraging a metering capability. The measured service can control and optimize the resource usage and then report to the customer in a "Pay-as-you-go" model.

- **On-Demand Self-Service:**

This characteristic enables the customer to order and manage services through a web portal or management interface without human interaction with the service provider.



**Figure 2.2: NIST Visual Model of Cloud Computing Definition (Mell & Grance, 2009, p. 1)**

### 2.2.2 Cloud Service Model

Cloud computing consists of three basic service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These models have been broadly used, implemented and well accepted by the users. A good example of IaaS is the Amazon Web Services, Elastic Compute Cloud (EC2) and the Simple Storage Service (S3). The Google App Engine is an

example of a PaaS. Some of the well known SaaS examples are, Salesforce.com and Netsuite.

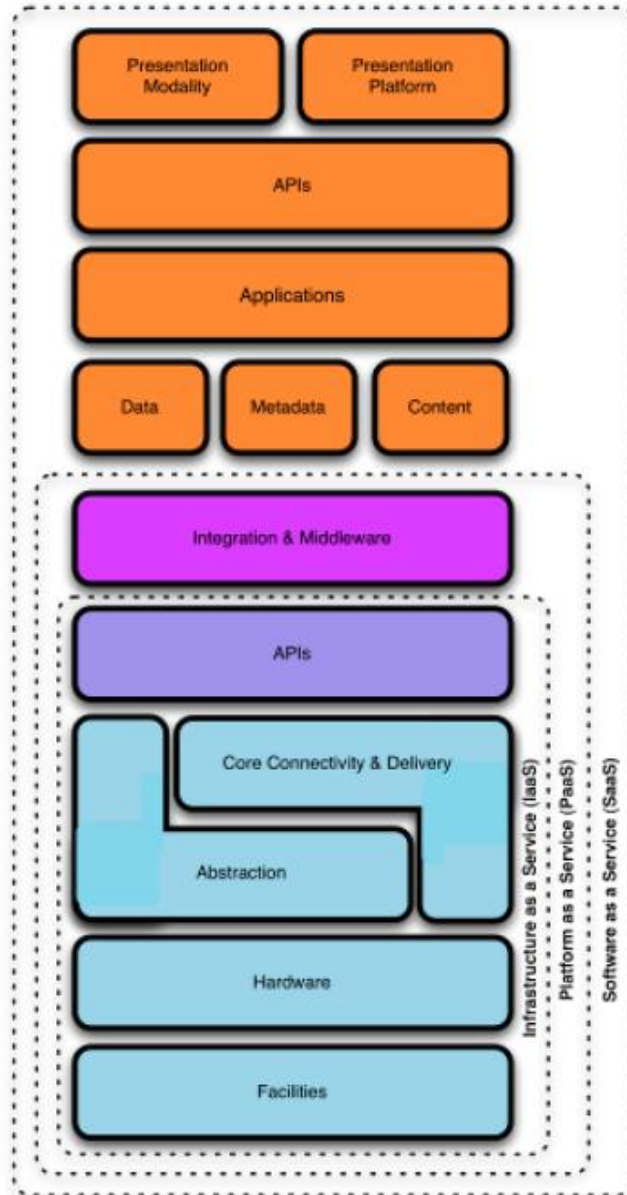
The definition of IaaS, PaaS and SaaS varies from country to country, and from industry to industry. Despite this, almost everyone agrees with Cloud Security Alliance (Brunette & Mogull, 2009) who state that IaaS is the foundation of all Cloud services, and that PaaS builds upon IaaS, and SaaS in turn builds upon PaaS, as described in the Cloud Reference Model designed by Cloud Security Alliance in Figure 2.3.

#### **2.2.2.1 SaaS**

Software as a service (SaaS) offers applications as services on demand. The Cloud provider supplies applications running on their own Cloud infrastructure and these applications can be accessed by various client devices through a thin client interface such as a web browser. For example, a web-based E-mail (Mell & Grance, 2009). Such characteristics of SaaS easily enable users of a mobile device to connect and access applications at the Cloud end. The consumer does not manage or control the underlying Cloud infrastructure, including the network, servers, operating systems, storage, or even the individual application capabilities. The consumer simply controls the limited user-specific application configuration settings.

#### **2.2.2.2 PaaS**

Oracle (2009) defines PaaS as an application development and deployment platform delivered as a service to developers over the Web. PaaS is able to provide all the computing resources needed to build a whole development life cycle of building and delivering web applications and services. The programming tools and programming languages environment required to build the applications will be provided by the service provider. Users do not need to manage or control the underlying Cloud infrastructure, but have control over the deployed applications and possibly application hosting environment configurations.



**Figure 2.3: Cloud Reference Model (Brunette & Mogull, 2009, p.18)**

### **2.2.2.3 IaaS**

Oracle (2009) view IaaS as the delivery of hardware (server, storage and network), and associated software (operating systems virtualization technology, file system), as a service. IaaS offers basic storage and computational capabilities as standard services on this infrastructure over the internet, where customers can deploy and run any operating system and applications. There are lower management requirements for the IaaS service provider than for PaaS, because the customers take the responsibility of managing their own data and software.

However, IaaS users do not need to manage or control the server, operating system or storage, which underlies the Cloud infrastructure.

### **2.2.3 Deployment Models**

The industry publications from Oracle (2009) and Sun Microsystems (2009) classify Cloud deployment models into three categories; Public Cloud, Private Cloud and Hybrid Cloud. However, NIST (Mell & Grance, 2009) adds another deployment model to the other three deployment models; the Community Cloud.

In a Private Cloud, the infrastructure is operated solely for an organization. The physical infrastructure is implemented and deployed in the enterprise's own data centre, or at a particular data storage collection facility, and is managed from inside by that enterprise's staff.

Community Cloud infrastructures are shared by several organizations and support a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). A Community Cloud infrastructure can be managed by either the organizations or a third party.

Public Cloud infrastructure is made available to the general public, or a large industry group. A Public Cloud infrastructure is owned and managed by a designated third party service provider and stored in that service providers' data centres. These data centres can be distributed anywhere around world.

The Hybrid Cloud infrastructure is a composition of two or more Private, Community, or Public Clouds which remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., Cloud bursting for load-balancing between Clouds).

### **2.2.4 Core Technologies of Cloud Computing**

In 2010 an article, "Understanding Cloud Computing Vulnerabilities" published in IEEE Security and Privacy, claimed there are three core technologies that Cloud computing relies heavily on. These technologies are Web Applications and Services, Virtualization, and Cryptography.

Web Applications and Services is the first key technology in Cloud Computing. SaaS and PaaS are heavily reliant on web applications and services (Grobauer & Schreck, 2010). SaaS is typically implemented as a web application and PaaS provides an environment for the development and run-time of web applications and web services. Associated services and APIs such as the management access for customers are typically implemented using web applications in IaaS.

Virtualization is one of the most important Cloud computing technologies. Many publications agree on the importance of virtualization technology to Cloud computing. Virtualized Infrastructure was proposed in Oracle (2009) as part of the key components in Cloud architecture. CSA (Cloud Security Alliance) (Brunette & Mogull, 2009) also claims that the ability to provide multi-tenant Cloud services at infrastructure, platform or software level is often underpinned by the ability to provide some form of virtualization to create economic scale. Virtualization plays a very important role in IaaS as it ensures that an application or business service is not directly tied to the underlying hardware infrastructure, such as servers, storage, or networks (Oracle, 2009). Cloud computing employs such an approach so as to optimize availability in a limited hardware environment.

### **2.2.5 Cloud Forensics**

Cloud computing brings significant changes to existing traditional computer infrastructures. These changes potentially change the entire traditional forensics framework. In the traditional digital forensics environment, investigators are permitted to seize computers, servers and other digital equipment and perform detailed analysis after transporting it back to the lab (Biggs & Vidalis, 2009). However, due to the nature of Cloud computing, everything runs virtualized, thus potential data evidence could be distributed over several servers in different geographic locations. As a result, gaining direct physical access to the servers is one of the most challenging parts in forensics investigation, due to multi-jurisdiction and multi-tenancy becoming a default setting of Cloud forensics. Cloud forensics is still a new growing area of forensics, so currently there are only a few publications available. However, the Department of Justice's research arm, the "NIJ, recently revealed plans to fund research into improved electronic

forensics in several areas, including the Cloud” (Lawton, 2011, p. 1). Based on the existing publications on Cloud computing, the differences between traditional computer forensics and Cloud forensics are identified in the following sections.

#### 2.2.5.1 Preservation Phase

Cloud forensics investigation is limited to acquiring machine images (ISO) rather than seizing all the hard drives of the physical machines. Thus virtualization forensics can be assumed to be used the most in a Cloud computing forensics environment. Virtual images can be easily examined via existing well recognized forensic software, such as Encase. These images can be transferred electronically over the Cloud, and inner Cloud file transferring is free and fast. Travelling to crime scenes to preserve evidence and transporting the evidence is not as much of a concern for Cloud computing forensics. For traditional computer forensics seized evidence is stored in the evidence room, whereas in Cloud forensics the evidence remains stored in the Cloud service provider's data centre, which can be a private or a public Cloud. A comparison table is shown in Table 2.3.

**Table 2.3: Comparison of Computer Forensics and Cloud Forensics during the Preservation Phase.**

Preservation processes	Sub-processes	Computer Forensics	Cloud Forensics
<b>Securing and Evaluating the Scene</b>	Go to crime scene	Yes	No
<b>Documenting the Scene</b>	Document the scene	Yes	No
<b>Evidence Collection</b>	Source of evidence	Physical hardware	Virtual Image
	Location	Crime scene	Cloud service provider's data centre
<b>Packaging Transportation</b>	Form of transportation	Physically	Electronically via Internet
<b>Storage of Digital Evidence</b>	Location	Evidence room	Cloud service provider's data centre.

### 2.2.5.2 Acquisition Phase

The amount of time needed for evidence acquisition in Cloud forensics is decreasing. Firstly, the MD5 is provided by the Cloud service provider, which saves lots of time in computing MD5 checksums (Reilly, Wren, & Berry, 2011). There is no need to travel offsite, which significantly saves on travel costs and the time needed to configure the software while working offsite. Cloud providers take care of the software configuration, and if a server in the Cloud gets compromised, a clone of the data off that server to the Cloud forensics server is only one click away. “Within the same Cloud, bit for bit copies are super fast” (Bolding, 2008, p. 1). RAM acquisition is extremely hard to perform in a Cloud computing infrastructure, as different RAM could be used to run different Virtual Machine (VM) or Cloud applications. However, in Cloud computing, it is very hard to determine where a VM was exactly executed as it dynamically migrates across physical systems and data centres. Specific Metadata needs to be accessed to locate where it was stored in the Cloud service providers’ data centre, and the data centre could be located anywhere in the world. “Metadata can also be lost if the data is downloaded from a Cloud” (Reilly et al., 2011, p. 33). Thus, any rich and useful source of information that could have been used as evidence, such as file creation, modification and access times could be lost.

**Table 2.4: Comparison of Computer Forensics and Cloud Forensics the during Acquisition Phase.**

Acquisition processes	Computer Forensics	Cloud Forensics
Acquisition time	Slow	Fast
RAM acquisition	Yes	Difficult
MD5 Hashing	Slow	Provided
Deleted data recovery	Possible	Difficult
Acquire metadata	Yes	Possibilities of loss of metadata.
Time Stamp	Accurate	Hard to keep the consistency.

Acquisition processes	Computer Forensics	Cloud Forensics
<b>Configure forensics software offsite</b>	<ul style="list-style-type: none"> <li>• Costly</li> <li>• Time taken for travel</li> <li>• Long Software configuration time</li> </ul>	<ul style="list-style-type: none"> <li>• Cheap</li> <li>• No need to travel</li> <li>• Supplied by the Cloud provider</li> </ul>

### 2.2.5.3 Examination Phase

For traditional computer forensics, evidence can be anything that is related to the crime, such as routers, printers and the hard drive. In Cloud computing, all the evidence will be provided by the Cloud service provider. Due to the powerful computational capability offered by Cloud, the time needed to access password protected documents is decreasing. Faster computational speed enables the system to test more possibilities within the same timeframe taken for traditional cryptography forensics.

**Table 2.5: Comparison of Computer Forensics and Cloud Forensics during Examination**

Examination processes	Computer Forensics	Cloud Forensics
Evidence collection	Hardware, network service provider	Cloud service provider
Cryptography	Slow	Fast

### 2.2.5.4 Reporting Phase

The reporting phase will remain the same for both mobile computer forensics, and mobile Cloud forensics. There are currently no publications available to comment on the reporting phase.

### 2.2.5.5 Benefits

Cloud computing can potentially benefit digital forensics investigations in many different ways. The first potential benefit could be the ability to store large amounts of audit logs at low cost. Logging normally needs huge storage space and high computational abilities. Insufficient disk space allocated by current infrastructure often makes logging an afterthought. Cloud storage is expandable, thus “logging everything then building logic around those logs is one of the many benefits which might make the network forensics investigators life easier”



(Morrill, 2010, p. 2). Cloud can potentially help with log searching by adding log indexing. Such an approach could save lots of time finding the right logs and make for more efficient reviewing also.

The successful implementation of forensic readiness is the second benefit. In the old infrastructure, it is very costly to implement forensic readiness as it requires lots of storage space and resources. As Cloud provides the service of IaaS, it would be very easy to implement and add a new forensics server in the Cloud. This would provide forensics readiness, and placing the forensics server offline until needed would also save money at the same time. Storage space is the only thing needing to be paid for and Cloud storage is cheap.

Another potential benefit is the elimination of forensics image verification time as some Cloud storage providers implement a cryptographic hash; for example Amazon S3. “Amazon S3 generates an MD5 (Message-Digest algorithm 5) hash automatically when the object is stored” (Reilly et al., 2011, p. 32). Thus there is no need to use external tools to do the MD5 check sums. The last benefit lies in preserving the evidence. The evidence can be stored in a secure Cloud environment as virtual images (ISO) without influencing the local data centre. Such an approach can reduce the list of people who can access the forensics images, thus providing a better chain of custody than locking them in a filing cabinet for years, where it might be damaged, lost or stolen (Morrill, 2010).

#### **2.2.5.6 Limitation / Challenges**

Cloud computing can potentially bring lots of benefits to the forensics investigation, but at the same time it also causes some limitations and challenges; one being the cross border jurisdiction problem. This is due to the Cloud data centres being distributed in many different locations. For example, one is being held in China and the other is running in New Zealand. Data stored across different data centres has the potential to impact significantly on the digital investigator and their ability to conduct an effect investigation (Biggs & Vidalis, 2009). For a digital investigation to be effective and admissible in court, certain changes in International cooperation are needed. “These changes must begin with the overhaul of International legislation that will police the boundaryless face of the internet and the technology that is facilitated by it; Cloud Computing” (Biggs

& Vidalis, 2009, p. 5). If these changes are not made, the number of unpunished crimes will be great.

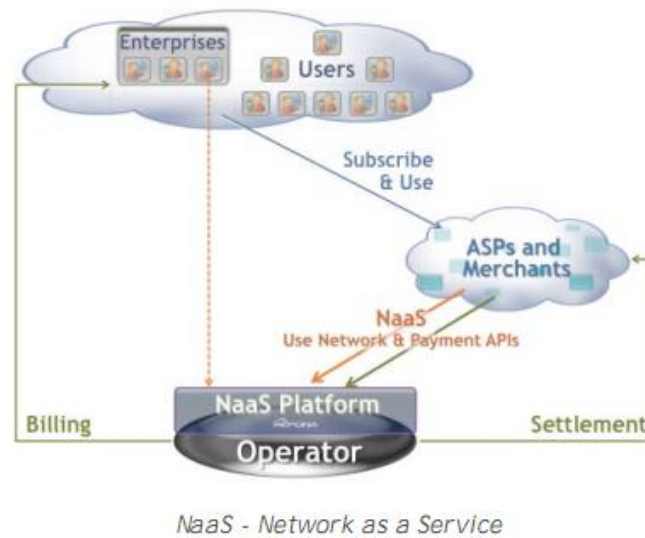
There are certain laws that need to be changed, such as the data protection Act in the United States. Businesses are required to control the way personal data is processed and stored. This is impossible within the public Cloud. Once the Cloud is implemented, the data is handed over into the Cloud guardians' hands. Thus, it is extremely unlikely for businesses to be able to control their data, and there is also no real assurances that when contracts are finished, that there will be no data left behind (Biggs & Vidalis, 2009).

### **2.3 MOBILE CLOUD COMPUTING**

Mobile Cloud Computing can be referred to as “technology utilizing Cloud computing in a mobile environment” (Liu et al., 2009, p. 2). The intention of the mobile Cloud computing concept is to take the Cloud Computing advantages and make them available to mobile users, and at the same time provide additional functionality to the Cloud (Klein, Mannweiler, Schneider, & Schotten, 2010). Mobile Cloud computing helps standard mobile devices to overcome the constraints faced by the current mobile architecture; in particular the constraints of data storage and processing power. Cloud offers enormous storage and processing potential by executing computationally intensive applications on the Cloud, which also extends the mobile's battery life. ABI Research (2009) forecasts that “business productivity applications will soon dominate the mix of mobile Cloud applications, particularly collaborative document sharing, scheduling, and sale force management apps” (p. 1). There are many well known Cloud apps available in the marketplace, such as: Google mail, Google maps, Facebook, and Dropbox.

In the Cloud Computing section three basic service models were described. AEPCON (2010) proposes an additional service model: Network as a Service (NaaS) for Mobile Cloud computing. Smartphones require network connection to operate, thus the Smartphone is always connected either through a cellular providers' network or a wireless network. The mobile network is normally operated by a mobile subscriber service provider, such as Telecom or 2 degrees.

Mobiles can also connect to wireless networks, replacing 3G networks for internet data usage. With the proposed NaaS model shown in Figure 2.4, “Telcos treat their key network assets communications, information and intelligence, and a billable customer base as marketable resources that can be offered to third parties on a commercial basis” (AEPONA, 2010, p. 6).



**Figure 2.4: Network as a Service (AEPONA, 2010, p. 6)**

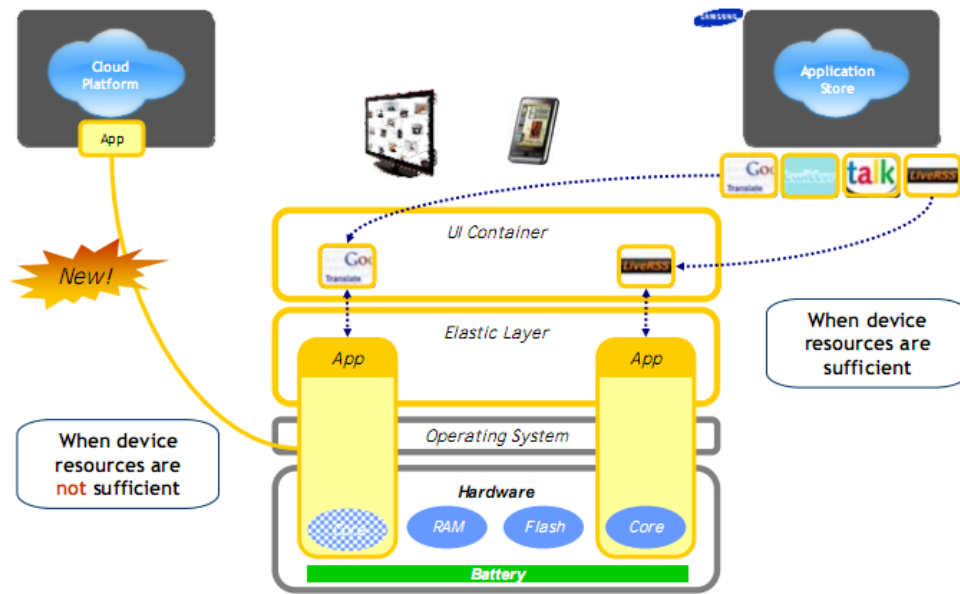
NaaS uses the *pay-as-you-go* model. Thus, NaaS will be billed based on the network usage via payment APIs when the applications provided by ASPs are being used. Different Telcos payment APIs can result in difficulties in port applications for subscribers from operator to operator and country to country. In order to solve this problem, Cross-network Service Providers (CNSPs) were proposed to provide “on-demand access across multiple networks to both network capabilities and payments resources” (AEPONA, 2010, p. 8).

### 2.3.1 Mobile Cloud Architecture

Mobile Cloud architecture has been proposed in many different papers using different approaches. In Giurgiu, Riva, Juric, Krivulev and Alonso (2009), the approach is to use the mobile phone as an interface that could connect and use the Cloud applications and resources. In this paper, Cloud is acting as a container for mobile applications. Mobile applications are pre-processed in the Cloud and offloaded to the mobile device interface. This paper mainly focuses on the

partition of policies to support the application execution on mobile devices. In Zhang, Schiffman, Gibbs, Kunjithapatham and Jeong (2009), an elastic mobile framework architecture is proposed and uses a similar approach to Giurgiu et al. (2009), with the difference being Smartphone users get to choose where to run their applications. This proposed model is shown in Figure 2.5. The proposed framework is built upon the existing mobile architecture. If the application requires heavy computation, the application will be calculated on the Cloud first and offloaded to the mobile device. If the device resources are sufficient, applications will run on the local device. An optimized mobile architecture is proposed by Liu et al. (2009). This architecture is a hybrid solution of combined mobile-agent technology and mobile Cloud computing. The mobile environments are divided into many cell regions and each cell region contains several Cloud units. The Cloud units from different cell regions connect together to form a mobile Cloud. The mobile Cloud supports computing ability and storage ability. The mobile is not communicating directly with the mobile Cloud but through a Universal Mobile Service Cell (UMSC). UMSC is used to search for the Cloud units that can answer the requests from the mobile host. Then the mobile host is connected to the Cloud units found by the UMSC.

In 2010, a different approach was proposed by Satyanarayanan, Bahl, Caceres and Davies (2010). The proposed architecture is similar to the architecture already reviewed where the mobile device acts as a thin client and the Cloud processes and stores all the data, and then offloads it to the mobile device. The difference is that the virtualization technology or Virtual Machine (VM) is used to connect the mobile to the Cloud via a Cloudlet. The mobile user “exploits VM technology to rapidly instantiate customized service software on a nearby Cloudlet, and then uses that service over a wireless LAN” (Satyanarayanan et al., 2010, p. 1). Network latency is a major issue in this proposed architecture. A Mobile Cloud Computing Middleware is proposed by Wang and Deters (2009) to enable mobiles to connect to existing resources efficiently and effectively in the Internet Cloud. The internet resources can then be accessed in two ways, either from a mobile application interface or the mobile browser.



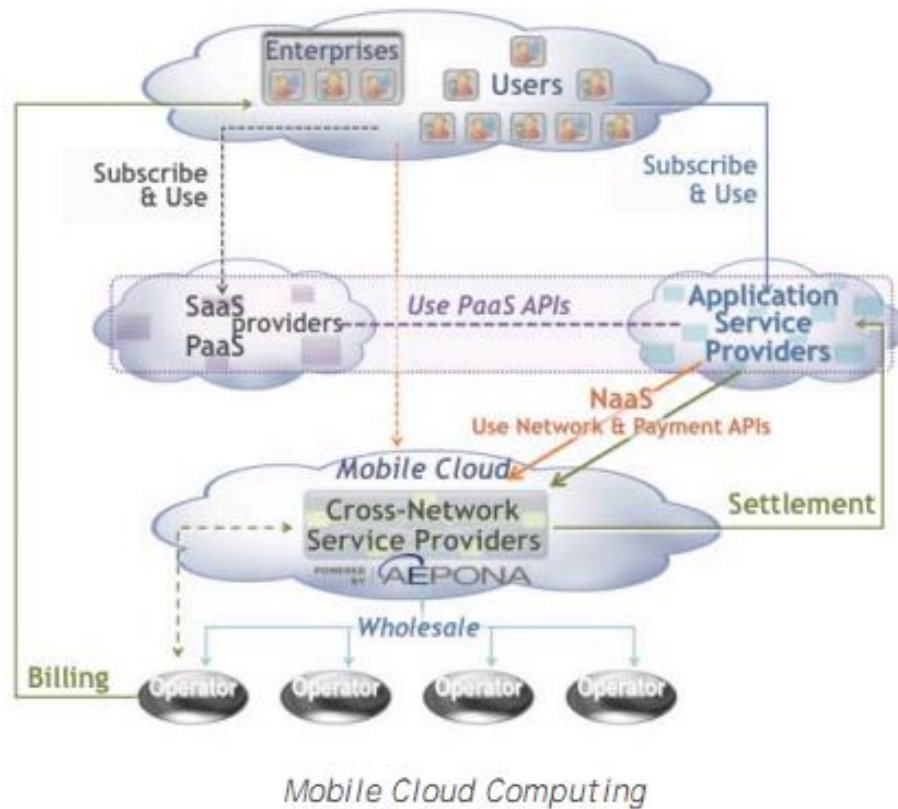
**Figure 2.5: Mobile Cloud Infrastructure (Zhang et al., 2009)**

The most recent Mobile Cloud Computing architecture is proposed by AEPONA (2010) and implements SaaS, PaaS and NaaS. Users obtain Cloud applications or storage through a web browser, or through a mobile API provided by ASP. The difference between this paper and other papers is the implementation of NaaS with which the users are billed, based on their network and application usage. The proposed architecture is shown in Figure 2.6.

### 2.3.2 Mobile Cloud Forensics

As proposed in the many papers outlined in the Mobile Cloud architecture section, the applications are mainly executed outside the mobile device and are running from the Cloud. As the Cloud contains forensic rich data, it is important to get the data that is stored or processed in the Cloud from the Cloud service providers. Currently, most commercially available forensic tools are able to interpret standard mobile telephone data, but extraction of relevant data from all third party applications has not as yet been developed (Levinson et al., 2011). However, commercial tools are slowly providing access to information stored by selected third-party application providers; an example being Oxygen, which has recently released an update to enable extraction of information from Skype applications and WiFi connections. In addition to the evidence that can be found on the

standard mobile devices, retrieval of forensic evidence from the Cloud service provider and the third party application providers is vital.



**Figure 2.6: Mobile Cloud Computing (AEPONA, 2010, p. 11)**

## 2.4 FORENSICS INVESTIGATION PROCEDURE

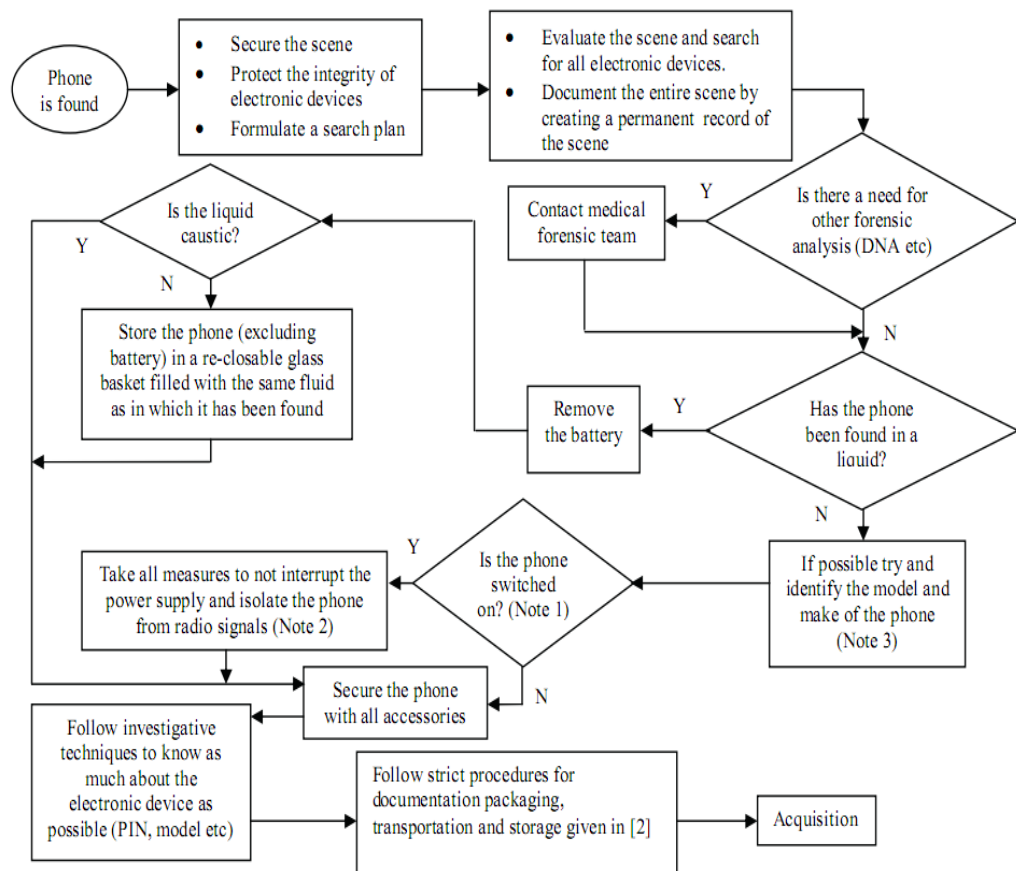
Digital forensics can also be defined as “the process of identifying, preserving, analysing, and presenting digital evidence in a manner that is legally accepted” (McKemmish, 1999, p. 1). Digital, or computer, forensics is the science that uses techniques to gather and analyse traces of human and computer generated activity in a manner that is suitable in a court of law (Wolthusen, 2009). Forensics investigation is divided into four domains: preservation, acquisition, examination and reporting. Digital evidence is extremely fragile and can be altered, damaged, or destroyed very easily by improper handling or examination. A failure made in the processes would result in the case being inadmissible in court and a waste of many hours of investigation (Biggs & Vidalis, 2009). Thus, proper and extra cautious handling of evidence is essential throughout the whole forensics investigation.

### **2.4.1 Preservation**

The National Institute of Standards and Technology (NIST) Guidelines - Special Publication 800-72 Guidelines on PDA Forensics (Jansen & Ayers, 2007) Guidelines on Cell Phone Forensics (Jansen & Ayers, 2007); and Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition (Raghav & Saxena, 2009) have similar preservation procedures and the procedures flowchart is presented below in Figure 2.7.

During forensics investigation, when the Smartphone is switched on, it is very important to isolate the phone from radio signals because remote wipe features are enabled on many Smartphones these days. Remote wipe software such as Mobileme could enable a user to wipe all their data remotely via a network connection. In the Guidelines on PDA, there were only two ways to isolate the radio signals, with one of them being turning off the phone. Turning off the device could pose the risk when activating the authentication codes to restart the phone. This could also result in complicating the acquisition by delaying examination through the difficulties of gaining access to the device. The second way was to keep the phone on and sealing it in a radio isolation container. This also poses problems. The battery life will be shortened due to increased power consumption from the phone raising its signal strength to the maximum as it tries unsuccessfully to connect to a network. This failure to connect to the network may cause some phones to reset, or clear their network data. The risk of improperly sealing the radio isolation container and unknowingly allowing access to the cell network also exists. The latter was introduced in Guidelines on Cell Phone Forensics in the enabling of the 'Airplane Mode'. Enabling the airplane mode means cutting off the network connection from the phone. This includes Cellular data services (text messaging, MMS, etc), WiFi, Bluetooth and GPS services. Enabling airplane mode can be applied to most Smartphones having 3G network connections. Such an approach requires interaction with the phone via the keypad, which poses the risk of potentially altering the evidence, making it less forensically sound. However, this method is not totally reliable either, because the airplane mode can be potentially disabled by a virus infected phone, meaning that

the network connection is not completely shut down and resulting potentially in the evidence being altered.



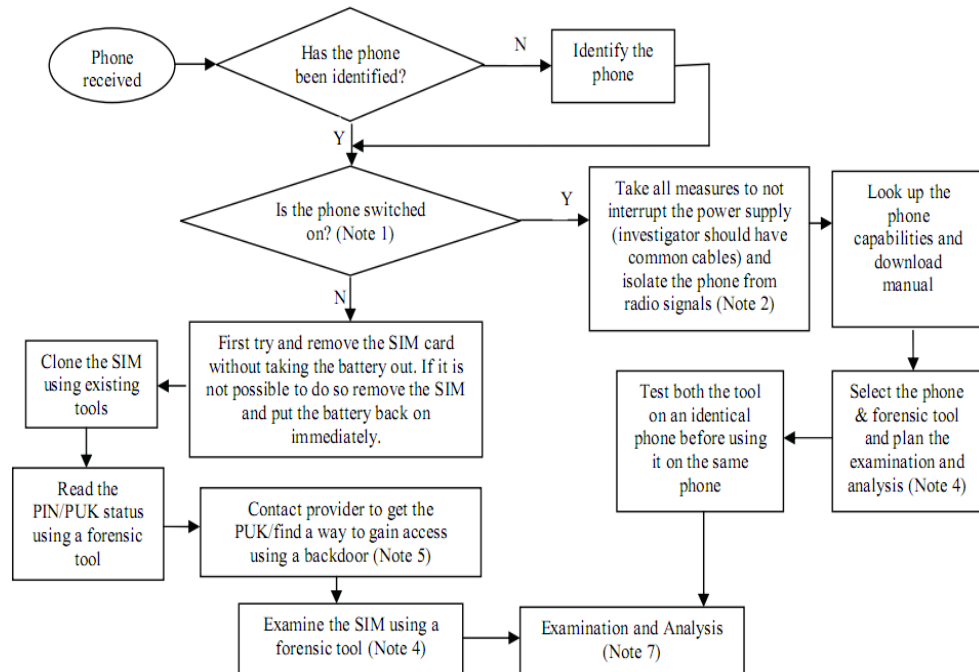
**Figure 2.7: Preservation Flow Chart (Raghav & Saxena, 2009, p. 7)**

## 2.4.2 Acquisition

The acquisition procedures proposed in Raghav and Saxena (2009) and Jansen and Ayers (2007) are focusing on the handset and SIM acquisition. Acquiring data from subscriber records is categorized in the examination phase. To recover the deleted data from the volatile or non-volatile memory was not mentioned in the Raghav and Saxena (2009) article, and data recovery is one of most important procedure in forensics investigation. “Potential evidence, particularly user data, may reside in either the volatile or non-volatile memory” (Jansen & Ayers, 2007, p. 44) and the phone’s memory often contains information, such as deleted data, that is not recoverable through either a logical acquisition or a manual examination. To preserve the integrity of the data, “a strong one-way



cryptographic hash (e.g., SHA1) should be performed to ensure that the additional images created from the master copy are identical” (Jansen & Ayers, 2007, p. 45).

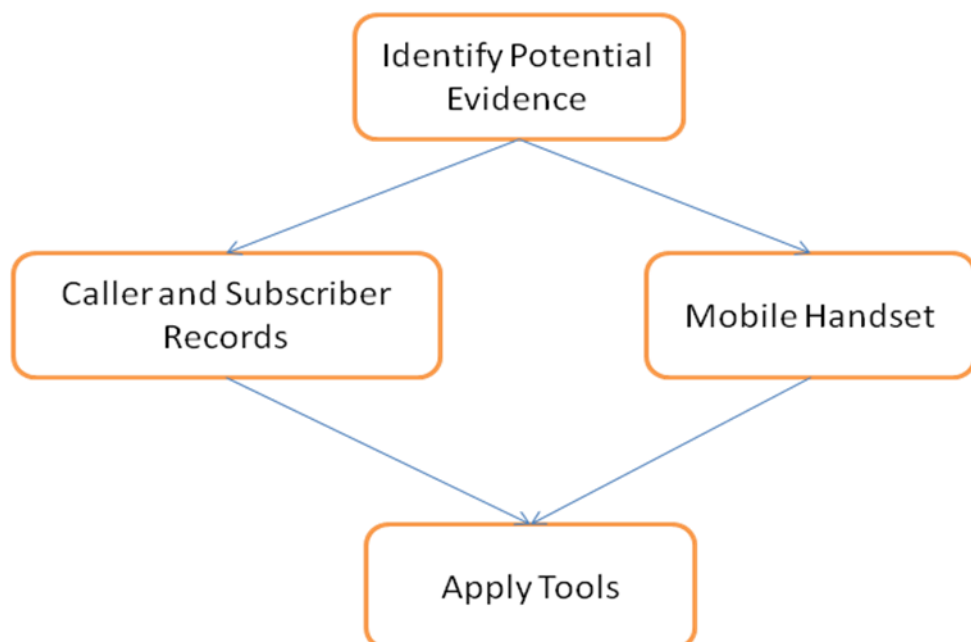


**Figure 2.8: Acquisition Flow Chart (Raghav & Saxena, 2009, p.8)**

In order to acquire data from a phone, a connection needs to be established from the device to the forensics workstation and the mobile device is required to be switched on. If the phone is switched off, the first evidentiary principle in ACPO (2007), that actions taken should not modify data contained on the device is violated. The goal during acquisition is to affect memory content as little as possible. A direct memory acquisition from the SIM recovers deleted data, whereas an indirect acquisition of the SIM can not recover this deleted data. However, a direct SIM acquisition requires the removal of the SIM from the phone, and typically the SIM is located beneath the battery. To remove the battery can result in losing both the non-volatile memory due to the power disruption, and the loss of the date and time values. If the phone is active, a joint acquisition of the handset and SIM contents should be carried out before a direct acquisition of the SIM is undertaken.

### 2.4.3 Examination

The NIST Guidelines - Special Publication 800-72 Guidelines on PDA Forensics (Jansen & Ayers, 2007) identifies only two important sections in the examination phase; one being the locating of evidence and the other being tool application. The potential evidence needs to first be identified in regard to the case scenario, and then the corresponding tools to apply to analyzing the evidence can be chosen. The evidence located in this guideline however, is only limited to handset data on the local PDA, and the potential evidence that can be extracted from a mobile carrier has not been taken into account. In the latter publication of NIST on Guidelines on Cell Phone Forensics (Jansen & Ayers, 2007) the call and subscriber records, as another important section in the examination phase has been added. Mobile Cloud computing technology, being widely applied to mobile phones, potentially has vast amounts of evidence stored in either the Cloud application or in Cloud storage. How to examine the potential information residing on the Cloud is one of the greatest concerns right now, as it is unclear what types of evidence data can be retrieved from the Cloud. The follow chat of examination is shown in Figure 2.9.



**Figure 2.9: Examination Flow Chart**

#### **2.4.4 Reporting**

Reporting is the process of maintaining careful records of all the actions and observations of all the steps taken, and conclusions reached from the investigation. The reports describe the results of the examinations and explain the inferences drawn from the evidence (Jansen & Ayers, 2007). Proper documentation enables individuals to re-create and examine the entire investigation process from beginning to end.

In general, the final report will contain the following information:

- Software-generated contents
- Data accumulated throughout the investigation
- Summarization of action taken
- Relevant evidence uncovered
- Audio or video types of evidentiary data. (These need to be included with the finalized report on removable media, such as thumb drive, CD or DVD-ROM, along with the appropriate application for proper display.)

“Incomplete reports or inconsistent testimony can negate even the best run investigations” (Britz, 2008, p. 343). Jansen and Ayers (2007) outline the importance of also identifying and eliminating any possible inconsistencies that may appear on the finalized report and the data presented on the user interface.

### **2.5 SUMMARY OF ISSUES AND PROBLEMS**

This section summarises the issues and problems identified in the research areas base on the literature review.

Standard mobile forensics posed few issues and challenges. There are no standardized data extraction methods for mobile forensics. The physical extraction methods extract more forensically sound data; however the costs are high and they require high technical expertise and longer duration periods to perform. Logical extraction methods are generally faster to perform. However, the integrity of the

data is less forensically sound and the mobile needs to stay active and connected in order to conduct the acquisition. In addition, a mobile can easily be contaminated during the acquisition due to most commercially available tools not currently offering write block features. The potential advantages brought by Cloud computing are huge; however the real impact it brings to traditional forensics is still unverified, as Cloud computing forensics is still in its infancy. The legislation and cross-border problems are more potentially serious than ever. There is no standard mobile Cloud computing infrastructure currently, even though all the proposed solutions of the applications being processed in the Cloud instead of running on the local device are similar. When the traditional forensics procedures were designed, the characteristics of Cloud computing were not taken into consideration, thus the current mobile forensics procedures only suit a small amount of the mobile Cloud forensics investigation.

A standard literature review should only contain references from reputable academic sources. However, because the topic under consideration in this thesis is still evolving in terms of mobile and Cloud developments, sometimes the best sources for illustrating contemporary developments are commercial and industrial, rather than academic. In many cases, this material is only available on the Internet. Every attempt has been made to ensure that the sources are as reputable as possible. However, no guarantee can be provided that the sources will continue to exist at their current URL locations for any length of time. The references are provided for readers to check the accuracy of the cited material and not as an indicator of authority or repute.

## **2.6 CONCLUSION**

Chapter two delivers a comprehensive literature review in the three main chosen research areas, mobile forensics, Cloud forensics and mobile Cloud forensics. In each of the chosen research areas, forensics capabilities, methodologies, limitations and challenges are discussed in details. As already stated in the literature review, the standard mobile forensic and Cloud computing forensic possesses a few issues and challenges and there is currently very little written about mobile Cloud computing forensics and its relationship to mobile forensics,

or to Cloud forensics. It is therefore unclear whether current mobile forensic tools, techniques and methodologies are still applicable to mobile Cloud forensics.

Chapter three will form a research plan and choose an appropriate methodology which could help to identify the relationship between mobile forensics, Cloud computing forensics and mobile Cloud forensics and then examine whether current mobile forensics tools, techniques and methodologies are still applicable to mobile Cloud forensics and if there is a need to create a completely new methodologies specifically for mobile Cloud Computing forensics.

## **Chapter 3**

### **RESEARCH METHODOLOGY**

#### **3.0 INTRODUCTION**

Chapter two reviewed literature relevant to Smartphones, mobile forensics, Cloud computing, Cloud computing forensics, and mobile Cloud computing forensics. With the aim of this thesis being to identify the impact of Cloud computing on the current mobile forensics tools, procedures and methodologies, which the literature review has now revealed, chapter three will establish the methods to help identify this impact.

Chapter three starts with establishing the research questions and research methodologies. Methodologies can be defined as “the analysis of the principles of methods, rules, and postulates employed by a discipline” (Creswell, 1998, p. 150). The experimental methodology of Computing Research Methods (CRM) is chosen to conduct the experiments in this thesis. Among all specific computing research methods, Action Research (AR) seems to be the best fit for this thesis project as AR forms an iteration of a learning cycle of constantly planning and reflecting to look for problems and solutions. The data collection methods, data processing methods, and data analysis and processing methods will also be introduced in section 3.2 under the data requirements section. Three experimental case scenarios for experimental purposes are then introduced in section 3.3. A data map will also be described in this section to display an overview of the research.

The review of five similar case studies conducted by scholars in the chosen fields will then be introduced in section 3.4. These case studies introduce different methodologies used in conducting investigation in mobile forensics and Cloud computing forensics. Learning from the existing methodologies outlined from these similar case studies could help investigators to pick the best suitable methodologies thus making investigation more efficient and forensically sound.

The limitations of current research methods will then be outlined in section 3.5, followed by a discussion of this chapter.

### **3.1 RESEARCH DESIGN**

In this section, the research questions and hypotheses are introduced to enable the achievement of the research aim. Based on these established research questions and hypotheses, a suitable methodology is investigated to then form a research model, upon which experiments are based. A blueprint of this thesis is delivered in a data map, which is also presented in this section.

#### **3.1.1 Questions and Hypotheses**

The research questions and hypotheses are constructed based on the literature review conducted in chapter two. This critically reviewed literature research has revealed that mobile Cloud computing remains a newly developed area of computing, and that the impact of Cloud computing on current mobile forensics investigation is still undefined, as there is still very little work that has been undertaken in this field. There are issues of how much current mobile forensics tools, techniques, procedures and methodology are affected due to the involvement of Cloud computing. Thus the aim of this thesis project is to identify these impacts that Cloud computing is having on mobile forensics and to make recommendations for mobile Cloud forensics investigation if appropriate. In order to achieve this research aim, the main research question for this thesis project is:

*Is there a need to develop new forensics tools, procedures and methodologies for mobile Cloud forensics investigation?*

The hypotheses for the main research question are as follows:

Null hypotheses:

*H<sub>0</sub>: Changes need to be made to current mobile forensics procedures; the combination of existing mobile forensics tools and methodologies are able to acquire and preserve the required evidence needed for mobile Cloud computing forensics investigations. Thus, there is no need to develop new mobile forensics tools, procedures and methodologies.*

*H<sub>1</sub>: The existing mobile forensics methodologies and procedure can retrieve all the data needed for Mobile Cloud computing forensics investigation. Thus, there is no need to develop new mobile forensics tools, procedures and methodologies.*

The alternative hypothesis:

*H<sub>2</sub>: There is a need to develop a new forensics methodology and associated procedures.*

In order to answer the main research question and identify the impact of Cloud computing on forensics investigation, the current mobile forensics need to be tested on mobile Cloud computing experimental case scenarios.

Thus the first sub-question is:

*What data can be acquired and preserved using the existing mobile forensics tools, methodologies and procedures in mobile Cloud computing forensic investigations?*

At present, there is still insufficient knowledge regarding the type of Cloud data that can be extracted from a Smartphone using existing mobile forensics tools and methodologies Cloud computing enable files to be stored and applications to be processed outside the Smartphone This raises the concern as to what data can be acquired and extracted from a Smartphone, and how much of this data that could be preserved using existing mobile forensics tools, procedures and methodologies. Thus the second sub-question is:

*Can existing mobile forensics tools, procedures and methodologies acquire and preserve all the evidence needed for mobile Cloud investigation?*

The third sub-question is reliant on the answer to the second sub-question. If the current mobile forensics tools, procedures and methodologies could retrieve all the evidence needed for mobile Cloud investigation, the hypothesis  $H_1$  is proved to be right. This means Cloud computing does not make an impact on Cloud mobile forensic investigations. Therefore, there is no need to develop a new



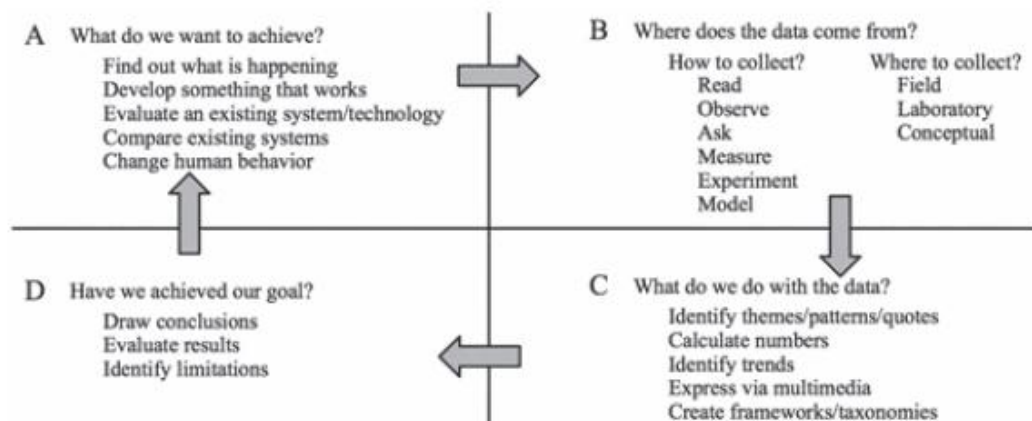
forensic methodologies and associated procedures. If the current mobile forensics tools, procedures and methodologies can not fully extract the evidence needed for undertaking an investigation, third sub-question need to be answered which is:

*Are there any existing methodologies that could help to seize the missing data?*

If the missing data can be acquired and preserved using the existing forensics methodologies, Null hypothesis  $H_0$  is then proved to be the answer to the research question. Otherwise, the alternative hypothesis  $H_2$  is the answer to the research question. Therefore, a need to develop new forensics tools, procedures and methodologies for mobile Cloud forensics exists.

### 3.1.2 Research Methodology

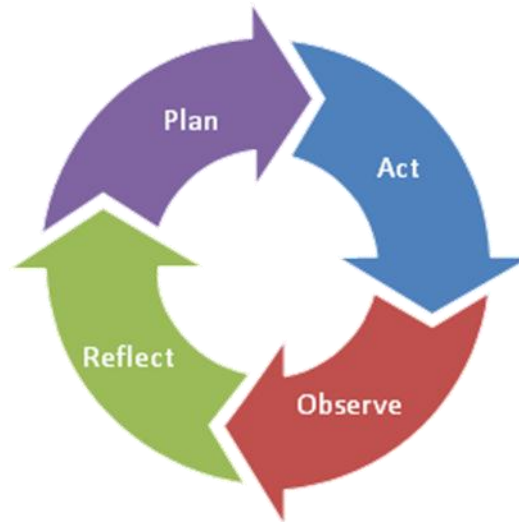
Computing Research Methodology framework shown in Figure 3.1 described in paper (Holz, et, al., 2006, p.102) is chosen to build the thesis experiments upon as the framework demonstrated a logical and constructive way to conduct experiments by seeking answers to the research questions during experimenting.



**Figure 3.1: CRM framework (Holz, et, al., 2006)**

Action research seems to fit in this framework very well as the four stages of the Action Research has been planning, acting, observing and reflecting. Action research is defined as “learning by doing” (O’Brien, 1998, p. 3). Action research is cyclic, with action and critical evaluation taking place in turn. Simple four

phase cyclic processes of plan, act, observe and reflect is the action research model proposed by Kemmis (1988). The research model is shown in Figure 3.1.



**Figure 3.2: Action Research Cycle (Kemmis, 1988)**

Once the evaluation phase of the action research process has reviewed the previous actions taken, and has identified the problems, then plans can be undertaken to solve these problems during the next action process. This is also the reason that action research was chosen to be the research methodology for this thesis project. The thesis research questions were developed in a logical manner, with sub-questions needing to be answered in sequence in order to answer the main research questions. Action research suited the theme of the research questions, thus enabling the testing of the Null hypothesis, as the Null hypothesis is established from the predicted answers of the sub-questions, which were developed based on the literature review.

### **3.1.3 The Research Model**

The research model chosen provides the framework within which experiments were undertaken. The aim of this research project is to identify the impact of Cloud computing on mobile forensics and answer the research question of whether or not there is a need to develop new forensics tools, procedures and methodologies for mobile Cloud forensics. Furthermore, the aim of this research

project is to give investigators recommendations for investigation in mobile Cloud forensics. This designed research model contains four phases. In the first phase case scenarios are established to conduct experiments, which took place in phase two of the action research. Based on the results collected and analysed from these experiments in phase two, phase three identifies the impacts of Cloud computing on mobile forensics. Phase four gives investigators recommendations for mobile Cloud forensics investigation.

The purpose of phase one was to set up experimental case scenarios for this research to experiment on. The three different case scenarios regarding mobile Cloud investigation are introduced in section 3.3. Action research was carried out based on these case scenarios, one by one.

Phase one needed to be completed before undertaking phase two. Phase two was where the action research took place. In this phase, most of the data needed to answer the research questions was collected and analysed. As shown in section 3.1.2, the four stages of the action research are *plan*, *act*, *observe* and *reflect*. In this stage plan, the experimental case scenarios established in phase one were simulated in a sandbox environment, one by one. Understanding and correctly simulating the experimental case scenarios was very important, as control data needed to be identified in this phase. Control data is the baseline of evaluating whether all the data needed for the investigation was acquired and preserved. The act stage was where NIST standard mobile forensic procedure and methodologies were applied in the investigation, using forensically sound mobile forensics tools. Journals were recorded based on the investigation methodologies, procedures and tools used throughout the investigation. In the next stage of observation, the extraction logs generated in the act stage were reviewed to identify the type of data that was extracted in order to answer the first sub-question. In the last stage of the action research, based on the control data generated in the plan stage, extraction logs were reviewed to identify what data was found and what was missing. Thus sub-question two is being answered. If all the data found compared to control data in the first iteration of the action research process, then hypotheses  $H_1$  was the answer for the research question. If only some of the data was found, the potential solutions for finding the missing data

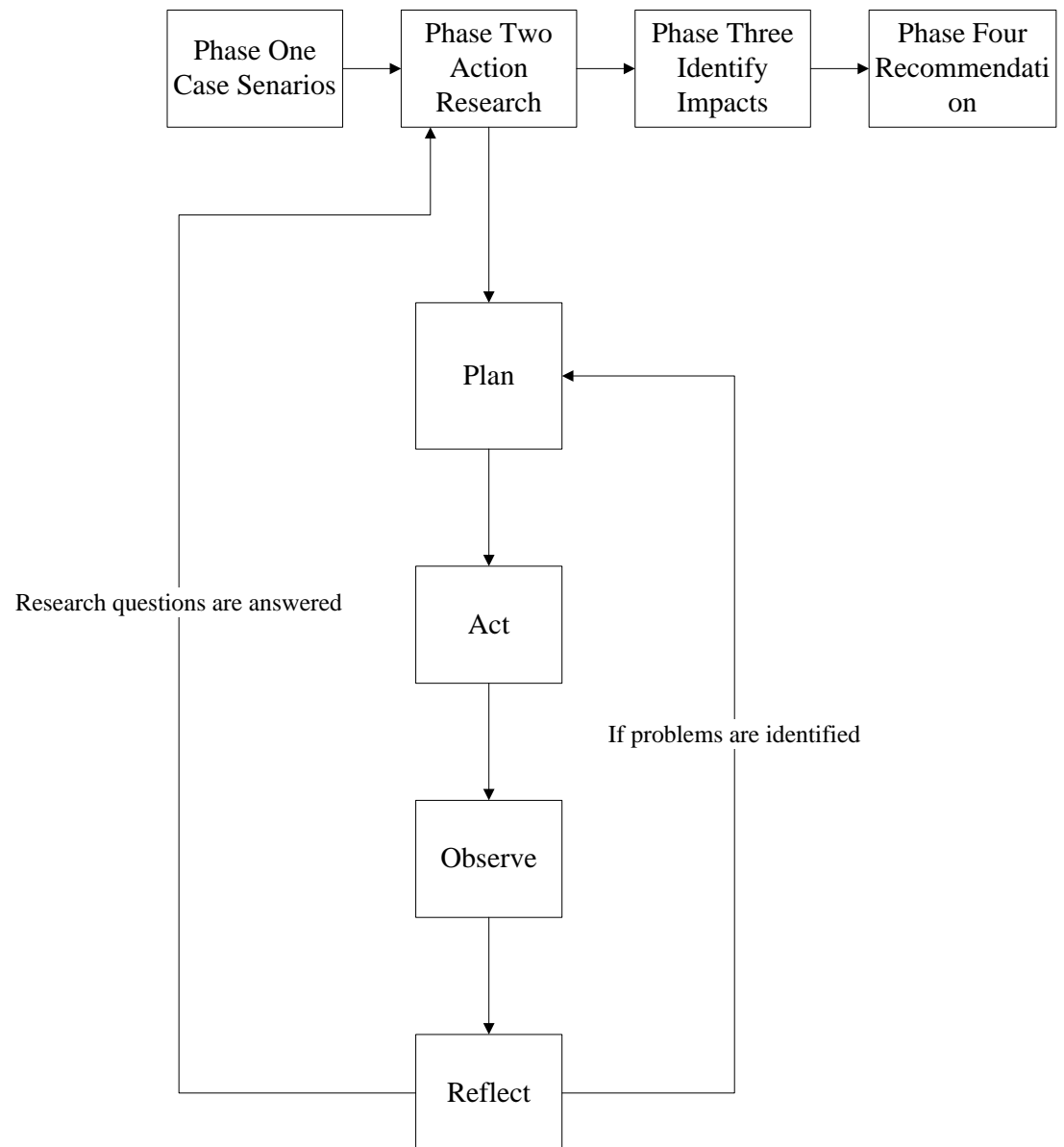
needed for the experiment would be investigated, and then the looking for existing forensics methodologies that could obtain the missing data. Thus, a new plan to answer sub-question three is formed. Then the whole action research model starts all over again to test the proposed methodologies. If the proposed methodology successfully obtained the missing data, the answer for the research question is hypotheses  $H_0$ . Otherwise,  $H_2$  is the answer for the research question.

Phase three of this research model was to identify the impacts of Cloud computing to mobile forensics investigation. Impacts to identify tools, procedures and methodologies will be made based in the three case scenario experiments in phase two. For each experimental case scenario, the impacts made by Cloud computing to the mobile forensics in context of the four investigation domains will be identified based on the data generated from phase two. The four mobile forensics investigation domains will be discussed in a sequence. The impacts to the tools and methodologies will be identified within the preservation, acquisition and examination domain.

The last phase of the research model is the giving of recommendations to investigators in mobile Cloud forensics investigation. The recommendations will be made on forensics procedures and methodologies according to the answers gained to the research questions and the impacts outlined in phase three.

### **3.2 DATA REQUIREMENTS**

The data required to answer the research questions and achieve the research aims will be identified in this section. There are five types of data that need to be collected and analysed throughout the research phases. They are scenario data, control data, journal, extraction logs, data comparison results and problem solutions.



**Figure 3.3: Research Model**

The first data needed is the data to set up the experimental case scenarios. Both real mobile forensics investigation case and cases generated based on the understanding of potential mobile Cloud computing investigation are used as case scenarios for the experiment tests. Control data needs to be collected from the first stage of phase two, to act as the baseline of data that can be used to make comparison, in order to answer the research sub-questions. A comprehensive journal will be documented of every action taken during the experiments, and this will be documented in chapter four to ensure all processes are repeatable.

Extraction logs are collected in stage three of phase two. Extraction logs are the experimental results generated by the forensics tools and is attached in the appendix. Comparison data needs to be collected to identify if the data extracted using the current mobile forensics tools, procedures and methodologies was all the data listed in the control data, so that the sub research question can be answered. Based on the comparison data analysis, and the data identified that can not be extracted by current forensic tools, procedures and methodologies, research will be conducted to find solutions.

### **3.2.1 Data Collection**

This section will describe how the six types of data required were collected, as introduced previously in the data requirements section. Data was mainly collected in the first two phases of the research model.

There were three experimental case scenarios established for the conducting of experiments. Due to mobile Cloud forensic still being in its infancy, there is very little literature written in this field. Thus, only one experimental case scenario is conducted based on a real case study; the other two are derived experimental case scenarios based on the facts gathered from research conducted from a wide range of reliable sources, from academic literature reviews through to news articles.

The control data identified depended upon the case scenario used. Based on the literature review conducted in chapter two and the advice given by the mobile forensics experts in the field, the given experimental case scenario control data was established.

The journal data was collected during the action stage of phase two. Journaling is a documentation process which records everything that has been done during the whole investigation process, including all the tools, procedures and methodologies used to conduct the experiments. The reason to keep the journal is to ensure that the same results can be produced using the same tools, procedures and methodologies recorded in the journal.

Extraction logs are the logs generated by the chosen forensics tools or methodologies employed to conduct the investigation. The tools can be both commercially available and forensically sound, or open sourced tools.

In order to collect data comparison results, a comparison needs to be made between the control data and the extraction logs. The collection of problem solutions is only needed if data comparison results proved there was data that was not able to be extracted using current forensics tools, procedures and methodologies. In order to collect data for problem solutions, firstly research will be undertaken to examine what methodologies, tools and procedures need to be taken to obtain the missing evidence. When the possible solutions are found, action research will be used to test these possible solutions, so that problem solving data can be collected.

### **3.2.2 Data Processing**

Collected data needs to be made into useable information, as only informative and well presented data is useful for research. This is called data processing.

Experimental case scenarios will be established with literary support, based on the data collected during the data collection period. These established case scenarios have to be able to be simulated with the available tools and equipment.

The control data will need to be processed in such a way that it is ready to use as a baseline to compare against the extraction logs. Depending on the scenario, varying types of data will be generated and will be processed differently. Only the available and most suitable methods will be chosen. Based on the literature reviews and advice given by experts, control data will be processed as a written summary to indentify the types of data needed in order to complete the investigation.

Extraction logs, generated by both software and hardware, include both logical and physical extraction data. Depending upon the case scenario and the best available tools and methodologies, the complete logical and physical image of the Smartphone memory and SIM (if applicable) will first be extracted. Based

on the tools used to extract the data, different evidence formatting may be produced for the logical extraction image. The physical image will be stored in a dd format.

A journal will be recorded throughout each investigation process. Each step taken to acquire evidence from the Smartphone during the investigation processes will be documented in detail. The problems encountered during the experiments will also be recorded in the journal.

Comparison data will be processed using control data as a baseline while looking for the data needed in the extraction logs. A keyword search may be applied. Based on the comparison result, if any data is not found in the extraction log, new plans will be formed based on the literature conduct to the nature of the data required. Different methodologies of existing forensics field are evaluated. The tools and methodologies will be selected from the five case studies reviewed in section 3.4, if applicable.

### **3.2.3 Data Analysis**

Data analysis will mainly take place in phase two and three of the research model. During phase two, extraction logs will be analysed and compared to the data listed in the control data collection. Data from the mobile flash memory, SIM, and removable memory will be analysed using different tools, depending on the experimental case scenario. The tools used for analysis of the data will be selected, depending upon the nature of the evidence, and the availability and capability of the tools.

The form of data analysis chosen will depend upon the methodologies used to solve the problem. Extraction logs produced by the chosen tool will be analysed to determine whether the missing data can be found using current mobile forensics investigation tools, procedures and methodologies.

In phase three, the research aim will be answered by analysing the data produced in phase two. Differences between the control data and experimental data will be identified and the reasons why these differences exist will be examined. At the same time the problems of the current forensics approach will be



identified. Any failure to obtain data by the current mobile forensics investigation tools, methodologies and procedures in the first action research iteration will be analysed in relation to Cloud computing.

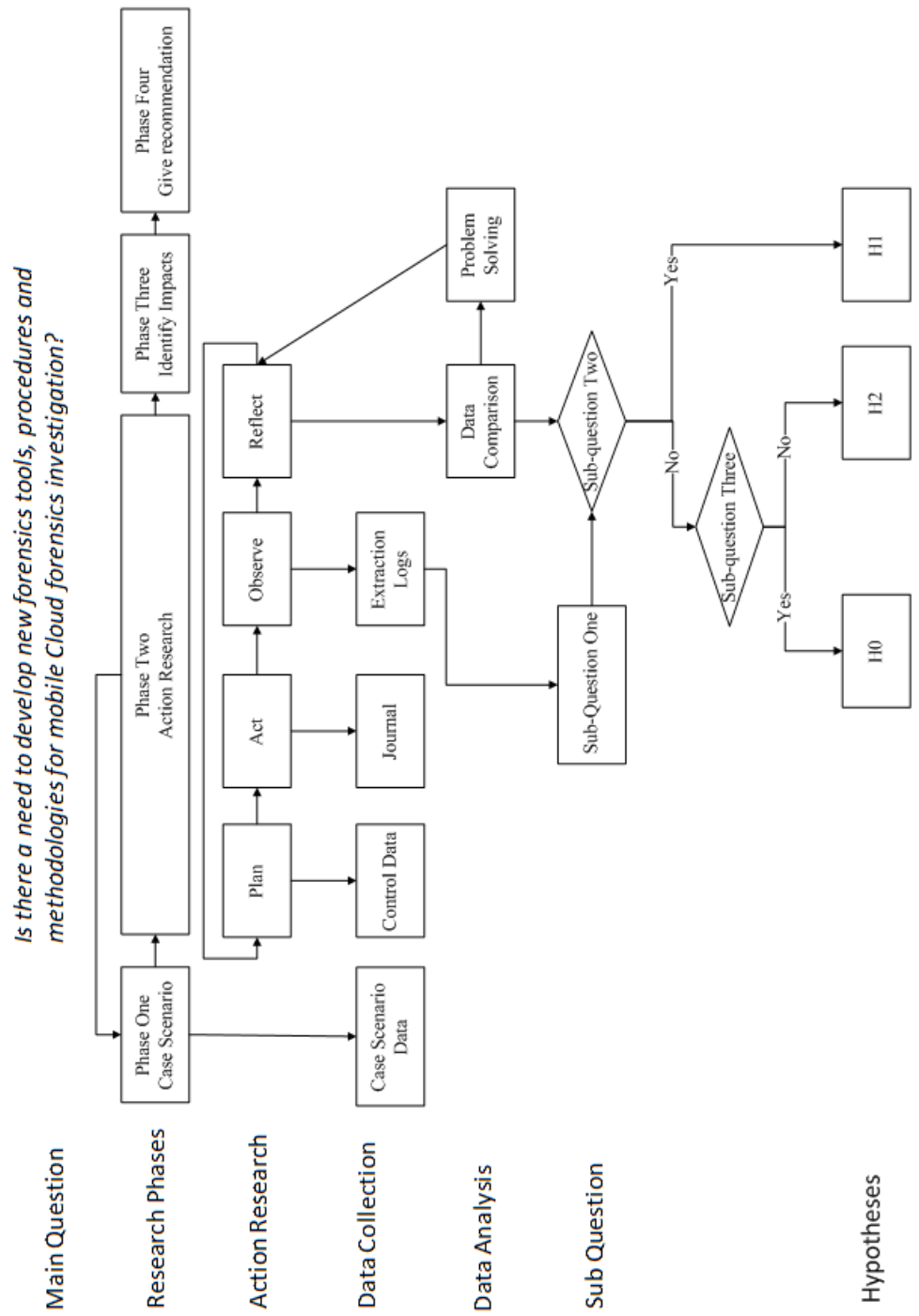
#### **3.2.4 Data Presentation**

Scenario data will be presented in story form. The investigation aim will first be defined, and the story of what really happened will be documented. A simulation of the case scenario will be based on the document, to ensure it is correctly simulated. Control data will be easily obtained from this process. The control data will then be presented in a table form containing all the evidence needed to complete the investigation.

The journal will record all the tools, methods and procedures used to conduct the procedure. The NIST standard mobile forensics guideline will serve as a baseline along with the flow charts surveyed in chapter two. The journal will be broken down into four parts, with each part recording each forensics investigation domain. The procedures will be presented in a table form and the action taken for each procedure will also be recorded in the next column of the table.

Extraction logs will be generated in a report form, being generated by user or by the extracting tool used. The generated reports will include all the data retrieved from the acquisition and examination phases of the investigation process, as happened in phase two, stages two to four.

The comparison data will be documented and compared in a table form. If the evidence listed in the control data table is found in the extraction log, then the evidence will be labelled as found and also backed up with the evidence. For the undetected data the table will be labelled as not found. The data problem solving now takes place. The extraction logs obtained from the observation stage will be analysed to determine whether the required evidence is obtainable by using the proposed tools, methodologies and procedure.



**Figure 3.4: Data Map**

### **3.3 EXPERIMENTAL CASE SENARIOS**

In this section, phase one of the research model is conducted. Three case scenarios regarding what have happened and what could potentially happen in mobile Cloud forensics investigation cases are established here with literature support. The three chosen scenarios cover the main Cloud computing facilitation, including Cloud computing application, Cloud storage and how Cloud computing is used for misconduct. The first case scenario is about how a virus, facilitated from Cloud computing, has already caused huge economic damage and is only the beginning of a growing trend. The second case scenario is about how terrorists could utilise the mobile Cloud in a criminal activity, and the last case scenario is built based on workplace misconduct, and how a Smartphone could be used in facilitating industrial espionage.

#### **3.3.1 Third Party Virus Application Investigation**

Virus integrated Cloud mobile applications are the one of the most frequently used terminal to spread the virus. For example, a recent android mobile virus called Geinimi spread within China, infecting over 150 million mobiles and causing damage to the economy estimated at US\$300,000 dollars a day, or 2 million Yuan (Chinese RMB). The malicious codes were integrated with third party game applications such as *Monkey Jump 2*, *President vs. Aliens*, *City Defence*, and *Baseball Superstars 2010*. When android mobile users downloaded any of these applications and installed them on their mobiles, the virus code ran automatically in the background without the mobile users noticing. The virus creator could then take control of the mobile. Geinimi virus invades the user's privacy, propagating advertisements and downloading malicious software. Once the mobile is infected, information including contacts, SMS messages, SIM card information, the current location of the phone and other private information are sent to a destination appointed by the hacker. This appointed destination can either be a server or a mobile. Geinimi virus had the potential to form botnets very easily, in accord with the ways that viruses are spread. The infected mobile would send 10 or more SMS messages to the people on the contact list without the mobile user's acknowledgement. The content of the SMS messages could be either

advertisements or URL links. If the mobile user on the contact list received the SMS message, opened it, and then clicked into the link, then that mobile became infected also. The new infected mobile repeated the process, getting even more mobiles infected. If one mobile sends out 10 SMS messages, then ten mobiles are very likely to be infected, and then those mobiles each send out another 10 SMS messages, then 100 mobile will be infected. With such a pattern, a huge botnet is formed. The infected mobiles connected to the website Geinimi.com at five minute intervals, to download other malicious applications automatically.

Based on the information drawn from the Geinimi virus news articles, the following case scenario for investigation was established. Alice installed a mobile Cloud based game application in her Motorola Milestone Android Smartphone. After that, she found her mobile credits drained out very quickly, even though she had not made many phone calls or sent any text messages. Suspecting the mobile is infected by a virus, Alice took her Smartphone to the AUT (Auckland University of Technology) forensics lab, wanting to know what was causing this fast draining of mobile credits. If the mobile was really infected by a virus, she wanted to know how the mobile became infected and who the virus distributor was.

### **3.3.2 Terrorists Utilise Mobile Cloud in a Criminal Act**

Cyberterrorism can be defined as the “premeditated, methodological, and ideologically motivated dissemination of information, facilitation of communication, or attack against digital information, computer systems, and/or computer programs” (Britz, 2008, p. 155). Cyberterrorism requires a great deal of planning which aims to cause “social, financial, physical, or psychological harm to non-combatant targets and audiences” (Britz, 2008, p. 155). Terrorist organizations have used the internet in a variety of ways over the past decade, which include:

- Propaganda
- Information dissemination
- Recruiting
- Fundraising

- Training
- Communication
- Research and planning
- Criminal activities
- Money laundering
- Attack mechanisms.

The internet can be utilised to gain knowledge and critical information of military deployments, satellite information, engineering schematics, or online tutorials of how to make a bomb. For example, the British Army Intelligence discovered printouts from Google Earth in the possession of insurgents, who were using them to pinpoint attacks (Britz, 2008). When French authorities arrested Kaci Warab, they discovered that he had been trained in sophisticated detonation devices at Abu Musab al Zarqawi's camp. One of the designs uncovered involved the use of Web-capable cell phones which could be remotely activated via a Web Site. Mobile Cloud opens up more facilities than those which were already available for terrorists. Mobile Cloud storage applications such as Dropbox, and mobile communication applications such as Skype can potentially benefit cyber criminals in their criminal activities. Dropbox applications are installed on a group of terrorists' mobiles. Once a file is uploaded or updated, all of the phones will update themselves instantly; such action keeps everyone in the terrorists group updated very quickly. For example, if an attack plan was changed, and some of the people were out of reach by phone, then file sharing and synchronisation would be the best way to get people updated. Instead of making phone calls and taking risks of being monitored and exposing their current location, communication via Skype would be a much more convenient and cheaper option. Internet calling can be made anyway, at anytime and it is relatively harder to trace. Apart from getting a decoder from Skype, it is almost impossible to monitor a Skype call conversation, due to the strong encryption applied.

The second case scenario was established based on a cyberterrorism model. Terrorist group A launched an attack to the local government house in Country C. There were five people in group A, each with an iPhone 3G. Group members shared the same Dropbox account and instructions to the group members from the

group leader are stored in the Dropbox in confidential folder. Only Skype and Viber calls and texting were permitted. One of the terrorists named Henry got arrested on suspicion of being one of the members of group A and the Police needed evidence to prosecute him. The iPhone 3G was seized as important evidence and transported to the forensics lab for investigation. The purpose of the iPhone 3G investigation was to find evidence to charge Henry, and possibly locate the other four terrorists of group A.

### **3.3.3 Workplace Misconduct - Dropbox Incident**

The typical Cloud storage application Dropbox can potentially be a very convenient tool for distributing information.

Storyline: John Smith, one of the employees from company A was promised a promotion, but a newcomer to the company was promoted instead. He aims to leave and go to their rival company B in the near future. However, before he goes he wants to take revenge. He has helped in the development of an important new technology and his plan is to give the top secret file to their rival company. Thus company A will lose huge amounts of income by not being the leader in the race to develop this new technology. Plus, this will help improve his salary negotiating with the rival company when he changes companies. (Company B has been head hunting John Smith for a while already.) Company A has received a tipoff and so has undertaken an internal investigation.

Interviews are firstly conducted within the team members who had access to the files and projects. The manger Lily Ann, during her interview points out that John has been behaving in an unusual manner and that his attitude has changed. The company seized John Smith's computer and his iPhone 4 as it's the company's property as well. E-mails belonging to John are also seized with the result showing John sent a suspect file to his work E-mail. However, there is no sign of him sending it to the rival company. The phone is transferred to the lab for a forensics investigation to be conducted. What John had done was, he sent this suspect file to his work E-mail. He then accessed the E-mail from his iPhone 4, downloaded the file and stored it in Dropbox. He then sent the file to the manger

of the rival company via E-mail. The question is, can they find the evidence to charge John with from the Smartphone?

### **3.4 REVIEW OF SIMILAR CASE STUDIES**

Five studies were reviewed in this section to observe the many different approaches and tools in acquiring and analyzing data from mobile devices and their related sources. The first study targeted acquiring data from a mobile's internal memory, using a designed software tool which dumps the data from flash memory onto the external memory. Android forensics was chosen as the second study in this paper, and how to acquire and analyse physical and logical data from an android OS. The third study introduced techniques used to perform investigations on third party applications installed on an iPhone. The fourth study utilised the network for another approach in acquiring data from a mobile device. The last study comes from the first FBI Cloud investigation and the approaches taken to solve the case. These five studies were chosen because the methodologies and techniques introduced potentially help in the carrying out of an investigation in a mobile Cloud Computing environment.

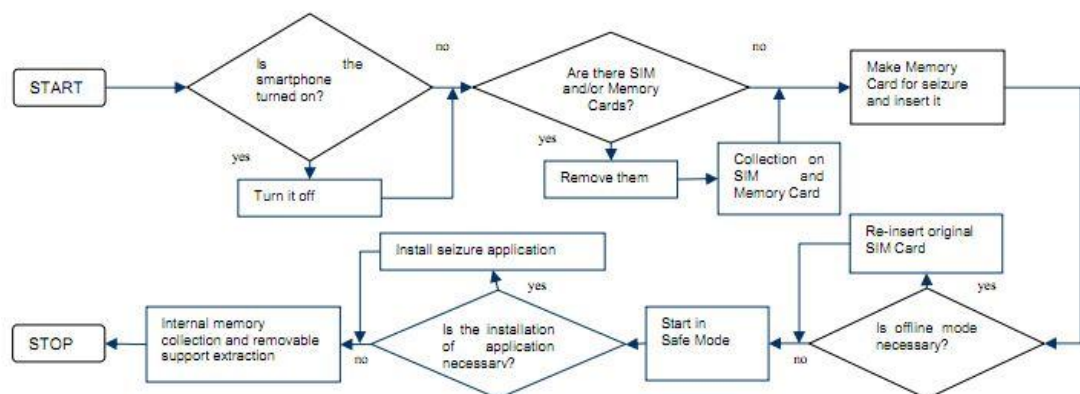
#### **3.4.1 Internal Forensic Acquisition for Mobile Equipment**

In this first study, Me and Rossi (2008) proposed an alternative methodological approach for acquiring data from a mobile's internal flash memory. The methodology involved using a software tool designed by Me and Rossi (2008) to acquire a physical copy of the internal memory of a mobile phone running a Symbian OS and to store the acquired data in a removable storage, such as a memory card. This paper summarized current mobile internal memory acquisition, and the problems of applying existing seizure methodology to a mobile device. The proposed methodology proved capable of overcoming some of the problems faced by the traditional methodology.

The proposed data collection workflow is shown in Figure 3.3 below. Using the proposed software tools built-in API (Application Programming Interface), data can be extracted from the flash memory in a read only mode. Such an approach makes the acquisition process more forensically sound. In order to

perform the data acquisition, the device needs to be turned off. After performing data acquisition from both the SIM and Memory cards, insert a new memory card. A seizer application can be installed, depending on the situation and the types of phone, and this application will allow direct execution without physically being installed on the device. Now the internal memory can be physically copied onto the memory card, and the memory card can then be physically removed for data analysis to be performed. However, this methodology has limitations. The software tool has been specifically designed for different versions of Symbian OS. For other mobile OS, such as Android and iPhone OS, a different software tool needs to be developed in order to conduct extraction.

This article is relevant because current forensics data analysis methodologies are less forensically sound due to the connection and interaction needed during data exaction procedures. The proposed alternative data extraction method of internal flash memory acquisition potentially makes for a more sound form of mobile forensics investigation.



**Figure 3.4: Data Collection Workflow (Me & Rossi, 2008, p. 2)**

### 3.4.2 Android Forensics

In the second study, *Android Forensics: Simplifying Cell Phone Examinations* by Lessard and Kessler (2010), the methods of conducting android mobile forensics investigation are listed. Both physical and logical extractions are made and tested, and the pros and cons for each extraction are made. In their first section, the architecture of the Android operating system was analysed, as the importance of understanding the system is necessary in order to be able locate data for retrieval.



The majority of the data that could be of interest in a forensic investigation will be found in the libraries, particularly the SQLite databases. Files can be stored on either the device's storage or on the removable secure digital (SD) card. Android Runtime System utilises the Dalvik virtual machine (VM), which allows multiple applications to be run concurrently, as each application is its own separate VM.

Lessard and Kessler (2010), in the second section of their article, used the AccessData FTK Imager v2.5.1 to perform a physical extraction of the memory card and made a forensic copy. In order to make a physical image of the entire phone memory, rather than a logical image of the partition, rooting was needed. "Rooting a device merely means to gain access to the root directory (/) and having the appropriate permissions to take root actions" (Lessard & Kessler, 2010, p. 3). However, gaining root access is often not forensically sound, as it usually requires installing an application. Once root permissions are gained, a dd image of the memory can be created and made ready for examination. The ways to root an Android device and the methods of creating a dd image of memory are also explained in this article. AccessData's Forensic Tool Kit (FTK) v1.81 was used for the data analysis.

In the third section, logical examination and analysis were described in detail. A logical dd image was generated first, and Cellbrite was used for analysis. Both the logical and physical examinations required root access. However, the logical image presented data in a more easily viewable way but could not find all the deleted SMS messages, phone records, and contact information. Physical extraction located all the deleted data, including text messages and contacts, but required long hours of data analysis.

The extracting and analysing data methodologies for android phones are relevant because android is the second biggest player in the use of mobile Cloud applications. Understanding how to extract and analyse information in a forensically sound manner is essential for mobile device examiners. The pros and cons outlined in each different examination help mobile device examiners decide which type of examination should be utilised, based on each particular case scenario.

### **3.4.3 Third party Application Acquisition**

The article by Levinson et al. (2011) proposes techniques that can perform forensics investigations on an Apple mobile device third party application. The type of evidence that can be retrieved from the evidence files in the iPhone flash memory and how to read them are introduced in this paper. Third party applications are useful in forensics investigation as they can contain forensically rich data. However, commercially available forensics tools only interpret typical mobile telephone data on Apple mobile devices. Levinson et al. (2011) found that commercial tools have not yet been developed to extract relevant data from all third party applications, but are slowly providing access to the information stored by a select number of third-party application providers; an example being Skype applications and WiFi connections from which Oxygen can access information.

In the methodology section of this article, data partitions on iPhones were being carefully analysed. An iPhone has two partitions; one being the System partition which contains all executables and the other being the User Data partition containing configuration information for the operating system and all the applications (Levinson et al., 2011). In this article the files inside the User Data partition have been identified. Third party application data lies under the private directory. Third party applications are often stored in different locations due to the fact that there is no standard for data storage. These third party applications are executed within a sandbox environment, which is built upon virtualization technology. Such an approach prevents any application from directly interacting with any other applications or their stored data. These applications include built-in phone applications, such as generating an E-mail. An analysis based on a real case study was performed. Using the proposed forensics techniques, a rich forensic timeline was built based on the data generated from third party applications on the seized iPhone.

This study was chosen because of the rich forensics data third party applications contain and that most third party applications developed for iPhones use Cloud computing technology. Making use of the extracted information from third party applications is one of the most important tasks in mobile Cloud forensics.

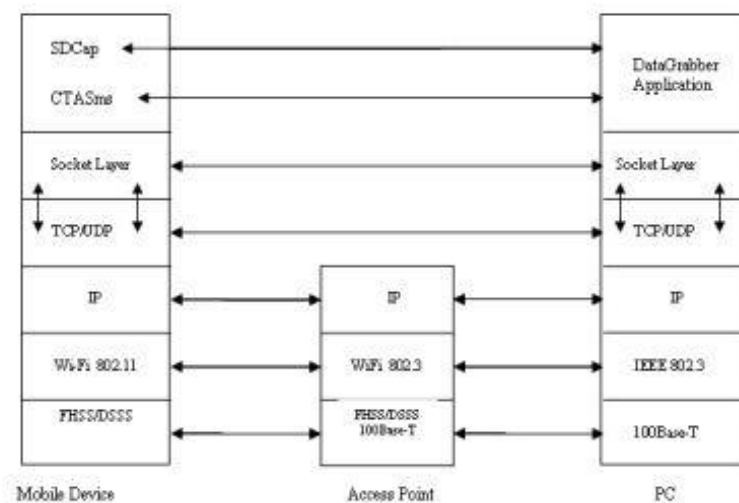
### **3.4.4 Forensic Information Acquisition in Mobile Networks**

The article proposed by Irwin and Hunt (2009) addressed new methods in data acquisition from Windows mobiles over wireless networks. Three software applications: DataGrabber, CTASms and SDCap were designed and developed especially to enable data extraction from mobile internal and external memory over a wireless network to a remote desktop computer. In this article, the experiment was successfully demonstrated using the proposed methods and software applications in copying folders and files.

The three software applications were designed for different purposes. DataGrabber is the main application designed to run alongside the desktop computer. The purpose of creating such an application is that while transmitting folders and files from the mobile device, physical connection of the mobile device to the computer is not required. The most important feature of DataGrabber is the wireless interface. This enables folders and files captured by the Storage Device Capture (SDCap) software, to be transmitted on an external storage card in the mobile device to the DataGrabber software application installed on a remote computer, through a WiFi connection. SDCap software needs to be installed on the mobile device and is designed to capture all information stored on the mobile device's removable media, such as the SD card. The CTASms (Contacts, Tasks, Appointments and SMS) needs to be installed on the mobile device to enable a search of the mobile device pocket outlook session. The retrieval of contacts, tasks and appointments from the personal information manager (PIM) and the storage of this information as XML files on the mobile device can then be undertaken. The information can then be extracted and manipulated by DataGrabber.

A mobile device has the ability to transmit information using the TCP or UDP transport protocol by WiFi (IEEE802.11a/b/g), which assigns the mobile device an IP address. The protocol stack is shown in Figure 3.4 for the forensics information acquisition of the mobile device over a wireless network. This article is relevant because of its extracting data over networks. Extraction without physical connection to the computer makes investigation more forensically sound. Possible ways to extract data via the 3G network by applying the proposed

methods are theoretically doable through an access point which supports lower layer UMTS protocols.



**Figure 3.5: Protocol Stack for Forensic Information Acquisition of a Mobile Device in a Wireless Network**

### 3.4.5 Cloud Computing Forensics

Poulsen (2010) in a news article, outlined an investigation case carried out by the FBI on a criminal spammer involving a Cloud computing scenario. The case was also the first publicly acknowledged search warrant of a suspect whose reliance was on Cloud computing. The warrant was issued on August 21 in the Western Districts of New York. Pulse Marketing Ltd was suspected of launching a deceptive E-mail campaign for a diet supplement called Acai Pure. According to a summary from the court records, the warrant demanded all Google apps, contents and E-mails belonging to Beers and de Diego. Google was issued the warrant, and provided the required files in 10 days. The FBI got two spreadsheets from Beers' account, one of them titled *Pulse\_weekly\_Report Q-3 2008*, which showed the firm had spammed 3,082,097 E-mail addresses, and another spreadsheet *Yahoo\_Hotmail\_G-mail – IDs*, listed 8,000 Yahoo webmail accounts.

Cloud is undoubtedly making investigation easier for the FBI. If the spammers kept their files on their local hard drive, the FBI agents would have to draw their guns, bang on the door and serve the warrants in person. This would be followed by seizure of the computers, leaving the suspects with a copy of the search warrant and a written inventory of everything taken. In contrast, the search

warrant was issued to Google Docs under seal, so the suspects had no knowledge of their files being seized and presented in court. The government was under no obligation to disclose the Cloud search to Beers and de Diego, because no criminal charges had been filed.

This news article was chosen because it addressed the very first criminal investigation in a Cloud computing scenario. The article provides proof that a physical acquisition is not needed in a Cloud computing investigation and after a warrant is issued, that data can be seized without the suspects knowledge from their Cloud service provider.

### **3.5 LIMITATIONS OF THE RESEARCH**

The research aims for this thesis are to indentify the impact of Cloud computing on the tools, procedures and methodologies of mobile forensics investigation and to give mobile Cloud forensics investigation recommendations. The main research question determines whether there is a need to develop new forensics tools, procedures and methodologies.

Due to mobile Cloud computing being still in its infancy, there are not many real case studies available for use. Only one case scenario is derived from a real case study. The other two case scenarios were constructed, based on information from the literature reviews and from potential future problems offered by mobile Cloud computing.

Different Smartphones are used in different scenarios and, for the best results different Smartphones need different tools to perform the acquisition and analysis. Tools will be selected based on their availability and capabilities. Budget constraints will limit the tools that can be used to conduct experiments on the Smartphone.

The experiment involves making a request to gathering data from the mobile service providers. Due to the nature of this data, and its unavailability to be open to public request, the accessing of this data may not be granted.

### **3.6 CONCLUSION**

Chapter three delivers the definition of the research experiments for this thesis project. The research questions and hypotheses are established based on the literature reviewed in chapter two. The research questions were derived to test the existing mobile forensics tools, methodologies and procedures, and then to identify the impact of Cloud computing on mobile Cloud computing investigation. To ensure the research purpose was fulfilled, action research was used to build the research model. The research model was then designed to provide logical progression of the testing phases to be conducted, thus achieving the research aims of identifying the impact of Cloud computing on the tools, procedures and methodologies of mobile forensics in an efficient manner. Furthermore, the proposed requirements of how data was to be collected, processed, analysed and presented are detailed and discussed. In order to conduct the experiments, three mobile Cloud forensic investigation experimental case scenarios were introduced, with literary support.

To better develop suitable methodologies to conduct the experiments, five reviews of similar case studies that were involved in Cloud computing technology were chosen based on the contents of the case scenarios set up in section 3.3. Use of appropriate methodologies in each stage of the data collection helped to produce an accurate outcome. Furthermore, the limitations of this research project were identified. As mobile Cloud computing is still in its early development, there are not many cases on mobile Cloud computing that are publicly available. Thus two of the case scenarios were made up from future potential problems. Resources and budgets available for the research were a constraint, so tools used to conduct the experiments were limited. The last constraint identified was the possibility of a limit in the gathering of data from the mobile network carriers, if that data was required.

## **Chapter 4**

### **RESEARCH FINDINGS AND ANALYSIS**

#### **4.0 INTRODUCTION**

Chapter three formulated the research plan. The research questions and hypotheses were also proposed and a research model was designed to conduct the experiments so that the research aim could be fulfilled. Action research was chosen to be the research methodology for this thesis due to its flexibility and purpose of learning and evaluating throughout the experimenting phase. The three experimental case scenarios were formed in chapter three to conduct experiments. Furthermore, expected outcomes were discussed, as well as the identifying of potential limitations of this research.

In this chapter, the findings from the experimenting phases (action research) proposed in chapter three will be reported in detail. Section 4.1 will present the first experimental case, which is an android third party application virus case scenario. In section 4.2, the second experimental case scenario will be performed on an iPhone 3G Smartphone, followed by the third experimental case scenario in section 4.3. These will be implemented first and then examined using the current NIST standard mobile forensics tools, procedures and methodologies. Data will be collected, processed and evaluated as discussed in chapter three in the data requirements section. The research findings will also be displayed in picture and table form. In the evaluation section, the data not meeting the research outcome will be taken into consideration and the finding of possible solutions to extract the missing data will be sought. For publication purposes, some of the data shown in the figures has been blacked out or changed for privacy protection.

#### **4.1 EXPERIMENTAL CASE SCENARIO ONE**

Alice installed a mobile Cloud based game application iLightr on her Android Motorola Milestone Smartphone. She then found her mobile credits drained out

very quickly, even though she had not made many phone calls or sent any text messages. Alice, suspecting that her mobile had become infected by a virus, took it to the AUT forensics lab.

The aims of the investigation were: to identify the reason for the quick loss of mobile credits, to identify if the mobile was really infected by a virus, and to trace the virus' origin.

#### **4.1.1 Stage One - Case Scenario Implementation**

A journal of the steps taken in the case simulation was documented in this section to ensure the experiment was simulated correctly.

##### **4.1.1.1 Pre-case simulation processing**

#### **Android mobile device**

In Table 4.1 the technical specification of the Motorola Milestone Smartphone is shown, as well as the SIM card used.

**Table 4.1: Android Device Specification**

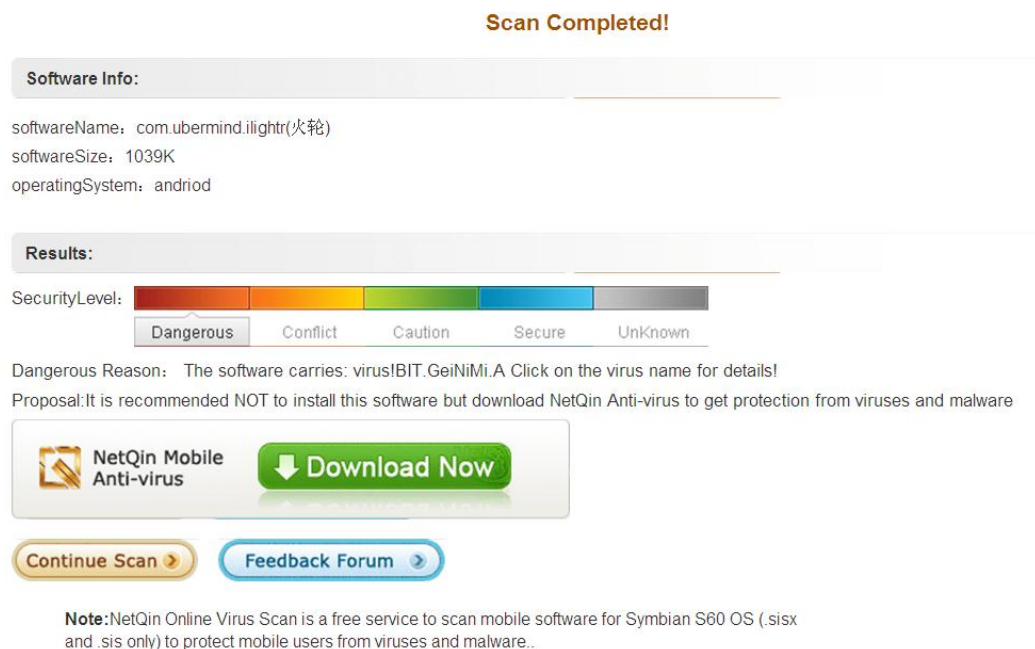
<b>Mobile device</b>	Motorola Milestone
<b>Operating system</b>	Android 2.0
<b>Processor Speed</b>	550 MHz
<b>SIM Card</b>	Vodafone Prepay 3G 128k
<b>Removable Memory</b>	8GB micro SD
<b>Networks</b>	3G WCDMA/900/2100 GSM 850/900/1800/1900 HSPA GPRS Class 12 WiFi Bluetooth

#### **GeiNiMi virus**

An android mobile game application, **iLighttr v1.0.2** was downloaded from a Chinese mobile game application website <http://www.yruan.com/softdetail/739>.



Using a web mobile antivirus scan via NetQin (<http://scan.netqin.com/en/>) a Geinimi virus BIT.GeNiMi.A was detected and identified. Figure 4.1 shows the result of the online virus scan. According to NetQin (2011c), the BIT.GeNiMi.A was found on 26th of November 2010 and was classified into three different virus category types: Fee Consuming, Privacy Stealing, and Backdoor making. The virus description shown on the NetQin (2011d) website as BIT.GeNiMi.A was disguised as a game to lure users to download it. Once activated, the virus connected to the internet in the background by a plug-in, and leaked the user's private data, and downloaded software without the user being aware. All this malicious performance not only incurred fees to the user, but also exposed them to further security threats (NetQin, 2011d).



**Figure 4.1: Online Virus Scan Result**

In order to conduct a fair experiment, the Motorola Milestone was formatted and restored to its manufactured status. This ensured there were no other factors affecting the mobile's normal operation. When the Smartphone was rebooted, the device was connected to a WIFI network locally called ThomsonAD82BB. In order to install the virus application, Mobile Assistance 911 application was downloaded and installed on the Smartphone. The Fire Bola game application (lightre) was then installed on the Smartphone by double clicking on the game

application. After installing, the game application was launched to ensure the virus was executed.

#### **4.1.1.2 Expected Outcome**

- Forensics tools used are able to extract data stored in the Milestone Smartphone especially text messages, internet browsing history and web activities.
- Ability to detect if the cause of the quick draining mobile credits is due to a virus infection, as Alice suspects.
- Ability to identify the virus' capability.

#### **4.1.2 Act - Apply Forensic Procedures and Methodologies**

The act stage will implement the current forensic tools, procedures and methodologies to the case scenario one based on the action research principles. The procedures taken and action performed will be recorded in the table's format.

##### **4.1.2.1 Preservation**

Forensics investigation procedures and methodologies were adopted from NIST standard publications, or well recognized publications which were introduced and outlined in the literature reviewed in chapter two. The preservation procedures and action are recorded in the Table 4.2 below.

**Table 4.2: Motorola Milestone Preservation Procedures and Actions**

<b>Preservation Procedures</b>	<b>Action</b>
1. Secure and evaluate the scene.	In this scenario, the phone was transported to the forensics lab. Thus, securing and evaluating the scene are not applicable.
2. Document the entire scene.	N/A
3. Is there a need for other forensic analysis (DNA etc)?	N/A
4. If possible try and identify the model and make of the phone.	The device was identified as a Motorola Milestone.
5. Is the phone switched on or switched off.	The device was switched on.

<b>Preservation Procedures</b>	<b>Action</b>
6. Take all measures to not interrupt the power supply and isolate the phone from radio signals.	The phone was preserved in a shielded container away from radio signals.
7. Secure the phone with all accessories.	The phone was secured and only authorized personal had access to it.
8. Follow strict procedures for documentation packaging, transportation and storage.	The phone was well packaged and safely transported to the forensics lab.

#### **4.1.2.2 Acquisition**

The acquisition methods used on the Motorola Millstone Smartphone are described and discussed in this section. NIST standard acquisition procedure was followed and Table 4.3 below shows the acquisition procedures and action taken in following the procedures.

**Table 4.3: Motorola Milestone Acquisition Procedures and Actions**

<b>Acquisition Procedures</b>	<b>Action</b>
1. Identify device.	Device was identified as a Motorola Milestone.
2. Is the phone switched on or off?	The phone was switched on.
2.1 Take all measures not to interrupt the power supply. Isolate the phone from radio signals.	The phone showed a full bar of battery and the phone was turned to Airplane mode.
2.2 Look up the phone capabilities and download the manual.	The Motorola Milestone manual was downloaded from the internet.
2.3 Select the phone and forensic tools and plan the examination and analysis.	Commercial tools: XRY and Oxygen Forensics Suite 2010. Open source tool: Nandroid
2.4 Test the tool on an identical phone before using it on the phone under investigation.	Tests were performed on an identical milestone Smartphone and the results showed only XRY could successfully extract evidence from the Smartphone. Nandroid was the only physical extraction method available, but this method required gaining root access, which means the evidence may be corrupted.
3. Is it an unobstructed or obstructed phone?	Unobstructed device.

4. Mobile phone acquisition.	The phone acquisition was performed and is documented shown in the following section.
------------------------------	---

XRY was chosen to conduct the examination, because the results from performing an examination on an identical phone showed the inability of Oxygen to perform an extraction on the Milestone Smartphone, as the OxyAgent failed to install on the phone and an error message was shown: *Cannot find the phone; connection failed*. The same error occurred after several attempts. In order to use Oxygen to extract data from a Smartphone, OxyAgent must first be installed. Even though XRY offers physical extraction of a Smartphone, XRY does not support physical extraction of a Milestone. However, XRY can be successfully managed to extract a logical copy of the phone. Thus physical extraction would only be performed if the data needed for the investigation could not be obtained from a logical copy. The reason being, that only a Nandroid can successfully perform a physical extraction from an android phone. In order to perform, a Nandroid requires root access, which means evidence is highly likely to have been altered.

#### 4.1.2.3 Examination

The collection of extraction logs and comparison data in this section will follow NIST investigation procedures and is shown in Table 4.4.

**Table 4.4: Motorola Milestone Examination Procedures and Actions.**

Examination procedures	Action
1. Identify potential evidence.	SMS, web browsing history, files downloaded from the internet, applications, anything that can consume bandwidth and money.
2. Collect and analyse evidence from call and subscriber records.	Only authorised personal, such as select government agencies have the privilege of accessing such sensitive data.
3. Analyse evidence extracted from the mobile handset.	The evidence extracted from the mobile handset was analysed. (The details of the extracted evidence analysis are listed below).

The types of data that are of interest for analysis in this investigation are those that generate potential money consuming activities. These data types include:

- Call logs
- SMS
- Web browsing history
- Applications, including third party applications

XRY only supports some extraction features on a Motorola Milestone phone and unfortunately E-mail and applications data extraction are not supported, as displayed in Figure 4.2. The Smartphone was successfully extracted by XRY version 5.2 and the extracted information was stored in extraction logs.

The logical extraction performed by XRY version 5.2 showed 20 entries of SMS, 0 pictures, 1 video, 8 documents, 5 files and 67 logs which were created during the extraction processed by XRY. As expected there were no records in regards to information on applications and E-mails. The detailed extraction log is shown in appendix A.

## **Motorola Milestone**

Network	GSM
OS	Android

### **Logical**

#### **Connectivity**

Cable	✓	microUSB Cable
Bluetooth	✗	Not Supported
Infrared	—	Not Available

#### **Features**

Contacts Sim	✗	Not Supported
Calls Sim	✗	Not Supported
SMS Sim	✓	Full Support
Contacts	✗	Not Supported
Calls	✓	Full Support
SMS	✓	Full Support
Pictures	✓	Full Support
Audio	✓	Full Support
Video	✓	Full Support
Files	✓	Full Support
MMS	✗	Not Supported
E-mail	✗	Not Supported
Calendar	✗	Not Supported
Tasks	—	Not Available
Notes	—	Not Available
Memory card	✓	Full Support



**Figure 4.2: XRY Features for Motorola Milestone**

A detailed analysis of the SMS messages was performed. The entire 20 SMS were retrieved from the phone, including the SMS stored in the SIM card. There were

no SMS messages sent from the phone. Thus, there are two possible assumptions. The first is that the virus deleted the SMS messages right after sending them. The other assumption is that the virus was not designed to send any SMS messages. To confirming which assumption was correct required obtaining a detailed report from the mobile service provider. There were no entries in the call logs either. The calling and texting history can be obtained from the phone carrier. If Alice examines the list, and recognizes all the phone calls made and there are no additional ones, then it indicates that her money was not consumed by the making of phone calls or from texting. However, the evidence needed to answer the investigation questions was not fully obtained by the extraction process. Table 4.5 shows the evidence that should be obtained and the evidence that was obtained using current mobile forensics tools, procedures and methodologies.

**Table 4.5: Evidence comparison table A**

<b>Evidence Required</b>	<b>Evidence Found</b>
Text messages	Yes
Call logs	Yes
Internet browsing history	Yes
Web activities	No
Is the phone infected by a virus?	No
What the virus does	No

To obtain the missing evidence, physical extraction was performed to see whether there was more data that could be retrieved. Rooting was performed in order to gain full access to the phone systems and files, for full extraction of the data from the mobile's physical memory. Rooting to get the superuser access was successfully performed using a tool developed from a hacker community called G.O.T Team Android, which is available on their web site (<http://groupoften.wordpress.com/g-o-t-s-openrecovery/>). The documented rooting procedures are listed in appendix B.

The G.O.T Team Andorid application offered options, such as that of creating a Nandroid backup. A Nandroid backup was created using the option from the menu, but whether the created Nandroid backup file was a bit to bit

image of the entire phone memory or just the image of the allocated partitions of the phone was undefined.

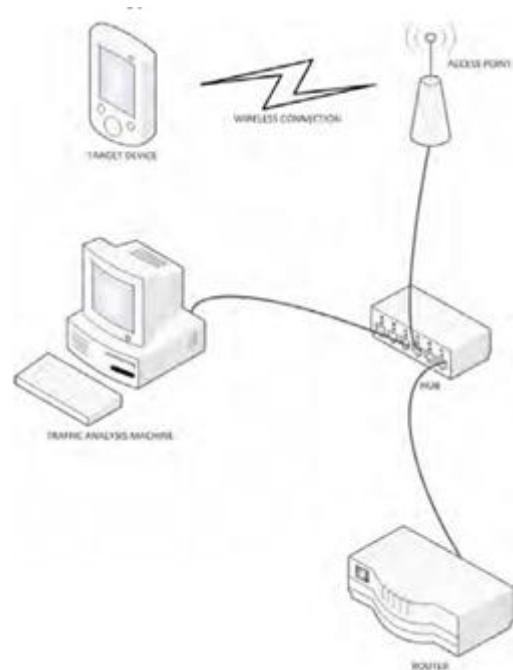
The Nandroid backup files were stored in the SD card and were located in the ADBRecovery folder. There were 7 files, including 6 .img files contained in the ADBRecovery folder. These files were: boot.img, bpsw.img, cache.img, cust.img, data.img, misc.img and MD5.txt. To examine these images, FTK was used and data carving was performed. Unfortunately, none of the files were recovered or picked up by FTK through the data carving processes. Thus there was no additional data obtained through physical extraction in this case.

A logical extraction is made after the phone is being rooted and can be found in appendix C. After successfully gaining access right to the root, there were still 20 entries of SMS, 2 pictures, 1 video, 9 document, 112 files and 207 logs.

From examination of the evidence, there were more files found on the rooted phone than the unrooted phone. There was significant growth in files and logs. (The files that exist in a jailbreak phone are files from the installation folder placed there during the rooting process.) The files were identified as those contained in both the update.zip and the open recovery folder. Many more files were added to the original evidence by using G.O.T to gain access to the phone root. This action therefore could not be counted as being forensically sound. There was no additional evidence found beyond that already found.

#### **4.1.2.4 Using other forensics methodologies to obtain missing evidence**

If the credits were not consumed via SMS or phone calls, then there was a good possibility of internet usage. Capturing the internet traffic was one way to determine what data had been sent and received. Network forensics should be used to help understand the network usage of the phone. For real time traffic capturing, Wireshark could be used to capture sent and received packets from the phone. The experiment is pictured in Figure 4.3.



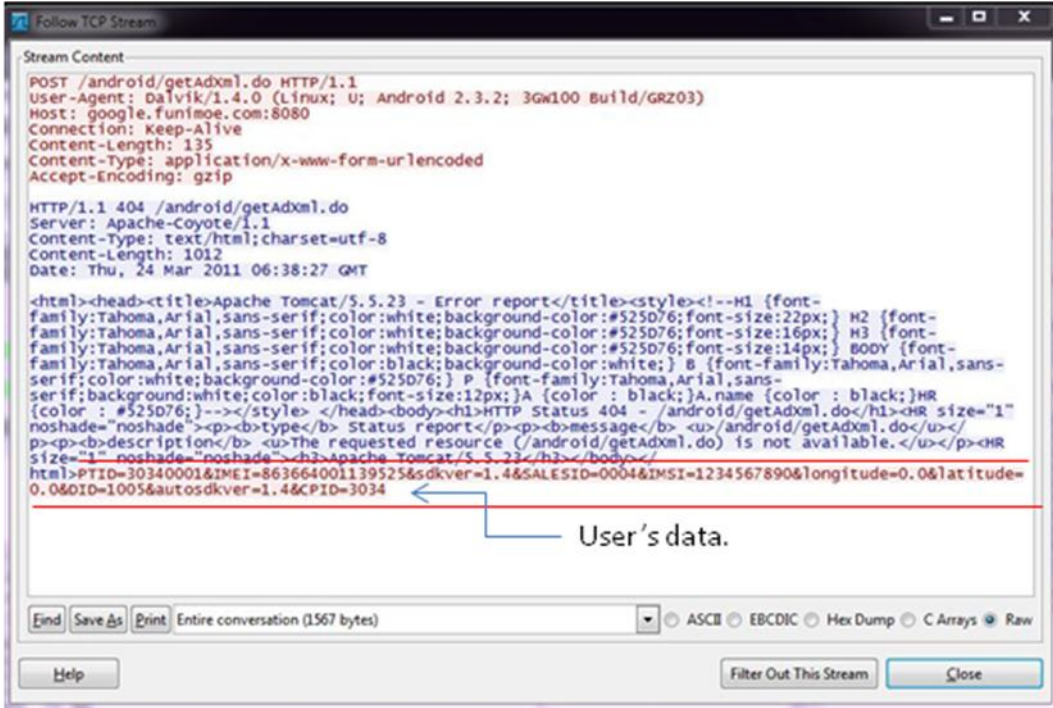
**Figure 4.3: Wireless Traffic Capture Set Up (Morrill, 2010, p. 337).**

In order to capture the incoming and outgoing traffic, an access point, router and a computer to run Wireshark were needed. The data that Wireshark captured demonstrated that the mobile was trying to connect to a `google.funimoe.com:8080` host at IP `202.106.0.20`, to enable the sending of the encrypted data. This data contained the user's private information, such as the device identifiers (IMEI) and location co-ordinates. Figure 4.4 shows a TCP stream of the device sending the encrypted data (`PTID=30340001&IMEI=863664001139525&sdkver=1.4&SALESID=0004&IMSI=1234567890&longitude=0.0&latitude=0.0&DID=1005&autosdkver=1.4&CPID=3034`) to a remote Apache-Coyote server.

Even though Wireshark captured the data, the application that endeavoured to send all the data to the remote server, and in which the virus was hiding, remained unknown. One approach to identify the application was to disable all the other applications on the phone. This would prevent them from running and then allow each application to be tested one at a time. Another approach was to use an anti-virus scanner to detect the virus.



To scan the mobile, NetQin Mobile Anti-virus was chosen. The anti-virus application was then downloaded from NetQin and installed. An anti-virus scan was performed and the scanned result showed the application 轮火iLightr (containing the BIT.GeNiMi.GEN virus).



**Figure 4.4: TCP Stream Captured by Wireshark Showing that The User’s Data is Transferred.**

Using Wireless forensics investigation methods, web activities can be identified by capturing the packets. This methodology confirmed the phone was infected by a virus and was sending the private information of phone to a remote server, thus using up the internet bandwidth. All the evidence needed for this investigation was gathered and shown in the Table 4.6.

**Table 4.6: Evidence Comparison Table B**

Evidence Required	Evidence Found
Text messages	Yes
Call logs	Yes
Internet browsing history	Yes
Web activities	Yes
Is the phone infected by a virus?	Yes
What the virus does	Yes

## **4.2 EXPERIMENTAL CASE SENARIO TWO**

A terrorist group launched an attack on a local government house in Country C. Group members shared the same Dropbox account, and instruction to the group members from the group leader were stored in their Dropbox in a confidential folder. Only Skype, Viber calls and texting were permitted.

Andrew, one of the terrorists, was arrested on suspicion of being a terrorist group member. Police needed evidence to charge him and hopefully to also find the other four terrorist members. Andrew's iPhone 3G was seized and transported to the forensics lab for investigation. The investigation purpose was twofold; to find evidence to charge Andrew and to find useful data that would locate the other four terrorists.

### **4.2.1 Stage one - Case Scenario Implementation**

In this section, the detailed information on the procedures taken to simulate the case scenario is presented.

#### **4.2.1.1 Pre-case simulation processing**

##### **iPhone**

A jail-broken iPhone 3G Smartphone was chosen for the simulation. Table 4.7 shows the technical specifications of the phone and its SIM card.

##### **Application requirements**

- Skype
- Viber
- G-mail
- Dropbox

Skype, G-mail, Viber and Dropbox were installed on the jailbreak iPhone 3G. To ensure there was data to be collected from all applications described above, the existing user account was signed in. Skype calls and Viber calls were made to a few different people and also text messages and conversations with a few contacts in the account list. MobileMe was also set up to protect the data in the phone if the device went missing, when remote wipe could be performed.

**Table 4.7: iPhone Specifications**

<b>Mobile device</b>	iPhone 3G
<b>Operating system</b>	iPhone OS 4
<b>Processor Speed</b>	550 MHz
<b>SIM Card</b>	2 Degrees, 128k
<b>Internal Memory</b>	8GB , 128 MB RAM
<b>Networks</b>	WiFi 802.11b/g
	WCDMA/900/2100
	GSM 850/900/1800/1900
	HSDPA 850 / 1900 / 2100
	GPRS
	EDGE
	Bluetooth

#### **4.2.1.2 Expected Outcome**

- Skype and Viber call logs and text messages would be obtained using the chosen forensics tools and methodologies.
- Data shared in the Dropbox would be extracted.
- E-mails messages would be obtained.
- The WiFi connection location would be obtained that could trace down places the terrorists had been.
- Pictures retrieved which could contain information of where the pictures were taken.

## 4.2.2 Act – Apply Forensics Methodologies and Procedures

### 4.2.2.1 Preservation

**Table 4.8: iPhone Preservation Procedures and Actions.**

Preservation Procedures	Action
1. Secure and evaluate the scene.	The scene was secured. Only authorised personal could access the scene.
2. Document the entire scene.	The scene was documented.
3. Is there a need for other forensic analysis, such as network analysis, or DNA?	Yes, a DNA test was performed to identify the suspect.
4. If possible, try and identify the model and make of the phone.	The device was identified as an iPhone 3G.
5. Is the phone switched on or switched off.	The device was switched off.
6. Secure the phone with all accessories.	The phone was secured and only authorized personal had access to it.
7. Follow strict procedures for documentation packaging, transportation and storage.	The phone was well packaged and was safely transported to the forensics lab.

### 4.2.2.2 Acquisition

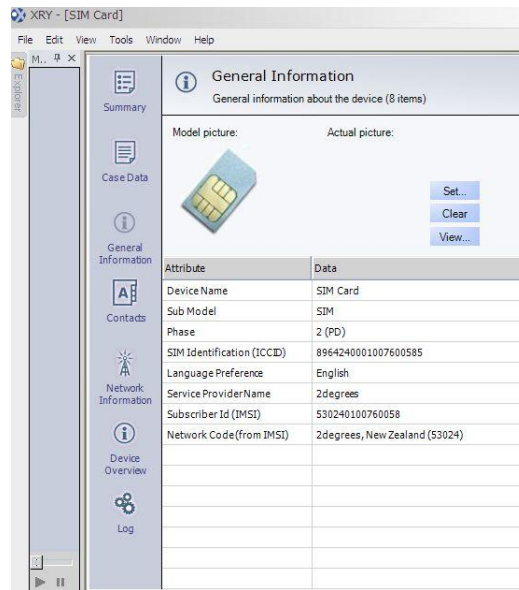
Acquisition procedures and action taken were recorded in Table 4.9 below. Both XRY and Oxygen were chosen to perform the extraction in order to compare the results. Physical extraction was performed using XRYv5.2.

**Table 4.9: iPhone Acquisition Procedures and Actions**

Acquisition Processes	Action
1. Identify device	Device was identified as an iPhone 3G.
2. Is the phone switched on or off?	The phone was switched off.
2.1 First try and remove the SIM card without taking the battery out. If it is not possible to do so remove the SIM and put the battery back in immediately.	The SIM was taken out of the iPhone 3G without removal of the battery.
2.2 Clone the SIM using existing tools.	A bit by bit copy of the SIM card was made using the XRY SIM id-Cloner.
2.3 Read the PIN/PUK status using a forensic tool.	The SIM Card reader bypassed the PIN/PUK number.
2.4 Contact provider to get the PUK/find a way to gain access using a backdoor.	N/A

Acquisition Processes	Action
2.5 Examine the SIM using a forensic tool.	The SIM was examined using XRY.
3. Tool selection and expectation.	XRY and Oxygen. Oxygen could only perform logical acquisition, while XRY supported both physical acquisitions, as the phone was already jail-broke.
4. Is it an unobstructed device or an obstructed device?	An obstructed device.

The XRY SIM id-Cloner system resolved two problem challenges that are currently faced when examining GSM based mobile phones. Cloning the SIM card prevents a GSM network connection, without affecting the normal operation of the device. This helps to minimize the risk of data contamination occurring. Such action can also be of assistance to examiners when no original SIM card is present, helping to gain full access to the operating system and function without any data alteration. Using the XRY SIM id-Cloner system a SIM card clone was made. Under GSM standards a mobile device should delete the call history if a new SIM card has been inserted. However, the cloned SIM card contained the same critical information as the original SIM, which allowed access to the handset without causing the device to delete the call history list. The duplicated SIM card was now inserted back into the iPhone 3G. Extraction was performed on the original SIM card using XRY. The SIM card was then successfully acquired. Figure 4.5 shows the general information about the SIM card and detailed extraction log can be found in appendix D.



**Figure 4.5: SIM Card Information**

#### **4.2.2.2.1 Logical exaction**

Both XRY and Oxygen Forensics Suite 2010 were chosen to conduct the examination, as both tools are sound mobile forensics investigation tools and the user manuals indicate their ability to perform logical extraction on an iPhone 3G.

XRY was used first and successfully extracted the logical data from the iPhone 3G. As shown in Figure 4.6, XRY can extract contacts, calls, SMS, pictures, audio, video, files, E-mail, MMS, calendar, and notes. In addition, XRY can also exact user accounts information for applications installed on the phone, network information and search history, which are logged in the extraction logs.

Oxygen Forensics Suite 2010 was used to perform logical extraction. Oxygen OxyAgent was successfully installed on the handset to extract data from the iPhone 3G. Oxygen was also successful in extracting the logical data from the handset. Oxygen offers a wide range of extraction features for the iPhone 3G, which include device information, phone book, messages, event log, calendar, notes, timeline, applications, web browsers cache analyser, dictionaries, Skype analyser, web connections and location service, which are shown in Figure 4.7.

# Apple iPhone 3G

Network	GSM
OS	iOS



## Logical

### Connectivity

Cable	✓	iPhone Cable 1
Bluetooth	✗	Not Supported
Infrared	—	Not Available

### Features

Contacts Sim	✗	Not Supported
Calls Sim	✗	Not Supported
SMS Sim	✗	Not Supported
Contacts	✓	Full Support
Calls	✓	Full Support
SMS	✓	Full Support
Pictures	✓	Full Support
Audio	✓	Full Support
Video	✓	Full Support
Files	✓	Full Support
MMS	✓	Full Support
E-mail	✓	Full Support
Calendar	✓	Full Support
Tasks	—	Not Available
Notes	✓	Full Support
Memory card	—	Not Available

Figure 4.6 :XRY Features for Apple iPhone 3G

Sections

Search data

Actions

Common sections

**Device Information**  
 Device Information shows additional device parameters and calculated statistic for common sections.

**Phonebook**  
 Phonebook section permits to view contacts with photos, custom field labels, birthdays and speed dials.

**Messages**  
 Messages section allows to view SMS, MMS, E-mail, Beamed and other messages types and their attachments in default and custom folders.

**Event Log**  
 Event Log section stores data about all calls, SMS messages sent and received, GPRS and WiFi sessions of the device owner.

**Calendar**  
 Calendar section allows to analyze meetings, anniversaries, reminders and other types of events.

**Notes**  
 Notes section enables users to examine notes of any length.

**File Browser**  
 File Browser section presents the entire mobile device file system, including photos, videos, voice records, documents, geo files and other important information.

Extras

**Timeline**  
 Timeline section summarizes all phone events in a chronological order.

**Web Connections and Location Services**  
 Web Connections and Location Services section allows to inspect all web connections in one list and shows hot spots on the map.

**Applications**  
 Applications section presents the whole list of pre-installed or custom applications.

**Web Browsers Cache Analyzer**  
 Web Browsers Cache Analyzer displays a list of Internet sites visited and files downloaded by the device owner.

**Dictionaries**  
 Dictionaries section allows to identify words entered by the phone owner while making notes, writing messages, etc.

**Skype Analyzer**  
 Skype Analyzer gives a possibility to examine all the data stored in the Skype Client on the mobile device.

Figure 4.7 - Oxygen Features for Apple iPhone 3G

#### 4.2.2.2.2 Physical exaction

Due to the seized iPhone 3G being already jail-broken, there was no additional work needed to perform a physical extraction. The XRY also provides the capability of extracting a physical image of the iPhone 3G. XRYv5.2 successfully extracted the physical dump from the phone. However, the physical extraction data could not be read by the XRYv5.2 sponsored by XRY. Neither EnCase nor FTK, which are both forensically sound software can not open or analyse the physical dump generated by XRY.

#### 4.2.2.3 Examination

XRY extracted 57 contacts, 100 calls, 2 notes, 578 SMS, 1 MMS, 50 E-mails, 4,844 pictures, 1 video, 52 audios, 9,023 documents, 6,124 files, and 27,636 logs. The logs included: accounts information, application information, network information and the search history. Oxygen extracted 57 contacts, 281 incoming and 288 outgoing messages, 48 answered calls, 41 dialled calls, 11 missed calls, 2 notes, 648 files including 102 images, 3 documents, 33 database files and 510 other files. There were 4,975 web connections and location services, including 7 WiFi connections, 4,942 locations, and 26 IP connections, as well as 41 system applications. Table 4.10 shows a comparison table of data extracted from these two forensically sound software.

**Table 4.10: Comparison of Data Extraction by XRY and Oxygen.**

	<b>XRY</b>	<b>Oxygen</b>
<b>Contacts</b>	57	57
<b>Calls</b>	100	100
<b>Notes</b>	2	2
<b>SMS</b>	578	569
<b>MMS</b>	1	N/A
<b>E-mail</b>	50	N/A
<b>Pictures</b>	4844	102
<b>Videos</b>	1	N/A
<b>Audio</b>	52	N/A
<b>Documents</b>	9023	3



	<b>XRY</b>	<b>Oxygen</b>
<b>Files</b>	6124	510
<b>Log</b>	27636	-
<b>Applications</b>	undefined	41
<b>WiFi Connections</b>	undefined	7 locations
<b>Locations</b>	undefined	4942
<b>IP connections</b>	undefined	26
<b>Key words</b>	715	715

Most pictures extracted are system generated pictures from different applications installed on the iPhone. There are five pictures that are identified as taken by Andrew. The GPS information embedded in the photo taken by the iPhone camera was able to locate where the picture were taken, thus leading to where the suspects had been. Photos were exported to Google earth, and use Google map is also sued to locate the exact location of these photos. Table 4.11 has shown the table overview of the photo names, GPS co-ordinates, location and the real picture.

**Table 4.11: Photos and Corresponding Location Overview**















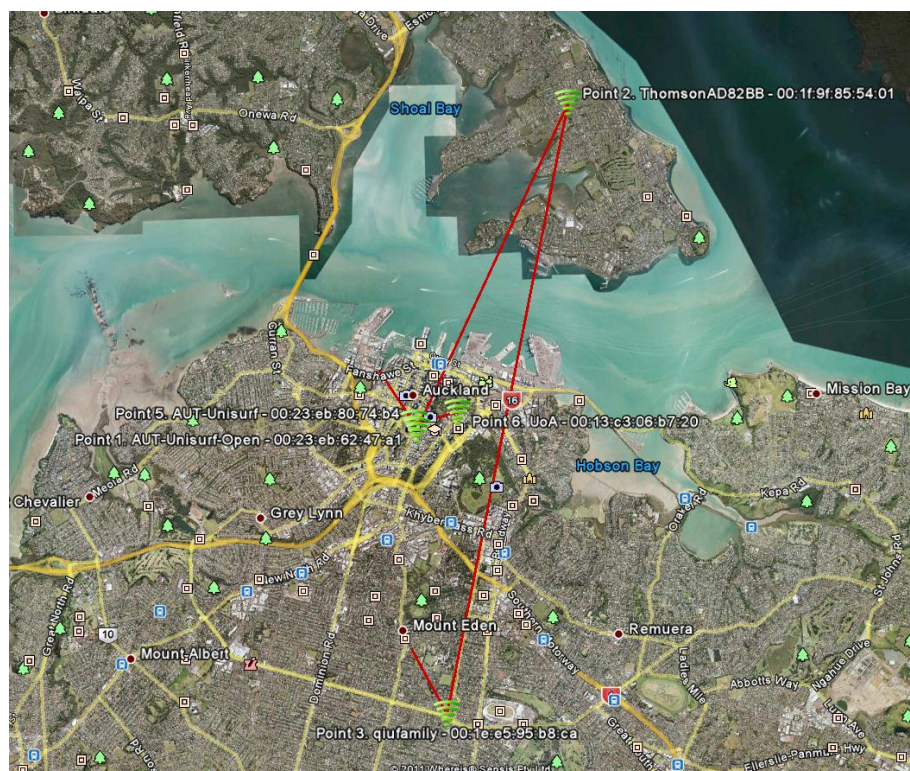
<b>Photo Name</b>	<b>GPS Co-ordinates</b>	<b>Location</b>	<b>Picture</b>
IMG_0115.JPG	-33.854800000°, 151.226000000°	Fort Denison, Sydney Australia	
IMG_0087.JPG	-33.867800000°, 151.216000000°	1 Art Gallery Rd, Sydney NSW 2000	
IMG_0030.JPG	-33.875300000°, 151.107000000°	18-36 Victoria Street E, Burwood, NSW, 2134	
IMG_0137.JPG	-33.858500000°, 151.211000000°	The rocks, Sydney, Australia	

Photo Name	GPS Co-ordinates	Location	Picture
IMG_0052.JPG	-33.426800000°, 151.341000000°	96 Donnison Street, Gosford New South Wales, Australia	

The WiFi connection logs were also extracted to locate the places where the suspects had been. Figure 4.8 shows the WiFi connections and the places where they were connected. The details of the WiFi connections, along with their locations are shown on the Google Maps attached in appendix G. Oxygen offers a function allowing these WiFi connections to be exported to Google Earth files. Thus, the locations where the WiFi was connected can be virtualized. The Google earth image of all connected accessed points is presented in Figure 4.9.

WiFi connections		IP connections		Locations (consolidated.db)			
		SSID	BSSID	Last joined time (...)	Last auto joined time (...)	Geo coordinates	A... Address
<input checked="" type="checkbox"/>		TP-LINK_660660	00:25:86:66:06:50	7/04/2011 12:52:05 AM	10/04/2011 11:10:39 AM	N/A	N/A N/A
<input checked="" type="checkbox"/>		UoA	00:13:c3:06:b7:20	29/03/2011 3:10:28 AM	30/03/2011 3:30:39 AM	S 36.8507928, E 174.7709154	51.0 New Zealand, Auckland, Symonds St, 44
<input checked="" type="checkbox"/>		AUT-Unisurf	00:23:eb:80:74:b4	13/03/2011 11:25:54 PM	1/04/2011 7:29:50 AM	S 36.8522517, E 174.76363	49.0 New Zealand, Auckland, Auckland Central, Queen St, 303
<input checked="" type="checkbox"/>		iptime	00:08:9f:b2:22:10	1/03/2011 1:29:54 AM	4/04/2011 8:25:08 PM	N 37.3845511, E 126.64261...	51.0 South Korea, Incheon, Songdo-dong, 8-20
<input checked="" type="checkbox"/>		qufamily	00:1e:e5:95:b8:ca	21/10/2010 9:02:24 AM	24/10/2010 7:44:04 AM	S 36.8915013, E 174.7691274	73.0 New Zealand, Auckland, Epsom, Wilding Ave, 17
<input checked="" type="checkbox"/>		ThomsonAD82BB	00:1f:9f:85:54:01	1/01/2000 3:41:39 AM	26/04/2011 12:36:28 PM	S 36.8089118, E 174.7896277	73.0 New Zealand, Auckland, Belmont, Bayswater Ave, 187
<input checked="" type="checkbox"/>		AUT-Unisurf-Open	00:23:eb:62:47:a1	1/01/2000 12:06:29 AM	13/03/2011 11:22:04 PM	S 36.8532236, E 174.7639751	73.0 New Zealand, Auckland, Auckland Central, Airedale St, 2

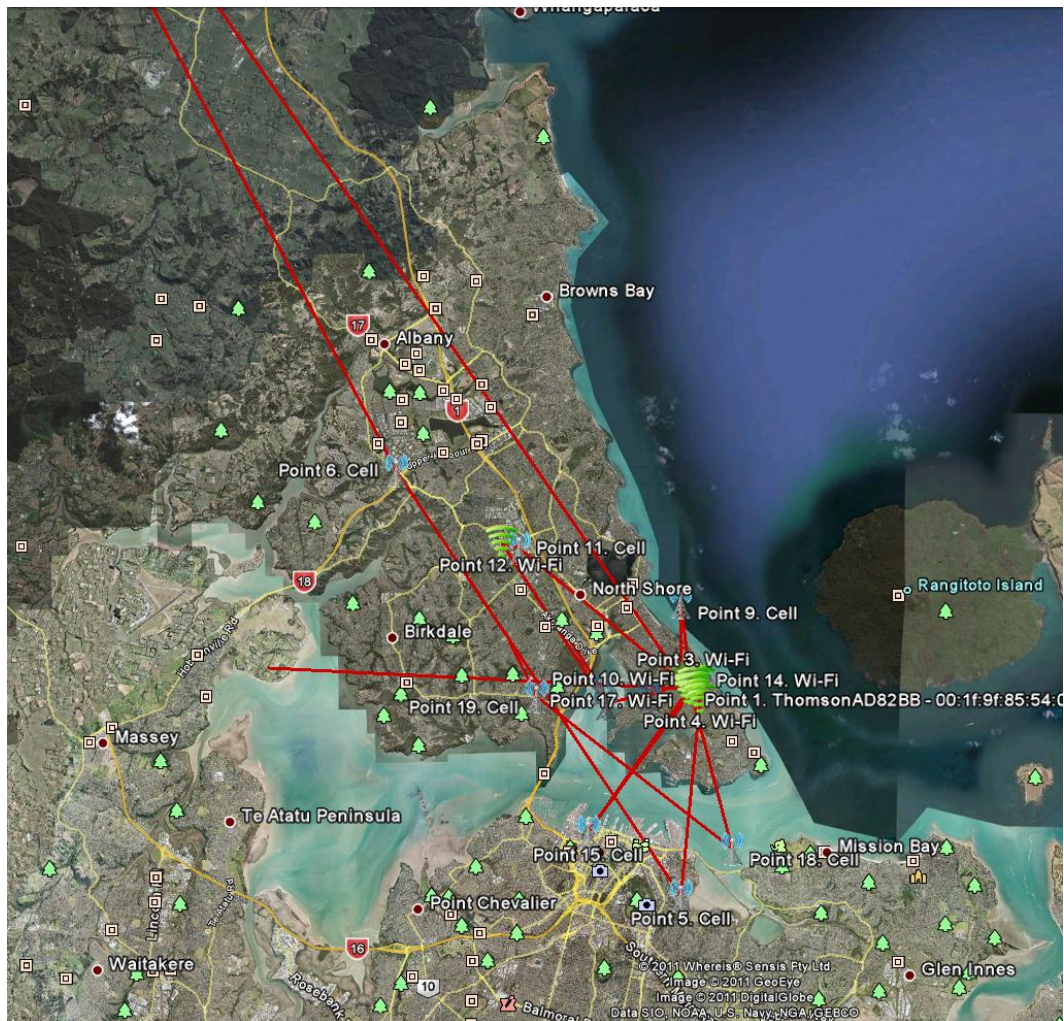
**Figure 4.8: WiFi Connections**



**Figure 4.9: Locations Where Andrew Connected to the Wireless Network.**




Where Andrew has been is also pictured on the location information for the iPhone. These points then were exported to Google earth. These locations contain both the location where the phone was connected to the WiFi and the locations where the phone detected an access point and asked if Andrew wanted to connect to that access point. By use of Google Maps, Figure 4.10 shows the places where Andrew has been.




**Figure 4.10: Locations Where Andrew Has Been**

Oxygen developed the Skype Analyser especially to extract information from Skype. The Skype Analyser can extract account contacts and signed in account information, including the user's photo, account name, display name, language, country, E-mail address, account balance, time zone, chat messages and counts, call counts and MD5 hash. An example of the account information displayed by the Skype Analyser is shown in Figure 4.11 below.

Accounts		
Andrew(andrew_fly)		
Account name	andrew_fly	
Display name	Andrew	
Language (ISO)	en	
Country (ISO)	nz	
Email	Andrew	@gmail.com
Balance	0 EUR	
Time zone	+12:00	
ChatMessages Count	9	
Calls Count	1	
MD5 Hash	e47ddb14d410f04d4a021f8b6a70aade	

**Figure 4.11: Skype Account Information**

The Skype Analyser extracted five account contacts. The information details of these extracted contacts are dependent on what was entered by each account contact. Figure 4.12 shows an example of an account contact.

Accounts		
Andrew(andrew_fly)		
Account name	andrew_fly	
Display name	Andrew	
Language (ISO)	en	
Country (ISO)	nz	
Email	Andrew	@gmail.com
Balance	0 EUR	
Time zone	+12:00	
ChatMessages Count	9	
Calls Count	1	
MD5 Hash	e47ddb14d410f04d4a021f8b6a70aade	

**Figure 4.12: Skype Account Contact Information.**

Chat messages between account owner and account contacts are also extracted along with the time stamp, message kind and the MD5 hashes. Figure 4.13 shows an example of a chat message.

Figure 4.14 show the account call information retrieved using the Skype Analyser. The Skype Analyser indicates that one call was made from Andrew to Louis at 1:23:37 PM on 26/04/2011 for 5 minutes and 6 seconds.

Remote party	Louis_run
Direction	Incoming
Time stamp	26/04/2011 1:23:34 PM
Message kind	Private message
MD5 Hash	4a01ab7d1841ac671b2ae8ae98b9d3f1
Yea, pretty good ay	
Remote party	Louis_run
Direction	Outgoing
Time stamp	26/04/2011 1:24:03 PM
Message kind	Private message
MD5 Hash	3b56a25d9ae86901f3110b0a7dc629b5
Lol	

Figure 4.13: Skype Chatting History

Account calls Andrew_fly	
Remote party	Louis_run
Duration	00:05:06
Call type	Skype call
Call direction	Outgoing call
Is missed	No
Cost	0
Time stamp	26/04/2011 1:23:37 PM
Response time stamp	26/04/2011
Online number	
MD5 Hash	68e396688f33eb2cd824e7881b76e572

Figure 4.14: Skype Account Calls

XRY extracted 73files and 306 documents from the Skype application. Callmember256.dbb shows the user made a phone call to a contact called Louis shown in Figure 4.15.

callmember256.dbb	
00000000	6C 33 33 6C 64 00 00 00 1F 00 00 00 41 0D 00 09 1331d
00000010	0D 03 98 07 6D 69 72 61 6E 64 61 6E 33 33 00 03 Andrew_fly
00000020	9C 07 4D 69 72 61 6E 64 61 20 5A 68 61 6E 67 00 Andrew
00000030	00 B1 07 02 00 B5 07 06 03 B8 01 31 2D 31 33 30 1-130
00000040	33 38 32 34 32 31 37 00 03 E0 19 00 00 07 1E 00 3824217
00000050	81 1A D9 8E DB ED 04 00 D1 22 00 00 D5 22 01 00
00000060	E5 19 E5 8E DB ED 04 00 A5 07 B3 02

Figure 4.15: Skype Call Contact Extracted by XRY.

Using SkypeLogView to read both chatmsg256.dbb and callmember256.dbb files extracted by XRY, the 8 chat messages and 1 outgoing call recorded are shown in Figure 4.16.

In user 4096.dbb, user1024.dbb, user512.dbb and user256.dbb files, 5 contacts information were extracted. In Figure 4.17, the heightened name is the contact name and heightened number is their mobile number, if the account user chose to fill it in as part of their user profile.



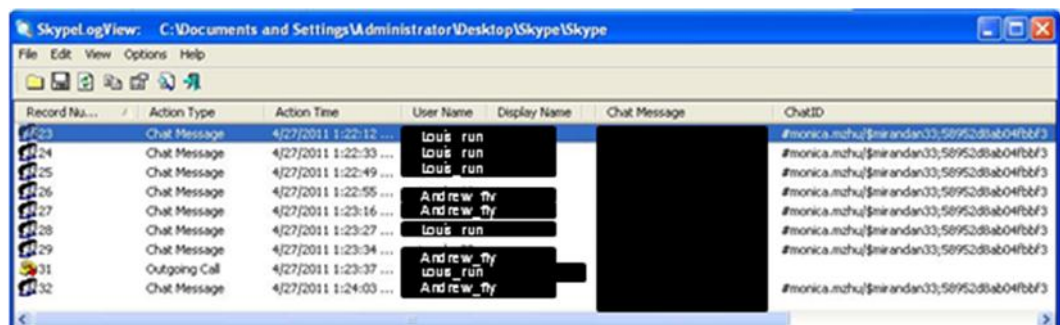


Figure 4.16: Messages Read by SkypeLogView.

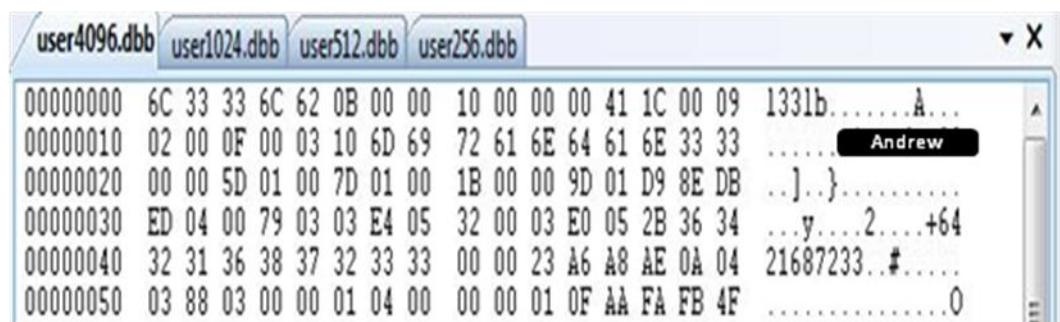


Figure 4.17: Skype Account Contact Information.

## Viber

Oxygen extracted three files from Viber, being: Contacts.data, Contacts~.data and settings. The Viber contacts and calling information could not be understood as the data was shown in a raw format. A sample is displayed in Figure 4.18.

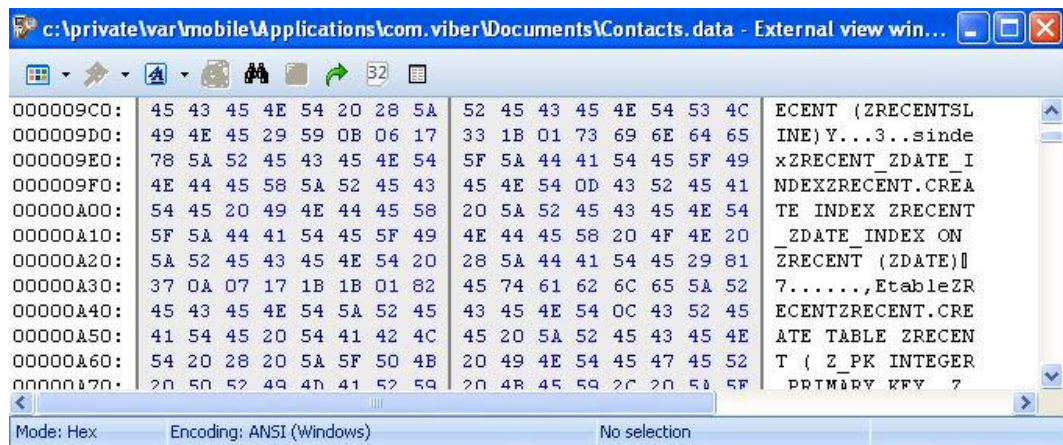


Figure 4.18: Viber Contacts Data

XRY extracted 35 documents and 20 files from Viber. However, the files were displayed in the same raw data unreadable form just like Oxygen, and are displayed in Figure 4.18 above.

## Dropbox:

As shown in Figure 4.19 Oxygen displayed the application information and status, such as the Dropbox user being andrew@hotmail.com. The files stored in this application however, were irretrievable.

Key	Type	Value
AnalyticsLastUploaded	Date	4/26/2011 12:59:55 PM
defaultsAccountInfoKey	Data	Hex: 0x62 0x70 0x6C 0x69 0x73 0x74 0x30 0x30 0xD4 0x01 0x02 0x03 0x04 0x05 0x08 0x3F 0...
Dropbox Username	String	Andrew@hotmail.com
DropboxBrowseState	Data	Hex: 0x62 0x70 0x6C 0x69 0x73 0x74 0x30 0x30 0xD4 0x01 0x02 0x03 0x04 0x05 0x08 0x34 0...
kDBDropboxSavedCred...	Dictionary	3 Key/values pairs
WebKitLocalStorageData...	String	/var/mobile/Applications/F5EA7BD8-7258-48A9-B2F1-DF52DE69D734/Library/WebKit/LocalStorage
WebKitOfflineWebApplicati...	Boolean	True
[save] Dropbox Show Tour	Boolean	True

**Figure 4.19: Dropbox Application Information**

XRY extracted 28 documents and 23 files. Again, none of the extracted documents or files was in human readable form. No information regarding the number of files was downloaded, uploaded or read inside the Dropbox folder, as shown in Table 4.12. The comparison data is shown in Table 4.13 where missing evidence required for completing the investigation is identified.

**Table 4.12: Comparison Table of Data Extraction from Third Party Application by XRY and Oxygen**

	XRY	Oxygen
Skype	Found 5 contacts, 9 chat messages and 1 calling record.	Found 5 contacts, 9 chat messages and 1 account calls.
Viber	Keyword search is performed. 35 documents and 20 files are extracted. However, by reviewing the extracted files, none of them gave the information regarding the phone calling and MSM messages.	Unknown. The data was in the hex format.
Mail	XRY exacted 50 E-mails which had been viewed on the phone.	Oxygen did not support E-mail acquisition.
Dropbox	Extracted 28 documents and 23 files. No information regarding files stored in the application, where uploaded.	Only application information and status were shown. Files stored in the Dropbox were irretrievable.

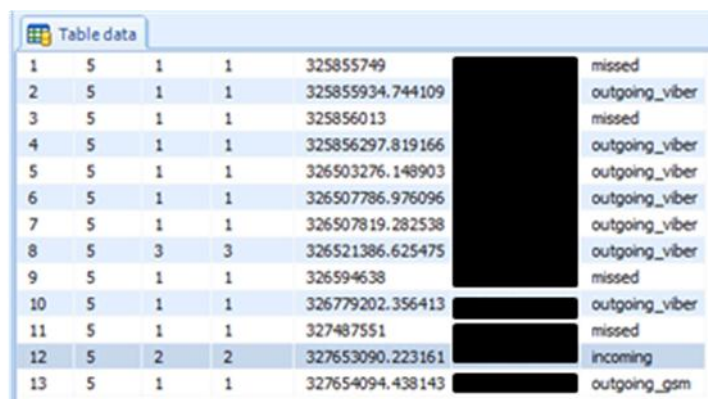
**Table 4.13: Evidence Required and Evidence Found Comparison Table A.**

Evidence Required	Evidence Found
Skype chatting logs and call logs	Yes
Viber chatting logs and call logs	No
G-mail	Yes

Evidence Required	Evidence Found
Files stored in Dropbox	No
WiFi connection	Yes
Picture	Yes

Files stored in the Dropbox are still not able to be extracted. The Dropbox service provider would be able to provide those files, if they have not already been overwritten. Viber chatting logs and calling logs can not be obtained from either Oxygen or XRY with the tools used. However a later version, XRYv5.5 offers the capability of extracting Viber chatting logs and call logs. From examining the *Contacts.data* file, the following information was gathered:

- There are 74 contacts in the Viber account.
- The account received 1 incoming call, 4 missed calls, 7 outgoing Viber calls and 1 outgoing GSM call. Figure 4.20 below shows the phone calls made on Viber.
- Chat messages between contacts and the contacts list were also recorded in the *Contacts.data.SQLite* file.



1	5	1	1	325855749	missed
2	5	1	1	325855934.744109	outgoing_viber
3	5	1	1	325856013	missed
4	5	1	1	325856297.819166	outgoing_viber
5	5	1	1	326503276.148903	outgoing_viber
6	5	1	1	326507786.976096	outgoing_viber
7	5	1	1	326507819.282538	outgoing_viber
8	5	3	3	326521386.625475	outgoing_viber
9	5	1	1	326594638	missed
10	5	1	1	326779202.356413	outgoing_viber
11	5	1	1	327487551	missed
12	5	2	2	327653090.223161	incoming
13	5	1	1	327654094.438143	outgoing_gsm

**Figure 4.20: Viber Call History**

Table 4.14 displays the final comparison data. All the evidence required for the investigation was seized, apart from the files stored in the Dropbox.



**Table 4.14: Evidence Required and Evidence Found Comparison Table B.**

<b>Evidence Required</b>	<b>Evidence Found</b>
Skype chatting logs and call logs	Yes
Viber chatting logs and call logs	Yes
G-mail	Yes
Files stored in Dropbox	N/A
WiFi connection	Yes
Picture	Yes

### **4.3 EXPERIMENTAL CASE SENARIO THREE**

John Smith is an employee of company A. Company A suspects him of taking important project information and giving it to their rivals, company B. John Smith's laptop and mobile phone have been seized. An investigation is under-way to examine John's case to establish whether he is guilty or not.

#### **4.3.1 Stage one – Experimental Case Scenario Implementation**

The case study was simulated exactly as it was documented, and the journal of steps taken appears later in this section.

##### **4.3.1.1 Pre-case simulation processing**

##### **iPhone 4 Smartphone**

**Table 4.15 – iPhone 4 Technical Specifications**

<b>Mobile device</b>	iPhone 4
<b>Operating system</b>	iPhone OS 4
<b>SIM Card</b>	Vodafone
<b>Internal Memory</b>	16GB
<b>Networks</b>	GSM model: UMTS/HSDPA/HSUPA (850, 900, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz) WiFi 802.11b/g
<b>Networks</b>	CDMA model: CDMA EV-DO Rev. A (800, 1900 MHz) Bluetooth 2.1 + EDR wireless technology

**Software:**

- Dropbox
- E-mail
- iBook
- Third party applications

John Smith scanned the confidential document and E-mailed it to his work E-mail. He then opened the E-mail on his iPhone and downloaded the attached file. He then uploaded the file to Dropbox. John then used the Dropbox to send the file via E-mail to Monica who works for a rival company.

**4.3.1.2 Expected Outcome**

- Be able to trace down the E-mail sent to the work file.
- Be able to find the file uploaded to Dropbox.
- Be able to trace down the E-mail sent by the iPhone.

**4.3.2 Act – Apply Proposed Forensics Methodologies and Procedures****4.3.2.1 Preservation**

The iPhone 4 was preserved and delivered to the company's forensic lab to perform the investigation and collect the evidence.

**Table 4.16: Preservation Procedures and Actions Taken**

<b>Preservation Procedures</b>	<b>Action</b>
1. Secure and evaluate the scene.	The device was handed over by the company, thus no scene was involved.
2. Document the entire scene.	N/A
3. Is there a need for other forensic analysis (DNA etc)?	N/A
4. If possible try and identify the model and make of the phone.	The device was identified as a iPhone 4.
5. Is the phone switched on or switched off.	The device was switched on.
6. Take all measures to not interrupt the power supply and isolate the phone from radio signals.	The phone was preserved in a shielded container away from radio signals.

Preservation Procedures	Action
7. Secure the phone with all accessories.	The phone was secured and only authorized personal had access to it.
8. Follow strict procedures for documentation packaging, transportation and storage.	The phone was well packaged and safely transported to the forensics lab.

#### 4.3.2.2 Acquisition

Acquisition procedures and action taken to forensically image followed NIST standard guidelines and is documented below as shown in Table 4.17.

**Table 4.17: Acquisition Procedures and Actions.**

Acquisition procedures	Actions
1. Identify the device.	The device was identified as an iPhone 4.
2. Is the phone switched on?	The phone was on.
When the phone is switched on:	
i. Make sure the phone has a high enough battery level. Isolate the phone from radio signals and all possible connections, including: WiFi, Bluetooth and infra-red.	The phone was already turned to airplane mode and stored in a radio isolated bag.
ii. Look up the phone capabilities and download the manual.	The iPhone 4 manual was downloaded and studied.
iii. Select the forensic tools. Plan the examination and analysis.	Oxygen Forensics Suite, XRY and iPhone Backup Extractor were selected.
iv. Test the tools on an identical phone before using it on the seized phone.	The tools were tested on an identical phone which demonstrated that the data could be extracted off the phone successfully.
3. Is it an obstructed or an unobstructed phone?	Obstructed
Investigation methods:	
1) Ask the suspect for the password.	The correct password was supplied by John.
2) Review the seized material.	N/A
3) Manually supply commonly used password input.	N/A
4) Ask the service provider for the password.	N/A

Acquisition procedures	Actions
5) Exploit possibly insecure settings.	N/A
4. Tool selection and expectation in examining evidence types below:	
a. Mobile phone.	XRY
b. SIM.	N/A
c. External physical storage.	N/A

#### 4.3.2.3 Examination

As E-mail was the most important evidence to this investigation, XRY was chosen to examine John Smith's iPhone. Oxygen does not support E-mail extraction, thus it was not chosen to conduct an examination for this case scenario. XRY extracted 824 contacts which also included Facebook contacts, 232 calls, 16 calendar records, 3 notes, 227 pictures, 217 SMS, 176 audio, 310 documents and 492 files.

Both logical and physical extraction can be performed by XRY. However physical extraction could not be performed, nor could the e-mails be extracted as the seized iPhone4 was not jail-broken. In addition, XRY does not support physical extraction of the iPhone4 (A1332) model according to the XRY manual. In John Smith's iPhone4, the entire file storing and document reading applications were analysed; these being Dropbox and iBook.

In reviewing the plist file, *com.getdropbox.Dropbox.plist*, the following information was gathered: The Dropbox account was [johnsmith2011@gmail.com](mailto:johnsmith2011@gmail.com). Under DropboxDocOffset-/Work folder, a pdf file was viewed (img-5201152-0002.pdf). Using the iPhone, under DropboxDocOffset-/AUT folder, both SSDFJ\_V@\_1\_Punja\_Mislan.pdf, and *code for excel.txt* were viewed. The analytics last uploaded data on the 21st of May 2011 at 11:15:10 PM.

A keyword search on *pdf*, returned only one hit:  
*E86E3A42E1FF86CDB3004A20C24CD23B.pdf* from the directory:  
*/private/var/mobile/Media/Books/Purchases*. On opening, the file was confirmed to be the confidential file and stored in the iBook application.

E-mails could not be extracted due to the iPhone4 not being jail-broken. Thus, the file received and sent from the iPhone4 could not be found. The confidential file was confirmed to have been opened by iBook and there was another pdf launched on Dropbox. However, because the files could not be extracted, it is not possible to confirm whether the launched file was the confidential file. The evidence required and evidence found data comparison results are shown in Table 4.18.

**Table 4.18: Evidence Required and Evidence Found Comparison Table A.**

<b>Evidence Required</b>	<b>Evidence Found</b>
E-mail that contains the confidential file.	No
Evidence of the confidential file was being uploaded and stored in Dropbox.	Partial
Evidence of the confidential file was sent from iPhone to the person in company B.	No

The company uses an exchange server to distribute E-mails. In this way, John's E-mail box can be obtained. From the obtained E-mails, the file is confirmed as being sent from one of the scanner machines from the company to his work mail. However, there is still no evidence that can prove that the file is opened from his mobile. The Dropbox service provider needs to be contacted and all the files under John Smith's Dropbox account requested and a warrant issued. A warrant is also needed to be issued to get mail from his G-mail account. [johnsmith2011@gmail.com](mailto:johnsmith2011@gmail.com). After implementing the different forensic methodology mentioned above, the new data comparison results are shown in Table 4.19.

**Table 4.19: Evidence Required and Evidence Found Comparison Table B.**

<b>Evidence Required</b>	<b>Evidence Found</b>
E-mail that contains the top secret development file	Yes
Evidence of the confidential file was being uploaded and stored in Dropbox	Yes, if Dropbox provides the files under John Smith's account.
Evidence of the confidential file was sent from iPhone to the person in company B.	Yes, if a warrant is issued and Google delivers the files to the forensics lab.

#### **4.4 CONCLUSION**

In this chapter, action research was carried out to perform experiments on the three different Cloud based case scenarios using NIST standard mobile forensics tools, procedures and methodologies.

For each case scenario, detailed descriptions of the experiment set up were undertaken in order to ensure a fair experiment was being delivered. Each forensics investigation phase was tested, followed by the procedures researched in chapter two. Each of the four different forensics domains was tabled with its procedure and methodology instructions, and the details of the actions taken. The data that failed to meet the expected outcome was outlined and possible solutions were proposed and tested. To perform investigations on Cloud based mobile forensics cases, the use of mobile forensics tools, procedures and techniques is insufficient. Network or wireless forensics is sometimes needed, depending on the nature of the case and the data. However, when wireless forensics was used it successfully obtained the data that was not obtained from the current mobile forensics methodologies. The obtaining of data from Cloud service providers was another point that arose from the experiments. Current mobile forensics tools can not extract files stored in the Cloud based storage application, Dropbox. A warrant may need to be obtained to gain the evidence needed for the investigation. The next chapter, chapter six will outline all the impacts of Cloud computing identified in the experiments conducted in this chapter, and also give suggestions to the forensics investigator when undertaking an investigation on mobile Cloud forensics cases.

## **Chapter 5**

### **RESERACH DISCUSSION AND RECOMMANDATION**

#### **5.0 INTRODUCTION**

Chapter four reported the research findings of investigation conducted on three Cloud based case scenarios. The aim of performing such experiments was to identify the impact of Cloud computing to current forensics investigation by answering the research questions. The current mobile forensics tools, procedures and methodologies were tested to help identify the type of data that could not be extracted using current mobile tools, procedures and methodologies.

Chapter five will outline the impact of Cloud computing to current mobile forensics tools, procedures and methodologies and then give recommendations to mobile Cloud forensics investigation regarding procedures that should be taken in order to perform forensically sound investigation without missing any potentially important evidence to the investigation case. The section 5.1 will analyse and discuss the data in regards to the impacts of Cloud computing on mobile Cloud forensics based on the experiments data collected in chapter four. The impact of Cloud computing will be discussed based on the results obtained from chapter four as well as the literature review conducted to support the opinion addressed. In section 5.2 the research limitations encountered during the experiments will be outlined. Section 5.3 will present the previously developed research questions and hypotheses. Based on the experiment results and the literature researched, the correct hypothesis will be selected along with the possible arguments for falsifying the Null Hypothesis. Recommended investigation procedures will be presented in section 5.4. The investigation procedures will be built based on the facts gathered from the investigations conducted in chapter four, under the recommended NIST investigation procedures. Thus the revised investigation procedures could help mobile forensics obtain the Cloud data required for an investigation in a more efficient and forensically sound manner.

## **5.1 DISCUSSION OF RESEARCH FINDING**

In this section, three experimental case scenarios will be discussed one by one regarding the impact of Cloud computing on mobile forensics investigation in terms of tools, procedures and methodologies.

### **5.1.1 Experimental Case Scenario One**

Logical extraction was attempted on a Motorola Milestone Smartphone by both XRY and Oxygen. Oxygen's OxyAgent failed to install onto the Smartphone, thus the extraction could not be performed. XRY successfully extracted the data from the Smartphone. However, XRY supports only limited extraction features on the Motorola Milestone Smartphone. The evidence that can be extracted are: SMS, pictures, video, documents, files and logs. There were 20 SMS, 1 video, 8 documents, 5 files and 67 log files. However, the data that was of interest in this investigation could not be acquired using both XRY and Oxygen. Physical exaction was then performed. In order to perform a physical extraction, the phone first needed to be rooted. However, rooting also means making changes to the Smartphone and may subject the original evidence to change. This action potentially violates the first principle of computer-based electronic evidence established by ACPO (2007): "No action taken should change data held on a computer or storage media which may subsequently be relied upon in court" (ACPO, 2007, p. 4). However the second principle states: "in circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions" (ACPO, 2007, p. 4). Thus, rooting was performed by downloading the tools developed by G.O.T Team Android. Again a logical extraction was attempted using both Oxygen and XRY on the rooted phone this time. Oxygen again failed to upload the OxyAgent onto the phone, but XRY exacted 20 SMS, 2 pictures, 1 video, 9 documents, 112 files and 207 log files. There was a significant growth noted in files and log files. After examining the extracted evidence, the extra files were found to have originated from the G.O.T Team Android file packages. There was also one deleted photo that was recovered and extracted after rooting. The extraction logs extracted from the rooted phone proved that the additional



information was being added to. Even in a life threatening situation, such action should not be performed unless the investigator is able to explain what the tool does. The most commonly used tools to root the phone were developed by a third party, which means what the tool is doing is unknown and there is a chance of malicious code being added into the applications. In this case, the rooting methodology may need to be well understood by the investigators. However, each Smartphone model is different, so the rooting is different also. Even though different versions of the Motorola Milestone were designed by the same manufacturer, in different countries different rooting approaches are required.

An XRY physical extraction was performed; unfortunately, the available tools at the time could not read the detailed data using the XRY v5.2 extractor. However, when loading the physical image into the XRY v5.5, the image was unable to be opened. Both EnCase and FTK forensics examination tools were tried on the image. However, neither of these tools supported the image. G.O.T Team Android has a function which produces a Nandroid backup. However, these backup files are displayed in Hex decimal. These Nandroid backup files were then added into FTK to perform an analysis, due to the data carving function offered by AccessData's FTK. Unfortunately, there were no files were being recovered during this process.

The data that could not be extracted from a standard mobile phone by XRY was data that would be of interest in a traditional mobile forensics examination. However, with the addition of Cloud computing technology, the Smartphone stays connected to the internet 24 hours a day, 7 days a week. Any data generated through the Cloud based applications is therefore of major interest to the mobile forensics investigation. However, an inability to extract Cloud based forensics data from the Motorola Milestone Smartphone resulted, when examined by recognised and commercially available mobile forensics software under the current examination procedures and methodologies.

Internet connection is a basic requirement for most third party applications, especially Cloud based applications. Thus internet ingoing and outgoing activities can potentially contains rich amounts of data that could be helpful in an investigation, especially in a case like experimental case scenario

one. Wireless forensics was then deployed to help in capturing ingoing and outgoing network traffic, once the cellular data traffic allowance was disabled. The aim of such was to determine what the ingoing and outgoing internet activities from the phone were, thus being able to identify if the Smartphone was really infected by a virus and if so, what the virus does. The examination results demonstrated that there was a virus, called GeiNiMi.A virus, sending the user's credential information to a server outside New Zealand. Even though the existence of the virus was confirmed, how the virus got into the mobile could not be determined. Wireless forensics provides a good way to determine what is happening on the phone, but it also poses the risk of the possible remote wiping of the mobile data being executed once an internet connection is established.

### **5.1.2 Experimental Case Scenario Two**

The seized iPhone 3G Smartphone was jail-broken, which means the user had full access to the Smartphone root, so he could customise the phone. Thus the possibilities of a self destruction application or a remote wipe application being installed on the device are relatively high. At the same time, a jail-broken phone means both logical extraction and physical extraction could both be performed to acquire and preserve evidence. E-mail records could also be extracted as the phone was jail-broken. However, only 50 E-mails were extracted due to the default numbers that are displayed on an iPhone. MobileMe is a remote wiping web application, and upon the mobile being connected to the internet, no matter whether it is a 3G network or a wireless network, a remote wipe could be performed remotely from anywhere and at any time using any device which has an internet connection. Thus, keeping the device disconnected from the internet and from radio signal is very important. The phone was thus turned to airplane mode to prevent any possible connection. However, such action can not be guaranteed 100% to keep it separated from internet connection, especially if the seized iPhone is jail-broken, as customising may still allow wiping to be performed while the phone is turned to airplane mode.

The first action taken was to make a SIM card clone using the XRY SIM id-Cloner system. The cloned SIM card has exactly the same data as contained on the original SIM card. The cloned card is inserted into the iPhone because the

cloned SIM card can stop the mobile receiving radio signals from the GSM network. However, both wireless and 3G networks can not be prevented from receiving radio signals. Acquisition is performed on the original SIM card. Contacts, network information and device information are extracted. Logical extractions on the iPhone were performed using both XRY and Oxygen to compare the results. The reason for using both of this software was that both of them are forensically recognised software. If the data can not be extracted using these software, it means data can not be forensically extracted using current forensically sound software.

The experiment results show that all application configuration data can be extracted from most Cloud based applications. The Skype analyser was especially developed by Oxygen to extract data from Skype. The entire logged in user's contact information, the text messages exchanged between contacts, and the calling information can be extracted. XRY can extract the same files as Oxygen, but the data remains in a raw format and is stored in the dbb extension files.

The Viber calling and SMS information can not be found in the files extracted by both Oxygen and XRY v5.2. However when a later version, XRY v5.5 and Oxygen are used again to perform the extraction, both Viber calling logs and SMS were extracted. This shows the significant improvements in mobile forensics software there now are in both XRY and Oxygen, and that mobile forensics providers are still working on ways to extract the data from popular mobile applications. However, is it realistic to think mobile forensics providers can go through each application and figuring out a way to extract and analyse all the data generated as there are thousands and thousands of applications. Data stored in a third party application is determined by the developer of the application and the type of data that the application retains (Morrill, 2010). This data is normally stored in text files, property lists and SQLite databases. The property list gives setting information about the application.

Oxygen does not support E-mail extraction. XRY only supports E-mail extraction when a phone is jailbroken and then it is limited to only the 50 E-mails that are offloaded on the phone. If the E-mail data served an important role as evidence, the E-mail service provider would need to be contacted and a request

made to provide that E-mail data. With the Dropbox Cloud storage application, data stored in the Dropbox can not be extracted or viewed. Where the data was uploaded and accessed, and which device or median was used in accessing the data are all unknown. If there was a group account, the access log of each team member will not be found on the seized phone. Thus the data, such as who made changes to the file and the people who have accessed the file remains unknown. If the same account was used by a group, then there is only one account that has been logged onto. If the service provider provides the record or logs containing the IP address of these connection devices and the types of these devices, all the people who logged onto the account could be tracked down.

The experiment results show that Cloud storage application data can not be extracted using existing software and methodologies. In the future with Cloud forensics, the Cloud service providers will be heavily relied on due to the nature of Cloud data and how the data is distributed. However, this may lead to cross jurisdiction problems. The service provider may have their data centres in America, China and South Africa at the same time. When the investigation is carried out in New Zealand, how data would be seized. However, some of this information is potentially addressed in SLA agreements between Cloud service provider and users. “Cloud computing represents just one of the fast-paced technological developments that is presenting an ongoing challenge to legislators, law enforcement officials and computer forensic analysis” (Frowen, 2011, p 1). Relying on removing everything from the data centre can not be a future solution for investigation of a Cloud based case. The nature of Cloud computing is that applications and files can be accessed anywhere and at any time. Thus it is important to review all Cloud based applications and to contact their service provider immediately, otherwise data is more than likely to be changed, overwritten or deleted.

Cloud computing can help an investigation in several different ways. Firstly, it can make data more visualised. The Metadata extracted from pictures contains GPS coordinates, which can be used in the detecting of where the photos were taken. The WiFi and IP connection data can also draw a picture of where the terrorists have been and find possible hiding places. WiFi connection data can be

used to exactly pinpoint the place where the phone was connected to the WiFi and the time that it was connected, by exporting the data to Google Earth. Thus Cloud computing can also help visualise the data evidence by translating coordinates into actual street addresses.

### **5.1.3 Experimental Case Scenario Three**

In experimental case scenario three, newer versions of XRY and Oxygen software were used. The inability to extract data from Cloud based applications using current tools and techniques was reflected though the investigation performed in chapter four. In this case, an E-mail that contained the top secret file sent from a scanner was not able to be obtained. There was only evidence of one pdf file being opened with Dropbox. However, the actual files stored in Dropbox were not viewable or able to be extracted. Thus, there is no evidence to prove whether or not the opened file was really the confidential file. The E-mail which sent the confidential file to company B is not obtainable either. In order to review the content of the file uploaded in Dropbox, a warrant needed to be issued to the Dropbox Cloud service provider. Even though, the evidence can be proved as it was downloaded and read in John's mobile, the important evidence of how the company competitor managed to receive the file is unknown. There are a few different ways that a file could have been transferred, or delivered to the company competitor. The first possibility is by E-mail. This poses a problem, as E-mail transaction records can not be extracted by logical extraction, and the seized phone would first be required to be jail-broken. However, the action of jail breaking a seized phone violates the ACPO (2007) principle 1, that no action taken should change data that may subsequently be relied on in court. Evidence however could be requested from the mail service provider. Another possibility would be to use Dropbox, as it can be accessed by anybody around the world as long as there is a device which can browse the internet and an internet connection is available. However, if there was a record of where the file was accessed, and the media that was used to open the files, then that would make the forensic investigation task a lot easier. There is always the possibility of sending the file physically by post.

Commercial mobile forensics products have demonstrated their ability to try and cope with the fast growing technologies and applications. However, they will always fall behind newer developing technology, and they will always have models that can not extract the evidence fully, as there are so many different mobile models and most of them are not identical. Data storage places for different phones are different, even on different models manufactured in the same company, as there are currently no standards to have to follow.

#### **5.1.4 Discussion Summary**

Cloud computing is impacting greatly on current mobile forensics in regards to tools, procedures and methodologies. The current mobile forensic tools can not keep up with the speed of growth in the availability of applications. Even though mobile forensics software providers are working their best to develop new features to acquire more data from different applications, there are never any 100% guarantees that the data required for a particular investigation can be extracted from the available data. Thus changes need to be made to the current mobile forensic procedures in order to acquire and preserve data in a more efficient and forensically sound manner. Different forensic methodologies derived from different forensics domains such as network forensics may need to be integrated as traditional mobile forensic methodologies can not preserve all the data that is generated from Smartphones. For example, Cloud based data can only be obtained from the Cloud service provider, which also potentially poses other constraints such as jurisdiction problems. However, Cloud computing technology does help in visualizing data, making it more meaningful and more easily understood by non-technical people.

## **5.2 RESEARCH LIMITATIONS**

There are many limitations in this research, and one of the biggest limitations is the acquiring of data from both cellular and Cloud service providers. A proper warrant needs to be presented to be able to get the evidence from both the cellular and the Cloud service providers. Getting telephone transaction records, including call logs and text messages from cellular service providers is doable, but unfortunately most of the service providers only keep logs for six months. Thus,

retrieving data that is older than half a year creates a hassle. Acquiring data from the Cloud service provider has proved to be doable, and there are two ways of gaining this data. One way is physically going to the data-centre where the service provider stores them and extracts the data from the server using old hard drive acquisition methods. However, such an approach would cause a huge economic drain and would also lack efficiency. Besides this, the data can be held anywhere around the world, and seizing data from across borders can raise many legislation issues. The other way is to present a warrant to the service provider and ask them for the data that belongs to the person or organization in question. This potentially solves the problem of seizing the evidence using traditional hard drive forensics. However, the integrity of the data provided by the Cloud service provider needs to be trustworthy as it would be heavily relied upon.

The software and hardware required to perform these experiments is limited. Even though a Nandroid backup was created, the backed up ISO image files could not be carved using FTK and the raw information data was not able to be read by humans. Physical extraction was performed using XRY on an iPhone 3G. However, the XRY extractor could not read the physical extraction. There was no more third party application data other than the data already obtained through logical extraction.

### **5.3 RESEARCH QUESTIONS AND HYPOTHESES**

In this section, the research questions are answered and the correct hypothesis is also identified. The possibilities of falsifying the Null hypothesis are also discussed.

#### **5.3.1 Research Question**

The main research question was to test whether existing forensics investigation procedures and methodologies could be adopted with the changes brought by the new computing technology of Cloud computing, with the aim of this thesis being to determine the impacts of Cloud computing on mobile forensics in terms of tools, procedures and methodologies. The main research question: *Is there a need to develop new forensics tool, procedures and methodologies for mobile Cloud*

*forensics investigations?* The sub research questions are designed to develop a systemic approach in working step by step to answer the main research question. Firstly, the question needs to be defined as to whether current forensics tools, procedures and methodologies still work for Cloud based mobile forensics investigation. Action research was chosen to conduct the test part of the research. To ensure the quality of the tests conducted, NIST standard mobile forensics procedures and methodologies were chosen to be the baseline of the mobile forensics investigation.

### **5.3.2 Sub-Question**

In order to answer the main research question, it was important to know the type of data that current mobile forensics tools, methodologies and procedures could obtained in a Cloud based case scenario. Thus, a sub research question needed to be answered first.

#### **5.3.2.1 Sub-Question one**

*What data can be acquired and preserved using the existing mobile forensics tools, methodologies and procedures in mobile Cloud computing forensic investigations?*

The standards need to be set in order to conclude the first sub question. The standard depends on the type and completeness of the evidence that is to be extracted. To help in answering this concern, the second sub research question is presented.

#### **5.3.2.2 Sub-Question Two**

*Can existing mobile forensics tools, procedures and methodologies acquire and preserve all the evidence needed for mobile Cloud investigation?*

If the data of interest to the investigation was not able to be extracted using the existing mobile forensics methodologies, then methodologies that can acquire the data need to be proposed. Thus the last sub research question could help to answer this concern.



### 5.3.2.3 Sub-Question Three

*If the current mobile forensics tools, procedures and methodologies could not fully extract the evidence needed for undertaking the investigation, are there any existing methodologies that could help to seize the missing data?*

### 5.3.3 Sub-Question Answers

In this section, research sub questions are answered with supporting evidence. The answer for the first sub-question is: The data that can be acquired and preserved using the current mobile forensics tools, methodologies and procedures in mobile Cloud computing forensics investigation is dependent on the tools used to extract the evidence and the features supported by that mobile model. Most of standard data required in traditional forensics, such as SMS messages, or call logs are supported by most tools across many mobile models. The mobile forensics tools providers are still working on developing more features, thus enabling the extracting of more evidence from the phone. An example: from the experiments Viber call logs and SMS messages could not be obtained using XRY v5.2. However, XRY v5.5 supports such a feature and in using v5.5 the call logs and SMS messages can be obtained.

The answer for sub-question two is: Current mobile forensics tools, procedures and methodologies can not acquire and preserve all the evidence needed for mobile Cloud investigation. In experimental case scenario one, without the help of wireless forensics, nothing relevant to the case could be extracted using XRY. Also, without the continual updating of forensics tools, data generated from new applications will not be obtained. E-mail poses another challenge to current mobile forensic also.

Sub-question three asks: *If the current mobile forensics tools, procedures and methodologies could not fully extract the evidence needed for undertaking the investigation, are there any existing methodologies that could help to seize the missing data?* Wireless forensics is one answer that may be considered as a great source to engage. Wireless forensics was employed in the experimental case scenario one, to extract useful evidence to answer the questions set up for that case scenario. However, performing extraction based on a live phone can pose some problems; the integrity of the data is questionable as it violates the first rule

of the good practice guide for computer-based electronic evidence which is, “no action taken should change data held on a computer or storage media which may subsequently be relied upon in court” (ACPO, 2007, p. 4). In the case two scenario, data from the Dropbox could not be acquired using existing mobile forensics procedures and methodologies. Instead, Dropbox Cloud service providers needed to be contacted to provide the documents belonging to John’s Dropbox account.

In order to extract E-mail from the mobile device, the iPhone needed to be jail-broken. However, the E-mail sent using the Dropbox application was not able to be traced. Thus, existing forensics procedures and methodologies were not enough to solve this case. If a warrant was issued to the service provider, and a copy of the E-mails from John Smith’s account was provided, it would be likely that the E-mail could be traced from the server, and then the E-mail sent from the iPhone using the Dropbox application could be found. Thus, the answer to the main research question would be, with additional help of other forensics methodologies, investigation into Cloud based mobile forensics can be achieved.

#### **5.3.4 Hypotheses**

Hypothesis  $H_1$  made in chapter three section 3.3.1 proved to be false, as existing mobile forensics methodologies and procedures could not retrieve all the data needed for Mobile Cloud Computing based forensics investigation. Hypothesis  $H_0$ : *A combination of existing mobile forensics and other forensic methodologies can retrieve all the data needed for Mobile Cloud Computing forensics investigations*, was proved to be a valid statement. Thus, the alternative hypothesis  $H_2$ : *There is a need to develop completely new forensics methodologies and procedures* were proved to be unnecessary, unless situations happened which could falsify the Null hypothesis. The possible situations that a Null hypothesis could be falsified will be addressed in the next section.

#### **5.3.5 Falsifying the Null Hypothesis**

The experiment results proved that Null hypothesis  $H_0$  was the answer to the main research question. However, the hypothesis could be falsified under the following situations: when the ISPs logs can not be made available; when the Cloud service

provider lost the data, which has happened on hotmail; when the Cloud provider refuses to hand over logs/data because of jurisdictional aspects, which could be an issue due to the Cloud computing nature of data centres being anywhere around the world; when a new type of mobile Cloud misuse is discovered that falls outside the current forensic methods; or when the mode of interaction between the mobile and ISPs/Cellular network is too difficult to analyse, because a cellular service provider can not preserve all the data sent from a mobile when it uses a wireless network as only live acquisition on a wireless network would capture the wireless data. If any of the situations listed above happened and critical evidence was lost, it could all result in the Null hypothesis being falsified.

#### **5.4 RECOMMENDED MOBILE INVESTIGATION PROCEDURES AND METHODOLOGIES**

In this section, the problems with current forensics tools procedures and methodologies are identified based on the research findings in chapter four. Correspondingly, changes of the forensics procedures to solve the problems identified need to be instigated so that the new mobile forensics procedures can be used in mobile Cloud forensics investigation.

The first problem identified was, existing mobile forensics software had difficulty in extracting data from an Android Motorola Milestone Smartphone. Even though the extraction was successfully performed by XRY, only a limited amount of data was extracted, due to the poorly support features from both software providers. Oxygen and XRY forensics solution providers are both still developing new features to add in their forensics software. The data that could not be extracted 2 months ago is now able to be extracted with a newer version of software.

The newly released XRY v5.6 notes state that XRY has developed new features for 858 devices, which is shown in Figure 5.1. The XRY v5.6 now introduces physical support, with both dumping and decoding, for more than 60 different models of Android devices (MSAB, 2011).

Forensic method	New devices	Total
XRY Logical	319	2,691
XRY Physical Dumping	125	929
XRY Physical Decoding	125	817
Security Codes	169	169
XRY Untested	120	311
<b>Total</b>	<b>858</b>	<b>4,917</b>

**Figure 5.1: XRY Forensics Method and Device Supported (MSAB, 2011)**

Oxygen v3.4 is also a new version released, which supports android automatic rooting as part of the Data Extraction Wizard, guiding the whole process of gaining temporary root rights to the device. The root access will be revoked immediately after rebooting the device, thus lessening the chance of altering any potential data. Thus, rooting and extraction can be done in a safer and more forensically sound manner. However there is no 100% successful rooting guaranteed. “Oxygen Forensic Suite 2011 is the only Smartphone forensics software that allows automatic rooting and provides powerful in-built tools for data analysis” (Oxygen Forensic Suite, 2011, P. 1).

Different digital forensics may need to be considered before conducting mobile forensics, such as wireless forensics. If possible, Cloud based applications need to be noted down before conducting the mobile forensics investigation, due to the nature of Cloud which allows data to be accessed and changed at any given time. At the same time as the phone is seized these Cloud services providers need to be contacted so that their service to the user is terminated.

In order to retrieve virus data, wireless forensic may need to be performed to monitoring the incoming and outgoing traffic of the Smartphone. Wireless forensics should be performed before the acquisition phase, as monitoring data can potentially change the data on the device, and this would result in inconsistencies in MD5 values. To make the right call, investigators will need to use their judgment as to whether or not wireless forensics investigation should be performed dependent on the situation and circumstances.

The second problem identified, is Cloud storage based application data cannot be extracted using mobile forensics tools, due to the fact that the data is

being opened and managed is at the Cloud end. Cloud service providers will take a very important role in the future of mobile forensics or computer forensics. Thus, instead of obtaining data only from the Smartphone and cellular provider, the Cloud service provider becomes the next biggest forensic data provider. Due to the nature of Cloud applications, being able to be accessed and modified anywhere, anytime using any device with an internet connection, it is important to first identify all the Cloud based applications, and contact their service providers thus preventing the possibility of any change being made to the Cloud data before a forensics investigation is performed.

## **5.5 UPDATE THE FORENSICS INVESTIGATION METHODOLOGIES AND PROCEDURES**

In this section, the changes that need to be made to current forensics investigation procedures and methodologies are identified below.

- Identify relevant data that can be used as evidence before conducting the investigation. Thus, tools, methodologies and procedures can be considered first.
- Consideration needs to be given to the performing of network forensics, such as traffic capture, depending on the case scenario and situation. Network forensics should not be performed after the acquisition, due to the fact that the incoming and outgoing traffic may change the data on the phone, thus changing the hash value and making the integrity of the evidence questionable and unusable in court.
- Browse through the phone and outline the Cloud based applications before the phone is switched on.
- Contact the service provider(s) to obtain the user's data.

Suggested investigation procedures and methodologies are listed in the following sections based on the procedures outlined in section 5.4.2.

### 5.5.1 Preservation

- Secure and Evaluate the Scene:
  - Secure and protect the integrity of both the traditional and the electronic evidence.
  - Evaluate the scene and the nature of the case, and then formulate a search plan.
  - Identify potential evidence and data that are of interest to the investigation.
  - Identify if there is a need to conduct other forensic analysis, such as DNA.
  - Conduct interviews to retrieve the password and pass codes.
- Document the entire scene including all potential evidence.
- Collect the evidence:
  - Is the phone switched on?
    - Phone is switched on:
      - Identify if there is a need to conduct a live forensics acquisition.
      - Obtain the password, if required.
      - Browse through the evidence and note down all the Cloud based applications and the contract service providers of the applications.
      - Take measures not to interrupt the power supply. Isolate the phone from all possible connections, including: radio signals, Wi-Fi, Bluetooth and infra-red.
    - Phone is switched off: Go to the next step.

- Secure the phone and all its accessories.
- Package, transport and store the evidence

### **5.5.2 Acquisition**

- Identify the device.
- Is the phone switched on?
  - When the phone is switched on:
    - Make sure the phone has a high enough battery level.  
Isolate the phone from radio signals and all possible connections, including: Wi-Fi, Bluetooth and infra-red.
    - Look up the phone capabilities and download the manual.
    - Select the forensic tools for the phone. Plan the examination and analysis.
    - Test the tools on an identical phone before using them on the seized phone.
  - When the phone is switched off:
    - First try and remove the SIM card without taking the battery out. If this is not possible, remove the SIM card and put the battery back in immediately.
    - Clone the SIM card.
    - Use a forensic tool and read the PIN/PUK status.
    - Contact the provider to get the PUK, or find a way to gain access using a backdoor.
    - Use a forensic tool and examine the SIM card.

- Is it an obstructed or an unobstructed phone?
  - Obstructed:
    - Investigation methods:
      - Ask the suspect for the password.
      - Review the seized material.
      - Manually supply commonly used password input.
      - Ask the service provider for the password.
      - Exploit potentially insecure settings.
    - Software based methods:
      - Exploit known weaknesses in authentication.
      - Gain access through a software backdoor.
      - Exploit known system vulnerabilities.
    - Hardware based methods:
      - Gain access though a hardware backdoor.
      - Examine the memory of the device independently.
      - Find and exploit vulnerabilities.
      - Infer information by monitoring the physical device characteristics.
      - Use automated brute force attack.
  - Unobstructed: Go to step 4.
- Tool selection and expectation after examining evidence from:



- Mobile phone.
- SIMS.
- External physical storage.

### **5.5.3 Examination**

- Identify the type of evidence that could be of interest to the investigation.
- Obtain evidence from:
  - Call and subscriber records.
  - Cloud service provider records.
- Use proper tools and techniques to examine and analyse the evidence from:
  - The SIM card.
  - The mobile handset.
  - External physical storage.
  - Call and subscriber records.
  - Cloud service provider records.

## **5.6 CONCLUSION**

Chapter five developed a detailed discussion over the research findings for each experimental case scenario investigated in chapter four. The impacts of Cloud computing on Mobile forensics in terms of tools, methodologies and procedures were discussed. Research limitations while conducting experiments were also discussed. The research questions proposed in the research methodology chapter have been answered and discussed in terms of the previously asserted hypotheses. The possible situations that could falsify the Null hypothesis were also discussed.

Furthermore, recommendations were also made on forensics procedures when undertaking mobile Cloud forensics investigation.

The experiments proved that Cloud based storage data which has not been offloaded to the Smartphone, cannot be extracted from the handset with current mobile forensics tools and techniques. In order to get the Cloud based storage data, the Cloud service provider needs to be contacted to provide the evidence once a warrant is issued. However, jurisdiction problems across borders could raise many challenges for Cloud based investigation.

The main research question of this thesis project was centred on testing the current mobile forensics tools, methodologies and procedures by applying the NIST forensic guidelines. Cloud computing has significantly changed how data is stored and operated on a Smartphone. Current forensic investigating tools, procedures and methodologies cannot acquire all the data needed for the mobile forensic investigation. In order to adapt to the changes brought by Cloud Computing, changes need to be made to the current forensics procedures. The impact brought by Cloud Computing to mobile forensics has been discussed in terms of the advantages and disadvantages to mobile forensics. Thus, recommendations on the Cloud mobile forensic guidelines were made and the current forensics procedures were updated based on the changes needing to be made that were identified by the three Cloud based scenarios.

Chapter six will conclude this thesis and presents a summary of the research conducted and the significant results that have been discovered. Limitations to the research will also be outlined and the future work needed in the prospective fields of research within the discipline area will be highlighted.

## **Chapter 6**

### **CONCLUSION AND FUTURE RESEARCH**

#### **6.0 INTRODUCTION**

Chapter one briefly introduced the topics of the chosen research area, and outlined the motivation for conducting such research. Cloud computing has significantly revolutionized current IT infrastructure, with the advantages of Cloud computing facilitating Mobile Cloud computing. Cloud computing will be the key driving technology to mobile computing (Perez, 2009). The current mobile forensics tools, methodologies and procedures are facing many constraints. Cloud computing potentially brings much more challenges to mobile forensics. Due to the changes brought by Cloud computing, the tasks that can be performed on Smartphones have significantly changed. More financial transactions are processed using Smartphones than ever, which has increased the spread of financially motivated fraud all around the world.

Chapter two presented the literature research on the topics in the chosen research area, which provides a better understanding of its problems. The research was divided into the four domains of: mobile computing, Cloud computing, mobile Cloud computing and mobile forensic procedures. Issues regarding each domain are outlined and discussed, especially the forensics implications.

In chapter three, the research questions and hypotheses were established. The research question and sub-questions were designed in a systematic way, so that the main research question would be answered after answering all the sub research questions. The research model was designed and created, so that the research questions could be answered and the research aim could be fulfilled. Chapter three also presented the plan for data collection, analysis and presentation. Three Cloud based experimental case scenarios were also formed in chapter three, so that the experiments could be carried out. Similar studies in the

chosen field were also introduced so that the best methodology could be chosen to conduct the forensic investigation.

The experiment results were presented in a journal format in chapter four, which recorded everything that was done in conducting the investigation. Based on the research findings, the impact of Cloud computing on mobile Cloud forensics were revealed in terms of tools, methodologies and procedures. Recommendations were also made on Smartphone Cloud forensic investigation in chapter five.

Chapter six presents the final conclusion of this thesis. Section 6.1 is a summary of findings, which were previously reported in chapter four and discussed in chapter five. The research having been conducted, the summary of the research findings presented in chapter four along with the subsequent review of the discussion of the research findings in chapter five are now concluded. The summary of the limitations predicted and encountered throughout the research will also be concluded in section 6.3. Furthermore, potential future research areas within the chosen topic area will be outlined in section 6.4.

## **6.1 SUMMARY OF FINDINGS**

In phase one of the research model (shown in Figure 3.2) case scenarios were established to act as a guideline which would enable experiments to be performed. The experimental case scenarios were derived based on real case studies and the facts gathered from the literature reviews. The first scenario was derived from a real case study of the known Android virus, GeiNiMi. To ensure the case scenario was correctly implemented, the theory of the virus was studied from both news paper articles and TV news. Case scenario two was derived from the facts gathered from the literature review in chapter two. This case scenario was inspired by the September 11 terrorist attack. If the terrorists utilised G-mail to send the commands to other terrorists, they could also have utilised mobile Cloud. The advantage is mobile Cloud gives greater flexibility, as people can have their mobile with them all day and every day. The purpose of this experimental case scenario was to test the type of data that could be extracted from third party Cloud applications on an iPhone 3G. A range of third party Cloud communication and

storage applications were chosen to test the capability of the current mobile forensics tools. The third party applications chosen included Skype, Viber, G-mail and Dropbox. The last case scenario was a demonstration of how Cloud computing applications could potentially be used to perform workplace misconduct. An iPhone 4 was chosen to conduct the experiment due to its popularity in the workplace. As E-mails contain rich forensic data, this scenario focused on E-mail extraction from the mobile using a non-jail broken phone. Logical extraction could not retrieve the E-mail messages from the iPhone as E-mail messages can only be extracted when the phone is jail-broken.

Phase two was the experiment phase of the thesis. Action research was implemented to produce the research findings. The reasons for using action research to conduct the experiments was due to the nature of action research with its learn by doing, and its cyclic process of action and critical evaluation taken in turn. Such characteristics fitted well with the nature of the research and were able to answer the research questions set up in section 3.1.1.

Phase two contained the four stages of planning, acting, observing and reflecting. Control data was collected from the Plan stage. Different types of data were collected in different stages of phase two, and control data was collected in stage one. Control data served as a benchmark, which the investigation should have achieved in order to be successfully completed. The control data for the experimental case scenario one was to be able to retrieve SMS messages, call logs, internet browsing history, web activities, identify the GeiNiMi virus and what the virus does. The control data for the case two scenario was to be able to retrieve Skype chatting logs and call logs, Viber chatting logs and call logs, G-mail, Files stored in the Dropbox, the Wi-Fi connections and the pictures. The control data for the case third case scenario was to be able to find the confidential file in the user's work E-mail, evidence that the file was uploaded to the Dropbox and evidence that the file was sent from the iPhone to the contact in company B.

Extraction logs are the logs generated from the chosen forensics tools and methodologies employed to conduct the investigation. The extraction logs are preserved in the appendix section. Appendix A is the report produced by XRY v5.2 on the Android Motorola Milestone Smartphone. Appendix B records all the

rooting procedures of the Android Motorola Milestone. Appendix C records the data logs extracted from the SIM card inserted in the iPhone 3G. Appendix E records the Wi-Fi connection report with the Google Map correspondents.

A journal was collected throughout the Action stage which preserved every action taken while conducting the experiments. The journal data includes the steps taken to set up the experiments; the actions taken to acquire and preserve evidence from the Smartphone across four forensic domains; and the preservation, acquisition and examination which includes the tools used, the procedures adopted and the methodologies employed. The outcome of the investigation was also presented in the journal. The problem solving data collected in the evaluation stage was also recorded in the journal. The problems identified were: the type of data which was not able to be extracted, and the possible solutions after looking at other forensic areas. Wireless forensics was used to solve the problem in case scenario one, different versions of tools were used to solve the problem in scenario two and that the Dropbox Cloud service provider and the G-mail provider may need to be contacted to obtain the documents and E-mails stored in the users' account.

Data comparison was presented in a table format. Experimental case scenario one showed that some of the evidence required was not able to be found using the current forensics tools, methodologies and procedures. Table 4.5 showed that the web activities, the phones virus infection status and the virus capabilities could not be acquired and preserved. However, after implementing the wireless forensic methodologies of using Wireshark to capture the incoming and outgoing network traffic, all the missing evidence was found, which was shown in table 4.6. In the case scenario two, the Viber chat logs and call logs, and the files stored in the Dropbox were not able to be extracted by the mobile forensic tools used. However, the files that were stored in John's Dropbox account could be provided by the Dropbox service provider, if a warrant was first issued. A later version of XRY v5.5 was used to extract the data from the iPhone 3G. Viber chat logs and call logs were extracted. However, there was only a little information that could be extracted from the Dropbox, and the files stored in the Dropbox still could not be extracted and viewed. In the case three scenario, the required

evidence was the finding of the E-mail that contained the confidential file and that the confidential file was sent from the seized iPhone to a person in company B; these were not able to be found. There was evidence that a pdf file had been opened in the Dropbox; however the name of the pdf file could not indicate whether the opened file was the confidential file. Thus, evidence that the confidential file had been uploaded and stored in the Dropbox was very vague.

Phase three identified the impact of Cloud computing on mobile forensics investigation in terms of forensically sound tools, procedures and methodologies. Cloud computing brings many advantages to mobile forensic investigation and at the same time poses challenges as well. Cloud computing is the key force driving development, and the growth in a wide range of features in applications now offered is the reason why Smartphones are so popular (MSAB, 2011). Currently there is more forensic data obtainable from Smartphone mobiles, such as the places the user has travelled and where photos were taken. GPS co-ordinates embedded in photos can be translated into real addresses on Google maps. From the series of Wi-Fi connection points a picture of the route the user has travelled can be virtualized on Google Earth. This enables the scaling down of the range to target the suspect by helping make the evidence more visualised, and allowing a greater amount of evidence to be understood earlier by investigators.

Currently, forensics tool developers such as XRY and Oxygen are still working on their tool features to enable extraction of more data from third party applications and the physical dump of the phones memory. The Viber chats and calls logs that could not be extracted with XRY v5.2, but are now able to be extracted using XRY v5.5. Android physical extractions can be successfully performed since mid June 2011 by either of the new releases of XRY or OXYGEN. However, even though there are 4,917 devices supported by XRY, there are still only limited features that can be extracted from a Motorola Milestone. Open source forensic tools are not very forensically sound and cannot be guaranteed to work 100%. Even a Nandroid backup, created using the tool developed by G.O.T, still has difficulties with reading and analyzing a Nandroid backup file.

Current forensic tools and methodologies could not extract data from Cloud storage based applications such as Dropbox and have difficulties in extracting Cloud based E-mail such as G-mail. To acquire and preserve data from Cloud storage applications poses a very unique challenge to forensic investigation, as the traditional way of conducting forensic work of physically going to the data centre and removing all the potential evidence, transporting it back to the lab and conducting analysis will not be the methodology for conducting an investigation in a Cloud environment, due to the fact that the data centre could potentially be in many different locations across many different borders. Jurisdiction problems may also arise. Removing hard drives would interrupt the service from normal operation, which could result in huge economic damage to many companies and the data extracted from the data centres could easily exceed 1000TB. Going through 1000TB hard drives could take a lifetime. Thus, collecting data from the service provider would be the most convenient way, but the integrity of the data may be questioned. Cloud based E-mail can only be extracted using forensics tool if the phone is jail-broken, or has a root access right. Jail-broken a phone means changes are made to the evidence, which would make the investigation less forensically sound. There can only be 50 E-mails offload to the Smartphone at the time of extraction, so there is the chance that the evidence has fallen outside the range of these 50 E-mails. Thus, collecting E-mail data from the E-mail service provider would be another methodology. However, the service provider cannot be relied on 100% either as a disaster may happen to their data centre, a good example being the 'hotmail incident' where the hotmail service provider lost E-mail for a number of customers and these E-mails were not able to be recovered (Windows Live, 2011).

Phase four gave the recommendations of forensics investigation procedures for helping to carry out investigations in a mobile Cloud environment in a more efficient and forensically sound manner. The procedures were a revision of the NIST standard forensics procedures. The changes were made in preservation, and examination. In the acquisition phase, if possible analyse the case first and form a search plan to identify the type of data of interest to the investigation. Instead of only being concerned with traditional forensics, such as DNA, other areas of the forensics domain may need to be considered such as



network forensics. Before securing a Smartphone, if the password is given the Cloud storage based applications need to be noted down first, and those service providers contacted immediately, as Cloud storage data can be accessed anywhere at any time using any device which has internet connection. During the examination phase, instead of only obtaining data from the Smartphone, SIM card, external storage cards and cellular provider, the Cloud service provider will act as one of the biggest forensics data distributors.

The research goals were successfully achieved as action research was well suited to this thesis project. All the research questions were answered and each hypothesis was tested. If another research methodology had been used, the hypothesis may not have been tested fully, resulting in the conclusion being another hypothesis. Even though surveys are the most popular research methodology, they do not suit this project as there are very few experts in this research topic field to survey.

The Null hypothesis was proved to be correct, in that changes need to be made to current mobile forensics procedures; the combination of existing mobile forensics tools and methodologies are able to acquire and preserve the required evidence needed for mobile Cloud computing forensics investigations. Thus, there is no need to develop new mobile forensics tools, procedures and methodologies.

This Null hypothesis could be falsified in the following situations:

- When there is a new Smartphone which no forensics tool supports
- When the ISPs logs can not be made available
- When the Cloud service provider lost the data
- When the Cloud provider refuses to hand over logs/data because of jurisdictional aspects
- When a new type of mobile Cloud misuse is discovered that falls outside the current forensic methods.

## **6.2 LIMITATION OF THE RESEARCH**

There are five limitations identified within this research. Due to the limitation in the availability of Cloud forensics academic publications, most of the literature

and information cited are from commercial and industrial sources. However, every attempt has been made to ensure that the sources are as reputable as possible. There is no guarantee either that the sources will continue to exist at their current URL locations. The second limitation is the lack of real cases studies in mobile Cloud forensics. Only three case scenarios are used to conduct this investigation. The chosen scenarios may not have covered all the perspectives of mobile Cloud computing. There are chances that Cloud elements were left untested. The third limitation is identified as the tools used to conduct the experiments. Due to the budget constraints, the software and hardware available in the lab to perform the experiments was limited. Only two mobile forensic extraction tools were used during the examination, and there may be another tool which can extract more features for the particular Smartphone models used in the experiment. However, both XRY and Oxygen are well known to be forensically sound tools. Another limitation identified was the privilege of accessing sensitive data. Without a warrant, acquiring data from both cellular service providers and Cloud service providers may not be possible. Thus, the data that should be acquired from a cellular service provider and the Cloud service provider were not available in this instance. Thus some of the theory proposed in the thesis has not been tested, so is purely supported by reviewed literature. In addition, even though a warrant could be issued, the service provider does not have to preserve logs which are older than 6 months in countries like American and China. If the evidence needed was greater than 6 months previous, there is a small chance that the data could not be provided from the service provider.

### **6.3 FUTURE RESEARCH**

The research conducted during the project has provided additional insight to the chosen topic areas in mobile Cloud forensics. This thesis also outlined a number of aspects for further research to be performed in mobile forensic investigation from the mobile Cloud forensic area.

The first area identified as a target for future study was with regard to Law and legislation issues, due to the factors of the multi-jurisdictional and multi-tenancy default setting of Cloud forensics. Thus, how data could be collected, and

what would happen in the case of an internationally collaborated investigation being required.

The second identified target area for future study was in the investigating and developing of forensically sound methods to gain root access to different models of Smartphone and the methods to read the physical dump created by the Nandroid. The research conducted in this thesis found an inability to read the Nandroid physical memory dump, even though the physical dump was created. Other forensic extraction methodologies, such as Chip-Off and Micro Read may be worth while testing on the Smartphone to examine if there is any further data that can be extracted beyond that obtained from logical extraction

The last identified target area for future study was in the testing of more tools on a greater variety of Smartphones or tablets, with more Cloud based applications installed. Cloud computing not only benefits the Smartphone, but also the significant market in other mobile devices, such as the tablet. “Juniper believes that as more tablets are brought into the enterprise over the forecast period, the proportion of tablets featuring security product will also increase and will overtake the protected Smartphone user levels” (JUNIPER Research, 2011, p. 1). Thus tablet forensic is indentified to be another area to conduct future research on.

## Publication

Presenter, Zhu, M. (2010, April). *Does mobile Cloud computing require a new forensics methodology?* Paper presented at China Computer Forensics Conference of China Computer Forensics Research Centre (CCFRC), China; Network Security Laboratory, China; Institute of High Energy Physics, China; Chinese Academy of Sciences, China; Center for Information Security and Cryptography (CISC), China; Dept. of Computer Science, HKU, Hong Kong; Information Security and Forensics Society (ISFS), China; Committee of Computer Forensics Experts in Chinese Electronic Institute, China.

## References

- ABI Research. (2009). *Mobile Cloud computing subscribers to total nearly one billion by 2014*. Retrieved May 25, 2011 from <http://www.abiresearch.com/press/1484-Mobile+Cloud+Computing+Subscribers+to+Total+Nearly+One+Billion+by+2014>
- ACPO. (2007). *Good practice guide for computer-based electronic evidence*. [Supported by 7 Safe Information Security.] Retrieved March 23, 2011 from [http://www.7safe.com/electronic\\_evidence/ACPO\\_guidelines\\_computer\\_evidence.pdf](http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf)
- AdMob Mobile Metrics. (2010). *45 millions US Smartphone Use – comScore*. Retrieved May 12, 2011, from <http://metrics.admob.com/2010/04/45-million-us-smartphone-users-comscore>
- AEPONA. (2010). Network as a service and mobile Cloud computing. *AEPONA White Paper*. Retrieved from <http://www.aepona.com/white-papers/network-as-a-service-and-mobile-Cloud-computing/>
- Ante, S. E. (2010). *Banks rush to fix security flaws in wireless apps*. Retrieved from April, 20, 2011 from <http://online.wsj.com/article/SB10001424052748703805704575594581203248658.html>
- Biggs, S., & Vidalis, S. (2009, November). Cloud computing: The impact on digital forensic investigations. *Proceeding of International Conference for International Technology and Secured Transaction., ICITST 2009*.

Retrieved from

[http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?arnumber=5402561](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5402561)

Bolding, C. (2008). *Assessing the security benefits of Cloud computing*. Retrieved August 5, 2010 from <http://Cloudsecurity.org/tags/forensics.html>

Botsman, R. (2011, June). Pay as you go. *AFR Boss Magazine*. Retrieved June 15, 2011 from [http://www.collaborativeconsumption.com/blog-and-writings/Pay\\_As\\_You\\_Go\\_BOSS\\_June.pdf](http://www.collaborativeconsumption.com/blog-and-writings/Pay_As_You_Go_BOSS_June.pdf)

Britz, M. T. (2008). *Computer forensics and cyber crime*. New Jersey, USA: Pearson Education Upper Saddle River.

Brothers, S. (2009). *Cell Phone and GPS Forensic Tool Classification System: 2009Update [PowerPoint slides]*. Presented at Mobile Forensics World 2009. Retrieved April 01, 2011 from [www.mobileforensicsworld.org/2009/presentations/MFW2009\\_BROTHERS\\_CellPhoneandGPSForensicToolClassificationSystem.pdf](http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhoneandGPSForensicToolClassificationSystem.pdf)

Brunette, G., & Mogull, R. (2009). *Security guidance for critical areas of focus on Cloud computing*. Cloud Security Alliance. Retrieved May 5, 2011 from <http://www.Cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>  
<http://direct.bl.uk/bld/PlaceOrder.do?UIN=151297443&ETOC=RN&from=searchengine>

Buecker, A., Lodewijkx, K., Moss, H., Skapinetz, K., Waidner, M. (2009). Cloud security guidance: IBM recommendations for the implementation of Cloud security. *IBM Redpaper*. [Press release]. Retrieved from <http://www.slideshare.net/IBMIndiaSS/Cloud-security-guidance-ibm-recommendations-for-the-implementation-of-Cloud-security>

CCTV13 News. (2010). 感染用户超过90频发”给你米“万病毒 [translated: Over 900,000 virus infected users “to give you rice” frequent]. [Video file].

Retrieved April 5, 2011 from  
<http://www.netqin.com/security/securityinfo.jsp?id=3691&type=3>

Creswell, J. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Thousand Oaks, California: Sage Publications.

Dai, J. (2007). Research cell phone forensics and electronic evidence acquisition. *Computer and Modernization*, 5. 100-102. Retrieved from  
<http://scholar.ilib.cn/A-QCode~jsjyxdh200705033.html>

Dick, B. (1997). *Action learning and action research*. Retrieved August 16, 2010, from <http://www.scu.edu.au/schools/gcm/ar/arp/actlearn.html>

Dikaiakos, M. D., Katsaros, D., Mehra, P., Pallis, G., Vakali, A. (2009). Cloud computing: distributed internet computing for IT and scientific research. *IEEE Internet Computing*, 13(5), 10-13. doi: 10.1109/MIC.2009.103

Frowen, A. (2011). *Cloud computing and computer forensics*. Retrieved April 5, 2011 from <http://www.articlesnatch.com/Article/Cloud-Computing-And-Computer-Forensics/663389>

Gartner. (2010). *Gartner analysts*. Retrieved March 25, 2011 from  
<http://www.gartner.com/technology/analysts.jsp>

Giurgiu, I., Riva, O., Juric, D., Krivulev, I., & Alonso, G. (2009). Calling the Cloud: Enabling mobile phones as interfaces to Cloud applications. *Proceedings of the 10<sup>th</sup> ACM/IFIP/USENIX International Conference on Middleware*. Retrieved from  
<http://www.springerlink.com/content/d654l77h78263602/>

Grobauer, B., & Schreck, T. (2010, October). Towards incident handling in the Cloud: Challenges and approaches. *Proceedings of the 2010 ACM workshop on Cloud computing security*. doi: 10.1145/1866835.1866850

- Holz, H., Applin, A., Haberman, B., Joyce, D., Purchase, H., & Reed, C. (2006). Research methods in computing: what are they, and how should we teach them? *Proceeding of the ITiCSE – WGR '06 Working group reports on ITiCSE on Innovation and technology in computer science education*. doi: 10.1145/1189215.1189180
- Hoog, A., & Strzempka, K. ( 2010). Independent research and reviews of iPhone forensic tools. *ViaForensics Innovative digital forensics and Security*. [Press release]. Retrieved from <http://viaforensics.com/edcation/white-papers/iphone-Forensics>
- Irwin, D. & Hunt, R. (2009). Forensic information acquisition in mobile networks. *Proceedings of 2009 IEEE Pacific Rim Conference on Communications Computers and Signal Processing*. doi: 10.1109/PACRIM.2009.5291378
- Jansen, W., & Ayers, R. (2007). Guidelines on cell phone forensics. *National Institute of Standards and Technology, Special Publication 800-101*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>
- JUNIPER Research. (2011). *Press release: Security threats to mobile devices increase but only 4% of Smartphones and tablets protected with security software, Juniper report finds*. Retrieved June 25, 2011 from <http://juniperresearch.com/viewpressrelease.php?pr=247>
- Keisler, P. D., Daley, C. K., & Hagy, D. W. (2007, October). Investigative uses of technology: Devices, tools, and techniques. *National Institute of Justice Special Report*. Retrieved March 20, from <http://www.ncjrs.gov/pdffiles1/nij/213030.pdf>



- Kemmis, S. (1988). Action Research in Retrospect and Prospect. In S. Kemmis & R. McTaggart (Eds.), *The action research reader* (3rd ed., pp. 27-39). Geelong, Australia: Deakin University Press.
- Klein, A., Mannweiler, C., Schneider, J., & Schotten, H. D. (2010). Access schemes for mobile Cloud computing. *2010 Eleventh International Conference on Mobile Data Management*. doi: 10.1109/MDM.2010.79
- Lawton, G. (2011). *Cloud computing crime poses unique forensics challenges*. Retrieved May 5, 2011 from <http://searchCloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges>
- Lessard, J. & Kessler, G. C. (2010). Android forensics: Simplifying cell phone examinations. *Small Scale Digital Device Forensics Journal*, 4(1), 1-12. Retrieved from [http://www.ssddfj.org/papers/SSDDFJ\\_V4\\_1\\_Lessard\\_Kessler.pdf](http://www.ssddfj.org/papers/SSDDFJ_V4_1_Lessard_Kessler.pdf)
- Levinson, A., Stackpole, B., & Johnson, D. (2011). Third party application forensics on apple mobile devices. *Proceedings of 2011 44<sup>th</sup> Hawaii International Conference on System Sciences*. doi: 10.1109/HICSS.2011.440
- Liu, Q., Jian, X., Hu, J., Zhao, H. & Zhang, S. (2009). An optimized solution for mobile environment using mobile Cloud computing. *Proceedings of the 5<sup>th</sup> International Conference on Wireless Communications, Networking and Mobile Computine, WiCom '09*. doi: 10.1109/WICOM.2009.5302240
- McKemmish, R. (1999). What is forensic computing. *Australian Institute of Criminology Trends and Issues in Crime and Criminal Justice*. No. 118. Retrieved March from <http://isis.poly.edu/kulesh/forensics/ti118.pdf>

- Me, G. & Rossi, M. (2008, April). Internal forensic acquisition for mobile equipments. *Proceedings of the 2008 IEEE International Symposium on Parallel and Distributed Processing*. doi: 10.1109/IPDPS.2008.4536557
- Mell, P & Grance, T. (2009). Draft NIST working definition of Cloud computing (draft). *National Institute of Standards and Technology, Special Publication 800-145 (draft)*. Retrieved from [http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145\\_Cloud-definition.pdf](http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_Cloud-definition.pdf)
- Morrill, D. (2010). *10 things to think about with Cloud computing and forensics*. Retrieved January 10, 2011 from <http://www.Cloudave.com/670/10-things-to-think-about-with-Cloud-computing-and-forensics>
- Morrissey, S. (2010). *iOS forensic analysis for iPhone, iPad and iPod touch*. Retrieved from <http://www.apress.com/info/bulksales>
- MSAB. (2011). *Release notes Xry 5.6*. Retrieved June, 24, 2011, from <http://www.pdfwindows.com/pdf/release-notes-xry-version-5-0/>
- NetQin. (2010a). *Mobile banking apps may be vulnerable: Testing and results*. Retrieved March 25, 2011 from [http://www.netqin.com/en/security/newsinfo\\_3548\\_3.html](http://www.netqin.com/en/security/newsinfo_3548_3.html)
- NetQin. (2010b). “手机僵尸”, “给你米” 领衔2010十大手机病毒 [translated: “Zombie phones,” “give you rice,” led 2010’s top ten mobile phone virus. Retrieved January 14, 2011 from <http://www.netqin.com/security/securityinfo.jsp?id=3584&type=2>
- NetQin (2010c). *70% of mobile users do not use encryption of their mobile devices*. Retrieved March 20, 2011, from [http://www.netqin.com/en/security/newsinfo\\_3583\\_3.html](http://www.netqin.com/en/security/newsinfo_3583_3.html)

NetQin. (2011a). *Mobile app growth challenges IT managers in 2011: Survey*.

Retrieved June 20, 2011 from

[http://www.netqin.com/en/security/newsinfo\\_4266\\_3.html](http://www.netqin.com/en/security/newsinfo_4266_3.html)

NetQin. (2011b). *Growing conflict between IT and mobility*. Retrieved June 1,

2011 from [http://www.netqin.com/en/security/newsinfo\\_4094\\_3.html](http://www.netqin.com/en/security/newsinfo_4094_3.html)

NetQin. (2011c). *Android virus*. Retrieved March 20, 2011 from

<http://virus.netqin.com/en/android/BIT.GeNiMi.A/>

NetQin (2011d). *Android virus*. Retrieved March 20, 2011 from

<http://virus.netqin.com/en/android/BIT.GeNiMi.D/>

Nicopolitidis, p., Obaidat, M. S., Papadimitriou, G. I. & Pomportsis. S. (2003).

*Wireless networks*. Chichester, England: John Wiley & Sons, Ltd

O'Brien, R. (1998). *An overview of the methodological approach of action*

*research*. Retrieved from <http://www.web.net/~robrien/papers/arfinal.doc>

ORACLE. (2009, August). Architectural strategies for Cloud computing. *An*

*Oracle White Paper in Enterprise Architecture*. Retrieved March 15, 2010

from <http://www.oracle.com/technetwork/topics/entarch/architectural-strategies-for-Cloud--128191.pdf>

Oxygen Forensic Suite. (2011). *Android rooting add-on*. Retrieved June 15, 2011

from <http://www.oxygen-forensic.com/en/features/androidroot/>

Perez, S. (2009). *Why Cloud computing is the future of mobile*. Retrieved August

25, 2010 from

[http://www.readwriteweb.com/archives/why\\_Cloud\\_computing\\_is\\_the\\_future\\_of\\_mobile.php](http://www.readwriteweb.com/archives/why_Cloud_computing_is_the_future_of_mobile.php)

- Poulsen, K (2010). *Spam suspect uses google docs; FBI happy*. Retrieved January 24, 2011 from <http://www.wired.com/threatlevel/2010/04/Cloud-warrant/>
- Raghav, S., & Saxena, A. K. (2009). Mobile forensics: Guidelines and challenges in data preservation and acquisition. *Proceedings of 2009 IEEE Student Conference on Research and Development*.  
doi: 10.1109/SCORED.2009.5443431
- Reilly, D., Wren, C., & Berry, T. (2011) Cloud computing: Pros and Cons for computer forensic investigations. *International Journal Multimedia and Image Processing*, 1(1), 26-34. Retrieved from [http://www.infonomics-society.org/IJMIP/Cloud%20Computing\\_Pros%20and%20Cons%20for%20Computer%20Forensic%20Investigations.pdf](http://www.infonomics-society.org/IJMIP/Cloud%20Computing_Pros%20and%20Cons%20for%20Computer%20Forensic%20Investigations.pdf)
- Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011, January). *Cloud forensics: An overview*. Paper presented at the 7<sup>th</sup> IFIP International Conference on Digital Forensics in Orlando, Florida, USA. Retrieved from [http://Cloudforensicsresearch.org/publication/Cloud\\_Forensics\\_An\\_Overview\\_7th\\_IFIP.pdf](http://Cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf)
- Satyanarayanan, M., Bahl, P., Caceres, R., & Davies, N. (2010). The case for VM-based Cloudlets in mobile computing. *IEEE Pervasive computing*, 8(4), 14-23. doi: [10.1109/MPRV.2009.82](https://doi.org/10.1109/MPRV.2009.82)
- Shukla, G. (2011). *Google wallet debuts, promises a wallet-free future*. Retrieved January 25, 2011 from <http://androidos.in/2011/05/google-wallet/>
- Sun Microsystems. (2009). *Introduction to Cloud computing architecture – White Paper. 1<sup>st</sup> Edition*. Retrieved from <http://www.eresearch.wiki.otago.ac.nz/images/7/75/Cloudcomputing.pdf>
- Tanwar, D. (2010). *Kaspersky detects first SMS Trojan for Smartphones running android*. Retrieved from March 25, 2011 from

<http://www.softwaretop100.org/kaspersky-detects-first-sms-trojan-for-smartphones-running-android>

Thia, T. (2010). *Next-gen banking Trojans hit APAC*. Retrieved March 25, 2011 from <http://www.zdnetasia.com/next-gen-banking-trojans-hit-apac-62204879.htm>

Turnbull, B., & Slay, J. (2008). WiFi network signals as a source of digital evidence: Wireless network forensics. *Proceedings of 2008 Third International Conference on Availability, Reliability and Security*. Retrieved from <http://www.computer.org/portal/web/csdl/doi/10.1109/ARES.2008.135>

Varshney, U., & Jain, R. (2001). Issues in emerging 4G wireless networks. *Computer*, 24(6), 94 – 96. doi: 10.1109/2.953469

Wang, Q., & Deters, R. (2009, October). SOA's last mile connecting Smartphones to the service Cloud. *Proceedings of Cloud'09 IEEE International Conference on Cloud Computing*. doi: 10.1109/CLOUD.2009.73

Westman, M. (2009). Complete mobile phones forensic examination: Why we need both logical & physical extractions. *Mobile Forensics World 2009 Conference*. Retrieved from [http://www.mobileforensicsworld.org/2009/presentations/MFW2009\\_Westman\\_LogicalandPhysicalExtractions.pdf](http://www.mobileforensicsworld.org/2009/presentations/MFW2009_Westman_LogicalandPhysicalExtractions.pdf)

Williamson, B., Apeldoorn, P., Cheam, B., & McDonald, M. (2006). *Forensic analysis of the contents of Nokia mobile phones*. Retrieved August 21, 2010 from [http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1035&context=adf&sei-redir=1#search="Forensic+analysis+of+the+contents+of+Nokia+mobile+phones"](http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1035&context=adf&sei-redir=1#search=)

Windows Live. (2011). *What happened in the recent Hotmail outage*. Retrieved June 25, 2011 from [http://windowsteamblog.com/windows\\_live/b/windowslive/archive/2011/01/06/what-happened-in-the-recent-hotmail-outage.aspx](http://windowsteamblog.com/windows_live/b/windowslive/archive/2011/01/06/what-happened-in-the-recent-hotmail-outage.aspx)

Wolthusen, S. D. (2009). Overcast: Forensic discovery in Cloud environments. *2009 Fifth International Conference on IT Security Incident Management and IT Forensics*. doi 10.1109/IMF.2009.21

Zareen, A., & Baig, S. (2010). Mobile phone forensics challenges, analysis and tools classification. *Fifth IEEE International Workshop on Systematic Approaches to digital Forensic Engineering*. doi:10.1109/SADFE.2010.24

Zhang, X., Schiffman, J., Gibbs, S., Kunjithapatham, A., & Jeong, S. (2009, November). Securing elastic applications on mobile devices for Cloud computing. *Proceddings of the 2009 ACM Workshop on Cloud Computing Security*. doi. 10.1145/1655008.1655026

## **Appendix A**

### **Motorola Milestone XRY Extraction Logs**

**(Disclaimer: Due to privacy issues, some of the data has been blacked out)**

## Summary

Summary and history of this report

Date Created: 4/22/2011 9:31:52 AM

Locked: No

XRY Version: 5.2

Is Subset: No

Is Encrypted: No

## General Information

*General information about the device (13 items)*

Device Name: Motorola Milestone

SIM Status: Ready

Subscriber Id (IMSI): 530016602864488

SIM Identification (ICCID): 8964010509268644884

Network Code (from IMSI): 53001

Service Provider Name: vodafone NZ

Mobile Id (IMEI): 354635031884054

Manufacturer: MOTO\_RTES

Model: Milestone

Revision: 2.1-update1/SHOLS\_U2\_02.38.1/9184485

Device Clock: 4/22/2011 8:32:08 AM (+01:00)

PC Clock: 4/22/2011 9:32:06 AM (+12:00)

WiFi Address: a4:ed:4e:5a:a7:69

## SMS

*SMS messages sent or received from the device (20 items)*

Number: [REDACTED]

Message: [REDACTED]

Time: 1/31/2010 12:02:33 AM (UTC)

Storage: SIM

Index: 1

Service Center: [REDACTED]

Number: [REDACTED]

Message: [REDACTED]

For add-on info txt HELP to 756

Time: 2/5/2011 9:48:39 AM (UTC)

Storage: SIM

Index: 2

Service Center: [REDACTED]

Number: [REDACTED]

Message: [REDACTED]

Time: 2/7/2011 3:28:51 AM (UTC)



Storage: SIM  
Index: 3  
Service Center: +[REDACTED]

Number: +61418401625

Message: [REDACTED]  
[REDACTED]

Time: 7/17/2009 9:42:44 AM (UTC)

Storage: SIM

Index: 4

Service Center: [REDACTED]

Number: [REDACTED]

Message: [REDACTED]

Time: 2/7/2011 8:50:25 PM (UTC)

Storage: SIM

Index: 5

Service Center: [REDACTED]

Number: [REDACTED]

Message: [REDACTED]  
[REDACTED]

Time: 12/14/2009 4:59:03 AM (UTC)

Storage: SIM

Index: 6

Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 1/19/2011 9:00:05 PM (UTC)

Storage: SIM

Index: 7

Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 5/25/2010 10:58:28 PM (UTC)

Storage: SIM

Index: 8

Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 2/7/2011 8:52:37 PM (UTC)

Storage: SIM

Index: 9

Service Center: +6421601170

Number: +64211795707

Message: [REDACTED]  
[REDACTED]

Time: 12/14/2009 4:59:07 AM (UTC)

Storage: SIM

Index: 10

Service Center: +[REDACTED]

Number: +64211795707

Message: [REDACTED]

Time: 12/14/2009 4:59:11 AM (UTC)

Storage: SIM

Index: 11

Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 5/25/2010 11:38:09 PM (UTC)

Storage: SIM

Index: 12

Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 2/7/2011 8:55:59 PM (UTC)

Storage: SIM

Index: 13

Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 1/20/2011 4:29:16 AM (UTC)

Storage: SIM

Index: 14

Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 3/22/2011 10:33:00 PM (UTC)

Storage: SIM

Index: 15

Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 2/13/2010 9:57:36 AM (UTC)

Storage: SIM

Index: 16

Service Center: +852161646000

Number: [REDACTED]

Message: [REDACTED]

Time: 12/28/2009 9:23:06 AM (UTC)  
Storage: SIM  
Index: 17  
Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

67 Eban Ave  
Fri 7:30pm  
Time: 2/4/2010 9:51:38 AM (UTC)  
Storage: SIM  
Index: 18  
Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 1/21/2011 7:04:17 AM (UTC)  
Storage: SIM  
Index: 19  
Service Center: +6421601170

Number: [REDACTED]

Message: [REDACTED]

Time: 2/8/2011 4:39:15 AM (UTC)  
Storage: SIM  
Index: 20  
Service Center: +6421601170

## **Pictures**

*Pictures stored on the device or on removable media (0 items)*

## **Videos**

*Videos stored on the device or on removable media (1 items)*

Name: title.mp4  
Type: Mp4  
Size: 43.77 KB  
Path: F:\ilightr  
Storage: Removable Media  
Created: 4/21/2011 5:39:31 PM  
Modified: 4/21/2011 5:39:30 PM  
Accessed: 4/21/2011 12:00:00 AM

## **Documents**

*Documents and settings stored on the device or on removable media (8 items)*

File Name: video.xml

File Path: F:\PandaSpace\hotkey  
Size: 558 Bytes  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM

Storage: Removable Media  
Accessed: 4/21/2011 12:00:00 AM

File Name: theme.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.16 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/21/2011 12:00:00 AM

File Name: ring.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.39 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/21/2011 12:00:00 AM

File Name: game.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.38 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/21/2011 12:00:00 AM

File Name: wallpaper.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.19 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/21/2011 12:00:00 AM

File Name: soft.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.29 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/21/2011 12:00:00 AM

File Name: soft.xml

File Path: F:\PandaSpace\matchkey  
Size: 234.39 KB  
Type: Xml  
Created: 4/20/2011 9:25:59 AM  
Modified: 4/20/2011 9:25:58 AM  
Storage: Removable Media  
Accessed: 4/21/2011 12:00:00 AM

File Name: ndsoft.txt  
File Path: F:\ndcommplatform  
Size: 49 Bytes  
Type: Text  
Created: 4/21/2011 8:13:46 AM  
Modified: 4/21/2011 8:13:46 AM  
Storage: Removable Media  
Accessed: 4/21/2011 12:00:00 AM

### **Files**

*Files with unrecognized format stored on the device or on removable media (5 items)*

Name: .udstate  
Size: 16 Bytes  
Path: F:\  
Storage: Removable Media  
Created: 4/21/2011 5:25:41 PM  
Modified: 4/21/2011 5:25:40 PM  
Accessed: 4/21/2011 12:00:00 AM

Name: update.zip  
Size: 30.00 MB  
Path: F:\  
Storage: Removable Media  
Created: 1/23/2000 3:51:55 AM  
Modified: 3/30/2011 6:05:10 PM  
Accessed: 4/20/2011 12:00:00 AM

Name: .thumbdata3--1967290299  
Size: 11.90 KB  
Path: F:\dcim\thumbnails  
Storage: Removable Media  
Created: 4/21/2011 5:08:20 PM  
Modified: 4/21/2011 5:08:20 PM  
Accessed: 4/21/2011 12:00:00 AM

Name: .thumbdata3-1763508120  
Size: 0 Bytes  
Path: F:\dcim\thumbnails  
Storage: Removable Media  
Created: 4/21/2011 5:08:19 PM  
Modified: 4/21/2011 5:08:18 PM  
Accessed: 4/21/2011 12:00:00 AM

Name: 9lpandaspace\_for\_android\_v2.8\_6282.988878825835.apk

Size: 2.29 MB  
Path: F:\PandaSpace\apps  
Storage: Removable Media  
Created: 4/20/2011 9:29:01 AM  
Modified: 4/20/2011 9:29:00 AM  
Accessed: 4/20/2011 12:00:00 AM

### Device Overview

*Detailed information about this device (0 items)*

### Log

Log of extraction process created by XRY (67 items)

Index: 1  
Module: MAIN  
Status: Success  
Time: 9:31:52 AM  
Message: Initiating Process at 9:31

Index: 2  
Module: MAIN  
Status: Success  
Time: 9:31:52 AM  
Message: XRY Version 5.2

Index: 3  
Module: MAIN  
Status: Success  
Time: 9:31:52 AM  
Message: Selected views: [All]

Index: 4  
Module: MAIN  
Status: Success  
Time: 9:31:52 AM  
Message: Processing device [Motorola Milestone] connected to DummyPort []...

Index: 5  
Module: MAIN  
Status: Success  
Time: 9:31:52 AM  
Message: Starting process of ANDROID (5.1)

Index: 6  
Module: ANDROID  
Status: Success  
Time: 9:31:52 AM  
Message: Connecting

Index: 7  
Module: ANDROID  
Status: Success

Time: 9:32:06 AM  
Message: Connected

Index: 8  
Module: ANDROID  
Status: Success  
Time: 9:32:06 AM  
Message: Reading General Information

Index: 9  
Module: ANDROID  
Status: Success  
Time: 9:32:06 AM  
Message: Memory card state in relation to phone: "shared"

Index: 10  
Module: ANDROID  
Status: Success  
Time: 9:32:06 AM  
Message: Reading Contacts

Index: 11  
Module: ANDROID  
Status: Success  
Time: 9:32:08 AM  
Message: Reading Calls

Index: 12  
Module: ANDROID  
Status: Success  
Time: 9:32:08 AM  
Message: Reading SMS

Index: 13  
Module: ANDROID  
Status: Success  
Time: 9:32:08 AM  
Message: Reading SMS

Index: 14  
Module: ANDROID  
Status: Success  
Time: 9:32:10 AM  
Message: Reading Calendar

Index: 15  
Module: ANDROID  
Status: Success  
Time: 9:32:10 AM  
Message: Browser bookmark "Google" <http://www.google.com/>  
(visited 0 times)

Index: 16  
Module: ANDROID  
Status: Success

Time: 9:32:10 AM  
Message: Browser bookmark "Picasa"  
<http://picasaweb.google.com/m/viewer?source=androidclient>  
(visited 0 times)

Index: 17  
Module: ANDROID  
Status: Success  
Time: 9:32:10 AM  
Message: Browser bookmark "Yahoo!" <http://www.yahoo.com/>  
(visited 0 times)

Index: 18  
Module: ANDROID  
Status: Success  
Time: 9:32:10 AM  
Message: Browser bookmark "MSN" <http://www.msn.com/>  
(visited 0 times)

Index: 19  
Module: ANDROID  
Status: Success  
Time: 9:32:10 AM  
Message: Browser bookmark "MySpace"  
<http://www.myspace.com/> (visited 0 times)

Index: 20  
Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "Facebook"  
<http://www.facebook.com/> (visited 0 times)

Index: 21  
Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "Wikipedia"  
<http://www.wikipedia.org/> (visited 0 times)

Index: 22  
Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "eBay" <http://www.ebay.com/>  
(visited 0 times)

Index: 23  
Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "CNN"  
<http://www.cnn.com/index.html> (visited 0 times)

Index: 24



Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "NY Times"  
<http://www.nytimes.com/> (visited 0 times)

Index: 25  
Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "ESPN" <http://espn.com/> (visited 0 times)

Index: 26  
Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "Amazon" <http://www.amazon.com/> (visited 0 times)

Index: 27  
Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "Weather Channel"  
<http://www.weather.com/> (visited 0 times)

Index: 28  
Module: ANDROID  
Status: Success  
Time: 9:32:11 AM  
Message: Browser bookmark "BBC" <http://www.bbc.co.uk/> (visited 0 times)

Index: 29  
Module: ANDROID  
Status: Success  
Time: 9:32:12 AM  
Message: Disconnecting

Index: 30  
Module: ANDROID  
Status: Success  
Time: 9:32:23 AM  
Message: Kill command failed, code: 1

Index: 31  
Module: MAIN  
Status: Success  
Time: 9:32:26 AM  
Message: ANDROID (5.1) completed successfully

Index: 32  
Module: MAIN  
Status: Success

Time: 9:32:26 AM  
Message: Starting process of DISKSTOR (5.1)

Index: 33  
Module: DISKSTOR  
Status: Success  
Time: 9:32:26 AM  
Message: Connecting

Index: 34  
Module: DISKSTOR  
Status: Success  
Time: 9:32:26 AM  
Message: Analyzing F:\

Index: 35  
Module: DISKSTOR  
Status: Success  
Time: 9:32:26 AM  
Message: Reading .udstate

Index: 36  
Module: DISKSTOR  
Status: Success  
Time: 9:32:26 AM  
Message: Reading update.zip

Index: 37  
Module: DISKSTOR  
Status: Success  
Time: 9:32:52 AM  
Message: Analyzing F:\LOST.DIR

Index: 38  
Module: DISKSTOR  
Status: Success  
Time: 9:32:52 AM  
Message: Analyzing F:\dcim

Index: 39  
Module: DISKSTOR  
Status: Success  
Time: 9:32:52 AM  
Message: Analyzing F:\dcim\thumbnails

Index: 40  
Module: DISKSTOR  
Status: Success  
Time: 9:32:52 AM  
Message: Reading .thumbdata3--1967290299

Index: 41  
Module: DISKSTOR  
Status: Success  
Time: 9:32:52 AM

Message: Reading .thumbdata3-1763508120

Index: 42  
Module: DISKSTOR  
Status: Success  
Time: 9:32:53 AM  
Message: Reading 1303405700842.jpg

Index: 43  
Module: DISKSTOR  
Status: Success  
Time: 9:32:53 AM  
Message: Analyzing F:\dcim\Camera

Index: 44  
Module: DISKSTOR  
Status: Success  
Time: 9:32:53 AM  
Message: Reading 2000-01-22\_10-09-50\_543.jpg

Index: 45  
Module: DISKSTOR  
Status: Success  
Time: 9:32:53 AM  
Message: Analyzing F:\.quickoffice

Index: 46  
Module: DISKSTOR  
Status: Success  
Time: 9:32:53 AM  
Message: Analyzing F:\.quickoffice\temp

Index: 47  
Module: DISKSTOR  
Status: Success  
Time: 9:32:53 AM  
Message: Analyzing F:\PandaSpace

Index: 48  
Module: DISKSTOR  
Status: Success  
Time: 9:32:53 AM  
Message: Analyzing F:\PandaSpace\hotkey

Index: 49  
Module: DISKSTOR  
Status: Success  
Time: 9:32:53 AM  
Message: Reading video.xml

Index: 50  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Reading theme.xml

Index: 51  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Reading ring.xml

Index: 52  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Reading game.xml

Index: 53  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Reading wallpaper.xml

Index: 54  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Reading soft.xml

Index: 55  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Analyzing F:\PandaSpace\matchkey

Index: 56  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Reading soft.xml

Index: 57  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Analyzing F:\PandaSpace\apps

Index: 58  
Module: DISKSTOR  
Status: Success  
Time: 9:32:54 AM  
Message: Reading  
9lpandaspace\_for\_android\_v2.8\_6282.988878825835.apk

Index: 59  
Module: DISKSTOR  
Status: Success  
Time: 9:32:56 AM  
Message: Analyzing F:\Playlists

Index: 60  
Module: DISKSTOR  
Status: Success  
Time: 9:32:56 AM  
Message: Analyzing F:\Albums

Index: 61  
Module: DISKSTOR  
Status: Success  
Time: 9:32:56 AM  
Message: Analyzing F:\ndcommplatform

Index: 62  
Module: DISKSTOR  
Status: Success  
Time: 9:32:56 AM  
Message: Reading ndsoft.txt

Index: 63  
Module: DISKSTOR  
Status: Success  
Time: 9:32:56 AM  
Message: Analyzing F:\ndcommplatform\preference

Index: 64  
Module: DISKSTOR  
Status: Success  
Time: 9:32:56 AM  
Message: Analyzing F:\ilightr

Index: 65  
Module: DISKSTOR  
Status: Success  
Time: 9:32:56 AM  
Message: Reading title.mp4

Index: 66  
Module: DISKSTOR  
Status: Success  
Time: 9:32:56 AM  
Message: Disconnecting

Index: 67  
Module: MAIN  
Status: Success  
Time: 9:32:56 AM  
Message: DISKSTOR (5.1) completed successfully

## **Appendix B**

### **Motorola Milestone Rooting Procedures**

### **Hardware requirements**

- Motorola Milestone
- Connection cable
- Computer running XP operating system

### **Software requirements**

- Motorola Mobile Phone USB Driver
- RSD Lite 4.6
- vulnerable\_recovery\_only\_RAMDLD90\_78.sbf (Vulnerable Recovery SBF (CG47) for mobile with bootloader RAMDLD 90.78 and lower)
- GOT OpenRecovery

### **Action**

- Installed Motorola Mobile Phone USB Driver and RSD Lite 4.6 on the computer.
- Chose First-Come-First-Serve DeviceID Mode from the Config menu and ran RSD Lite 4.6
- Connected Motorola Milestone via cable.
- Extracted GOT OpenRecovery.zip; there were two files in the update.zip and open recovery folder. All the files in the mobile SD card were copied.
- The Vulnerable Recovery SBF file was loaded into the RSD Lite 4.6 system. See figure 1.
- Clicked Start.
- Figure 2 shows the Vulnerable Recovery SBF file was successfully verified.
- Turned off the device.
- Pressed and held X key and Power key until the recovery mood screen came up.
- Pressed camera button and upper volume key, this lead to the recovery menu.
- Chose update.zip option, which lead to the GOT Menu.

- Selected root for the phone
- Selected Nandroid and created a Nandroid backup.
- Rooting was completed.

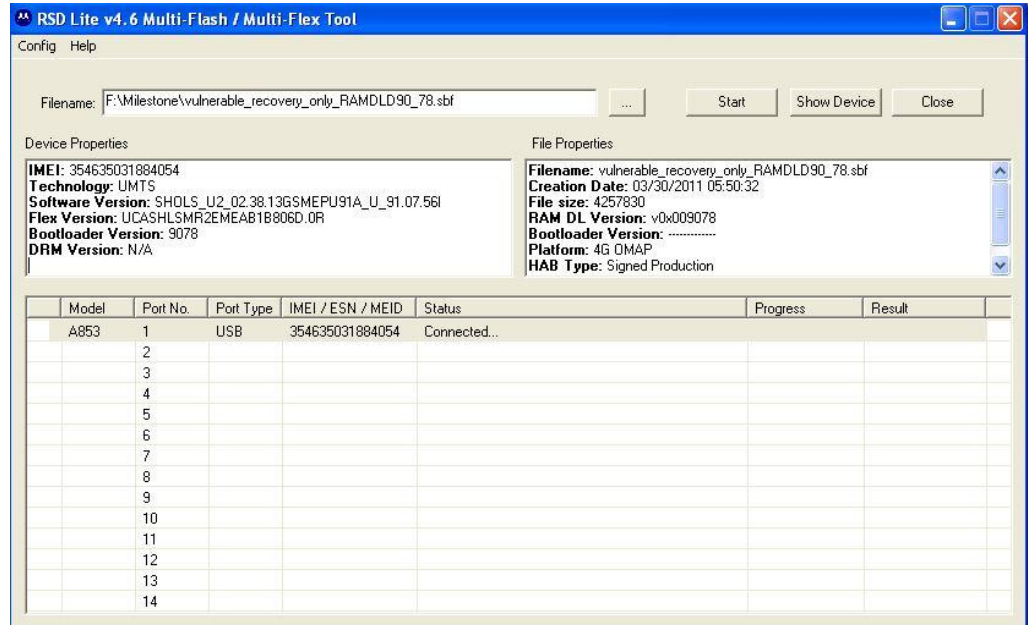


Figure 1: RSD Lite 4.6

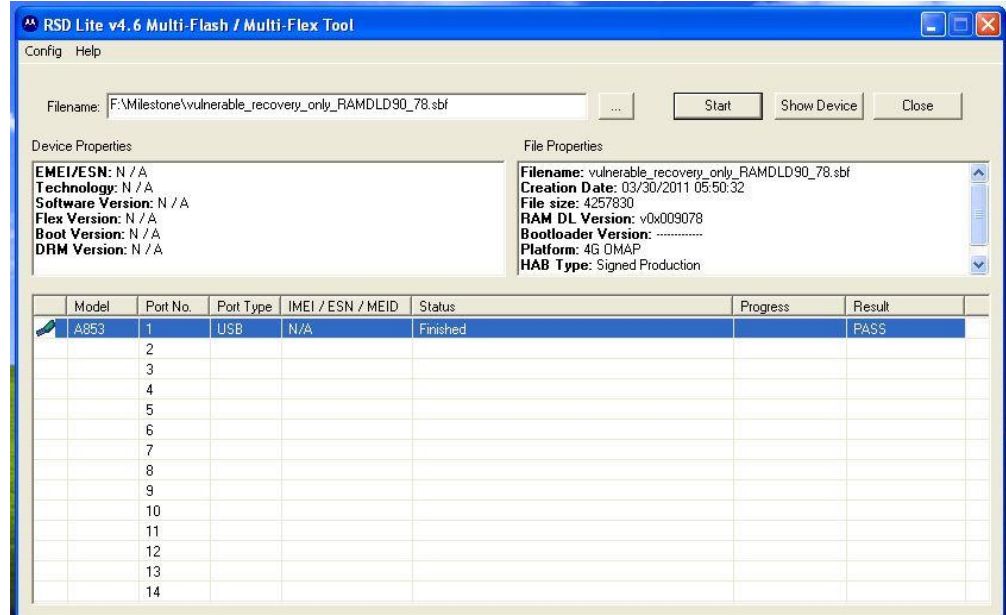


Figure 2 : Vulnerable recovery SBF file is successfully verified.



**Appendix C**

**Motorola Milestone XRY Extraction Logs**  
**after Rooting**

## Summary

*Summary and history of this report*

Date Created: 4/22/2011 11:31:52 PM

Locked: No

XRY Version: 5.2

Is Subset: No

Is Encrypted: No

## SMS

*SMS messages sent or received from the device (20 items)*

Number: [REDACTED]

Message: [REDACTED]

Time: 1/31/2010 12:02:33 AM (UTC)

Storage: SIM

Index: 1

Service Center: [REDACTED]

Number: [REDACTED]

Message: [REDACTED]

For add-on info txt HELP to 756

Time: 2/5/2011 9:48:39 AM (UTC)

Storage: SIM

Index: 2

Service Center: [REDACTED]

Number: [REDACTED]

Message: [REDACTED]

Time: 2/7/2011 3:28:51 AM (UTC)

Storage: SIM

Index: 3

Service Center: +[REDACTED]

Number: +61418401625

Message: [REDACTED]

Time: 7/17/2009 9:42:44 AM (UTC)

Storage: SIM

Index: 4

Service Center: [REDACTED]

Number: [REDACTED]  
Message: [REDACTED]  
Time: 2/7/2011 8:50:25 PM (UTC)  
Storage: SIM  
Index: 5  
Service Center: [REDACTED]

Number: [REDACTED]  
Message: [REDACTED]  
Time: 12/14/2009 4:59:03 AM (UTC)  
Storage: SIM  
Index: 6  
Service Center: +6421601170

Number: [REDACTED]  
Message: [REDACTED]  
Time: 1/19/2011 9:00:05 PM (UTC)  
Storage: SIM  
Index: 7  
Service Center: +6421601170

Number: [REDACTED]  
Message: [REDACTED]  
Time: 5/25/2010 10:58:28 PM (UTC)  
Storage: SIM  
Index: 8  
Service Center: +6421601170

Number: [REDACTED]  
Message: [REDACTED]  
Time: 2/7/2011 8:52:37 PM (UTC)  
Storage: SIM  
Index: 9  
Service Center: +6421601170

Number: +64211795707  
Message: [REDACTED]  
Time: 12/14/2009 4:59:07 AM (UTC)  
Storage: SIM  
Index: 10  
Service Center: +[REDACTED]

Number: +64211795707  
Message: [REDACTED]  
Time: 12/14/2009 4:59:11 AM (UTC)  
Storage: SIM  
Index: 11  
Service Center: +6421601170

Number: [REDACTED]

Message:

Time: 5/25/2010 11:38:09 PM (UTC)

Storage: SIM

Index: 12

Service Center: +6421601170

Number:

Message:

Time: 2/7/2011 8:55:59 PM (UTC)

Storage: SIM

Index: 13

Service Center: +6421601170

Number:

Message:

Time: 1/20/2011 4:29:16 AM (UTC)

Storage: SIM

Index: 14

Service Center: +6421601170

Number:

Message:

Time: 3/22/2011 10:33:00 PM (UTC)

Storage: SIM

Index: 15

Service Center: +6421601170

Number:

Message:

Time: 2/13/2010 9:57:36 AM (UTC)

Storage: SIM

Index: 16

Service Center: +852161646000

Number:

Message:

Time: 12/28/2009 9:23:06 AM (UTC)

Storage: SIM

Index: 17

Service Center: +6421601170

Number:

Message:

67 Eban Ave

Fri 7:30pm

Time: 2/4/2010 9:51:38 AM (UTC)

Storage: SIM

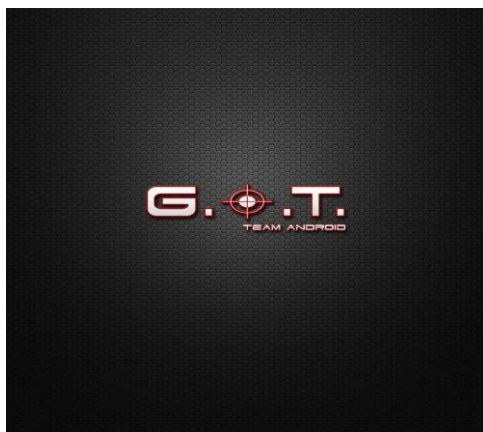
Index: 18  
Service Center: +6421601170

Number: [REDACTED]  
Message: [REDACTED]  
Time: 1/21/2011 7:04:17 AM (UTC)  
Storage: SIM  
Index: 19  
Service Center: +6421601170

Number: [REDACTED]  
Message: [REDACTED]  
Time: 2/8/2011 4:39:15 AM (UTC)  
Storage: SIM  
Index: 20  
Service Center: +6421601170

#### Pictures

*Pictures stored on the device or on removable media (17 items)*



Name: wallpaper  
Type: Png  
Size: 737.00 KB  
MetaData: DateTime: 2010:06:15 00:33:36  
Path: F:\OpenRecovery\GOT  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/15/2010 2:33:36 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: icon\_error.png  
Type: Png  
Size: 400.38 KB  
MetaData: PixelUnit: 1  
PixelPerUnitX: 2834  
PixelPerUnitY: 2834  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/14/2010 9:20:24 PM  
Accessed: 4/22/2011 12:00:00 AM



Name: icon\_firmware\_error.png  
Type: Png  
Size: 7.90 KB  
MetaData: PixelUnit: 1  
PixelPerUnitX: 2834  
PixelPerUnitY: 2834  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/10/2010 11:08:04 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: icon\_firmware\_install.png  
Type: Png  
Size: 0 Bytes  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media

Created: 4/22/2011 10:54:29 PM  
Modified: 6/10/2010 9:52:28 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: icon\_installing.png  
Type: Png  
Size: 19.23 KB  
MetaData: SoftwareUsed: Adobe ImageReady  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/9/2010 10:07:40 PM  
Accessed: 4/22/2011 12:00:00 AM



Name: indeterminatel.png  
Type: Png  
Size: 2.20 KB  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: indeterminate2.png  
Type: Png  
Size: 2.20 KB  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: indeterminate3.png  
Type: Png  
Size: 2.20 KB  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: indeterminate4.png

Type: Png  
Size: 2.20 KB  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: indeterminate5.png  
Type: Png  
Size: 2.19 KB  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: indeterminate6.png  
Type: Png  
Size: 2.21 KB  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: progress\_bar\_empty.png  
Type: Png  
Size: 148 Bytes  
MetaData: PixelUnit: 1  
PixelPerUnitX: 2834  
PixelPerUnitY: 2834  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: progress\_bar\_empty\_left\_round.png  
Type: Png  
Size: 220 Bytes  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM



Name: progress\_bar\_empty\_right\_round.png  
Type: Png



Size: 211 Bytes  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: progress\_bar\_fill.png  
Type: Png  
Size: 117 Bytes  
MetaData: PixelUnit: 1  
PixelPerUnitX: 2834  
PixelPerUnitY: 2834  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: progress\_bar\_left\_round.png  
Type: Png  
Size: 195 Bytes  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: progress\_bar\_right\_round.png  
Type: Png  
Size: 192 Bytes  
Path: F:\OpenRecovery\res\images  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/29/2010 5:22:40 AM  
Accessed: 4/22/2011 12:00:00 AM

## Videos

*Videos stored on the device or on removable media (1 items)*

Name: title.mp4  
Type: Mp4  
Size: 43.77 KB  
Path: F:\ilightr  
Storage: Removable Media  
Created: 4/22/2011 9:53:24 PM  
Modified: 4/22/2011 9:53:24 PM  
Accessed: 4/24/2011 12:00:00 AM

## Documents

*Documents and settings stored on the device or on removable media (9 items)*

File Name: readme.txt  
File Path: F:\OpenRecovery\GOT\bin\boot\_script  
Size: 78 Bytes  
Type: Text  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/14/2010 6:30:38 PM  
Storage: Removable Media  
Accessed: 4/22/2011 12:00:00 AM

File Name: video.xml  
File Path: F:\PandaSpace\hotkey  
Size: 558 Bytes  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/22/2011 12:00:00 AM

File Name: theme.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.16 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/22/2011 12:00:00 AM

File Name: ring.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.39 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/22/2011 12:00:00 AM

File Name: game.xml

File Path: F:\PandaSpace\hotkey  
Size: 3.38 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/22/2011 12:00:00 AM

File Name: wallpaper.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.19 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/22/2011 12:00:00 AM

File Name: soft.xml  
File Path: F:\PandaSpace\hotkey  
Size: 3.29 KB  
Type: Xml  
Created: 4/20/2011 9:25:43 AM  
Modified: 4/20/2011 9:25:42 AM  
Storage: Removable Media  
Accessed: 4/22/2011 12:00:00 AM

File Name: soft.xml  
File Path: F:\PandaSpace\matchkey  
Size: 234.39 KB  
Type: Xml  
Created: 4/20/2011 9:25:59 AM  
Modified: 4/20/2011 9:25:58 AM  
Storage: Removable Media  
Accessed: 4/22/2011 12:00:00 AM

File Name: ndsoft.txt  
File Path: F:\ndcommplatform

Size: 49 Bytes

Type: Text

Created: 4/21/2011 8:13:46 AM

Modified: 4/21/2011 8:13:46 AM

Storage: Removable Media

Accessed: 4/22/2011 12:00:00 AM

## **Files**

*Files with unrecognized format stored on the device or on removable media (112 items)*

Name: update.zip

Size: 12.87 MB

Path: F:\

Storage: Removable Media

Created: 4/22/2011 10:54:22 PM

Modified: 7/14/2010 3:50:44 PM

Accessed: 4/22/2011 12:00:00 AM

Name: .thumbdata3--1967290299

Size: 0 Bytes

Path: F:\dcim\thumbnails

Storage: Removable Media

Created: 4/24/2011 9:28:29 AM

Modified: 4/24/2011 9:28:28 AM

Accessed: 4/24/2011 12:00:00 AM

Name: .thumbdata3-1763508120

Size: 0 Bytes

Path: F:\dcim\thumbnails

Storage: Removable Media

Created: 4/24/2011 9:28:29 AM

Modified: 4/24/2011 9:28:28 AM

Accessed: 4/24/2011 12:00:00 AM

Name: boot.img

Size: 3.50 MB

Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105

Storage: Removable Media

Created: 4/22/2011 9:05:12 PM

Modified: 4/22/2011 9:05:12 PM

Accessed: 4/22/2011 12:00:00 AM

Name: misc.img

Size: 384.00 KB

Path: F:\nandroid\adbrecovery\BwCcDMS-20110422-2105

Storage: Removable Media

Created: 4/22/2011 9:05:15 PM

Modified: 4/22/2011 9:05:14 PM

Accessed: 4/22/2011 12:00:00 AM

Name: bpsw.img  
Size: 3.75 MB  
Path: F:\nandroid\adbrecovey\BwCcDMS-20110422-2105  
Storage: Removable Media  
Created: 4/22/2011 9:05:17 PM  
Modified: 4/22/2011 9:05:16 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: system.img  
Size: 153.91 MB  
Path: F:\nandroid\adbrecovey\BwCcDMS-20110422-2105  
Storage: Removable Media  
Created: 4/22/2011 9:05:47 PM  
Modified: 4/22/2011 9:05:46 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: data.img  
Size: 43.26 MB  
Path: F:\nandroid\adbrecovey\BwCcDMS-20110422-2105  
Storage: Removable Media  
Created: 4/22/2011 9:05:58 PM  
Modified: 4/22/2011 9:05:58 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: cache.img  
Size: 26.81 KB  
Path: F:\nandroid\adbrecovey\BwCcDMS-20110422-2105  
Storage: Removable Media  
Created: 4/22/2011 9:05:59 PM  
Modified: 4/22/2011 9:05:58 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: cust.img  
Size: 259.88 KB  
Path: F:\nandroid\adbrecovey\BwCcDMS-20110422-2105  
Storage: Removable Media  
Created: 4/22/2011 9:05:59 PM  
Modified: 4/22/2011 9:05:58 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: nandroid.md5  
Size: 304 Bytes  
Path: F:\nandroid\adbrecovey\BwCcDMS-20110422-2105  
Storage: Removable Media  
Created: 4/22/2011 9:06:15 PM  
Modified: 4/22/2011 9:06:14 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: ext2.ko  
Size: 839.82 KB  
Path: F:\OpenRecovery\app2sd\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 4/22/2010 10:35:52 AM

Accessed: 4/22/2011 12:00:00 AM

Name: mot\_boot\_mode  
Size: 137 Bytes  
Path: F:\OpenRecovery\app2sd\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/11/2010 9:13:38 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: parted  
Size: 338.55 KB  
Path: F:\OpenRecovery\app2sd\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 4/22/2010 2:36:50 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: 51\_app2sd.sh  
Size: 180 Bytes  
Path: F:\OpenRecovery\app2sd\bin\boot\_script  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/10/2010 3:24:30 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: 51\_app2sd\_sl.sh  
Size: 315 Bytes  
Path: F:\OpenRecovery\app2sd\bin\boot\_script  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/10/2010 3:25:56 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: .nobashcolors  
Size: 0 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/10/2010 8:02:56 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: adbd\_start.sh  
Size: 23 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 5/7/2010 4:47:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: adbd\_stop.sh  
Size: 96 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM

Modified: 4/2/2010 1:01:52 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: app2sd.sh  
Size: 7.50 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/10/2010 3:45:38 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: bash\_disable\_colors.sh  
Size: 162 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/6/2010 10:10:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: bash\_enable\_colors.sh  
Size: 161 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/6/2010 10:09:46 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: build.sh  
Size: 1.87 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/13/2010 12:11:18 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: busybox.sh  
Size: 1.16 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/20/2010 9:16:12 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: change\_keyboard\_layout.sh  
Size: 386 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:23:56 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: enable\_adb\_usbmode.sh  
Size: 48 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media

Created: 4/22/2011 10:54:28 PM  
Modified: 5/7/2010 1:07:08 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: flac.sh  
Size: 799 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/21/2010 11:55:34 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: init\_recovery.sh  
Size: 1.23 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/19/2010 11:27:38 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: jit.sh  
Size: 1.88 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/14/2010 4:51:14 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: memhack.sh  
Size: 814 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/21/2010 11:57:16 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_app2sd.sh  
Size: 520 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/13/2010 1:33:24 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_app2sd2.sh  
Size: 349 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/13/2010 1:32:48 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_bash.sh  
Size: 265 Bytes  
Path: F:\OpenRecovery\bin



Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/6/2010 10:06:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_busybox.sh  
Size: 338 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/21/2010 11:22:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_got.sh  
Size: 830 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/13/2010 12:06:28 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_keyboard\_layout.sh  
Size: 287 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:23:56 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_misc.sh  
Size: 336 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/14/2010 8:13:56 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_nandroid.sh  
Size: 400 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/11/2010 1:48:12 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_nandroid\_backup.sh  
Size: 506 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/6/2010 10:03:16 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_nandroid\_delete.sh  
Size: 279 Bytes

Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 5/30/2010 8:18:18 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_nandroid\_restore.sh  
Size: 297 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 5/30/2010 8:18:32 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_overclock.sh  
Size: 437 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/21/2010 11:27:44 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_restore.sh  
Size: 624 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/13/2010 12:05:34 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_scripts.sh  
Size: 388 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 5/30/2010 8:36:32 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: menu\_updates.sh  
Size: 426 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/9/2010 10:30:30 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: nandroid-delete\_adbrecovery.sh  
Size: 75 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/5/2010 9:55:18 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: nandroid-mobile\_adbrecovery.sh

Size: 69.03 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 5/11/2010 10:57:52 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: overclock.sh  
Size: 2.25 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 9:56:00 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: restore.sh  
Size: 1.90 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 7/13/2010 1:34:36 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: root.sh  
Size: 259 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/21/2010 1:17:04 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: scriptrunner  
Size: 89 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 5/31/2010 4:43:56 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: switch.sh  
Size: 2.45 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/10/2010 12:34:42 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: theme.sh  
Size: 2.10 KB  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/22/2010 12:07:26 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: wipe\_dalvik\_cache.sh  
Size: 79 Bytes  
Path: F:\OpenRecovery\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/6/2010 10:00:12 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: fstab  
Size: 929 Bytes  
Path: F:\OpenRecovery\etc  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/5/2010 12:17:26 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: profile  
Size: 941 Bytes  
Path: F:\OpenRecovery\etc  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/14/2010 9:07:56 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: AlarmClock.apk  
Size: 303.64 KB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: CalendarProvider.apk  
Size: 126.11 KB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: DownloadProvider.apk  
Size: 71.96 KB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: Facebook.apk  
Size: 1.51 MB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: GenieWidget.apk  
Size: 1.91 MB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: LatinIME.apk  
Size: 3.11 MB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: Launcher.apk  
Size: 1.67 MB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: Mms.apk  
Size: 715.62 KB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: Music.apk  
Size: 622.76 KB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: Phone.apk  
Size: 1.32 MB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: Settings.apk  
Size: 1.88 MB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM

Accessed: 4/22/2011 12:00:00 AM

Name: YouTube.apk  
Size: 855.74 KB  
Path: F:\OpenRecovery\GOT\apps  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: mot\_boot\_mode  
Size: 137 Bytes  
Path: F:\OpenRecovery\GOT\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/11/2010 9:13:38 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: mot\_boot\_mode.backup  
Size: 5.38 KB  
Path: F:\OpenRecovery\GOT\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/11/2010 6:55:14 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: 61\_memhack.sh  
Size: 272 Bytes  
Path: F:\OpenRecovery\GOT\bin\boot\_script  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/12/2010 11:03:46 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: 71\_overclock.sh  
Size: 170 Bytes  
Path: F:\OpenRecovery\GOT\bin\boot\_script  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/14/2010 8:46:38 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: Clockopia.ttf  
Size: 36.38 KB  
Path: F:\OpenRecovery\GOT\fonts  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: DroidSans-Bold.ttf  
Size: 36.38 KB  
Path: F:\OpenRecovery\GOT\fonts  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM

Modified: 6/25/2010 5:50:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: DroidSans.ttf  
Size: 36.38 KB  
Path: F:\OpenRecovery\GOT\fonts  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: framework-res.apk  
Size: 3.67 MB  
Path: F:\OpenRecovery\GOT\framework  
Storage: Removable Media  
Created: 4/22/2011 10:54:28 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: services.jar  
Size: 517.82 KB  
Path: F:\OpenRecovery\GOT\framework  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/25/2010 5:50:04 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: dalvikvm  
Size: 5.39 KB  
Path: F:\OpenRecovery\GOT\jit\system\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: dexopt  
Size: 9.52 KB  
Path: F:\OpenRecovery\GOT\jit\system\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: logcat  
Size: 9.54 KB  
Path: F:\OpenRecovery\GOT\jit\system\bin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: libcutils.so  
Size: 69.97 KB  
Path: F:\OpenRecovery\GOT\jit\system\lib  
Storage: Removable Media

Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: libdl.so  
Size: 9.01 KB  
Path: F:\OpenRecovery\GOT\jit\system\lib  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: libdvm.so  
Size: 767.36 KB  
Path: F:\OpenRecovery\GOT\jit\system\lib  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: liblog.so  
Size: 13.20 KB  
Path: F:\OpenRecovery\GOT\jit\system\lib  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: libm.so  
Size: 88.96 KB  
Path: F:\OpenRecovery\GOT\jit\system\lib  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: libnativehelper.so  
Size: 238.38 KB  
Path: F:\OpenRecovery\GOT\jit\system\lib  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: libz.so  
Size: 85.38 KB  
Path: F:\OpenRecovery\GOT\jit\system\lib  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/10/2010 7:58:22 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: overclock.ko  
Size: 11.73 KB  
Path: F:\OpenRecovery\GOT\lib\modules



Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 5/25/2010 9:31:24 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: framework.jar  
Size: 2.66 MB  
Path: F:\OpenRecovery\GOT\ocflac  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/16/2010 1:12:50 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: libFLAC.so  
Size: 78.70 KB  
Path: F:\OpenRecovery\GOT\ocflac  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/26/2010 1:45:28 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: libmediaplayerservice.so  
Size: 116.06 KB  
Path: F:\OpenRecovery\GOT\ocflac  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/26/2010 12:32:50 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: libopencore\_player.so  
Size: 785.53 KB  
Path: F:\OpenRecovery\GOT\ocflac  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/29/2010 3:49:10 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: busybox  
Size: 1009.87 KB  
Path: F:\OpenRecovery\GOT\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 4/22/2010 10:35:52 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: azerty  
Size: 896 Bytes  
Path: F:\OpenRecovery\keychars  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/25/2010 5:24:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: euro\_qwerty  
Size: 896 Bytes

Path: F:\OpenRecovery\keychars  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/25/2010 5:24:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: qwerty  
Size: 896 Bytes  
Path: F:\OpenRecovery\keychars  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/25/2010 5:24:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: qwertz  
Size: 896 Bytes  
Path: F:\OpenRecovery\keychars  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/25/2010 5:24:06 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: ext2.ko  
Size: 839.82 KB  
Path: F:\OpenRecovery\modules  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/5/2010 12:22:52 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: .nomedia  
Size: 0 Bytes  
Path: F:\OpenRecovery\res  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/14/2010 8:21:32 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: su  
Size: 21.61 KB  
Path: F:\OpenRecovery\root  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 5/16/2010 11:22:18 AM  
Accessed: 4/22/2011 12:00:00 AM

Name: Superuser.apk  
Size: 37.46 KB  
Path: F:\OpenRecovery\root  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 5/16/2010 6:09:40 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: adbd\_recovery

Size: 131.01 KB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/6/2010 1:17:56 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: bash  
Size: 1.45 MB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 6/7/2010 3:51:50 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: busybox  
Size: 1.63 MB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 4/22/2010 9:47:26 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: dump\_image-arm-uclibc  
Size: 47.56 KB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/16/2010 12:10:24 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: flash\_image-arm-uclibc  
Size: 47.87 KB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 1/26/2010 12:27:56 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: mkyaffs2image-arm-uclibc  
Size: 46.25 KB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/16/2010 12:10:24 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: open\_rcvr\_stone  
Size: 294.47 KB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 7/14/2010 3:52:28 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: toolbox  
Size: 156.30 KB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 5/7/2010 4:44:38 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: unyaffs-arm-uclibc  
Size: 34.18 KB  
Path: F:\OpenRecovery\sbin  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 3/16/2010 12:10:24 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: test.sh  
Size: 31 Bytes  
Path: F:\OpenRecovery\scripts  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 5/30/2010 10:20:48 PM  
Accessed: 4/22/2011 12:00:00 AM

Name: test-update-nosign.zip  
Size: 154.03 KB  
Path: F:\OpenRecovery\updates  
Storage: Removable Media  
Created: 4/22/2011 10:54:29 PM  
Modified: 5/1/2010 3:23:00 PM  
Accessed: 4/22/2011 12:00:00 AM

Log

*Log of extraction process created by XRY (207 items)*

Index: 1  
Module: MAIN  
Status: Success  
Time: 11:31:51 PM  
Message: Initiating Process at 23:31

Index: 2  
Module: MAIN  
Status: Success  
Time: 11:31:51 PM  
Message: XRY Version 5.2

Index: 3  
Module: MAIN  
Status: Success  
Time: 11:31:51 PM  
Message: Selected views: [All]

Index: 4

Module: MAIN  
Status: Success  
Time: 11:31:52 PM  
Message: Processing device [Motorola Milestone] connected to DummyPort []...

Index: 5  
Module: MAIN  
Status: Success  
Time: 11:31:52 PM  
Message: Starting process of ANDROID (5.1)

Index: 6  
Module: ANDROID  
Status: Success  
Time: 11:31:52 PM  
Message: Connecting

Index: 7  
Module: ANDROID  
Status: Success  
Time: 11:32:04 PM  
Message: Connected

Index: 8  
Module: ANDROID  
Status: Success  
Time: 11:32:04 PM  
Message: Reading General Information

Index: 9  
Module: ANDROID  
Status: Success  
Time: 11:32:04 PM  
Message: Memory card state in relation to phone: "shared"

Index: 10  
Module: ANDROID  
Status: Success  
Time: 11:32:04 PM  
Message: Reading Contacts

Index: 11  
Module: ANDROID  
Status: Success  
Time: 11:32:05 PM  
Message: Reading Calls

Index: 12  
Module: ANDROID  
Status: Success  
Time: 11:32:05 PM  
Message: Reading SMS

Index: 13

Module: ANDROID  
Status: Success  
Time: 11:32:06 PM  
Message: Reading SMS

Index: 14  
Module: ANDROID  
Status: Success  
Time: 11:32:08 PM  
Message: Reading Calendar

Index: 15  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "Google" <http://www.google.com/>  
(visited 0 times)

Index: 16  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "Picasa"  
<http://picasaweb.google.com/m/viewer?source=androidclient>  
(visited 0 times)

Index: 17  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "Yahoo!" <http://www.yahoo.com/>  
(visited 0 times)

Index: 18  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "MSN" <http://www.msn.com/>  
(visited 0 times)

Index: 19  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "MySpace"  
<http://www.myspace.com/> (visited 0 times)

Index: 20  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "Facebook"  
<http://www.facebook.com/> (visited 0 times)

Index: 21

Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "Wikipedia"  
<http://www.wikipedia.org/> (visited 0 times)

Index: 22  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "eBay" <http://www.ebay.com/>  
(visited 0 times)

Index: 23  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "CNN"  
<http://www.cnn.com/index.html> (visited 0 times)

Index: 24  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "NY Times"  
<http://www.nytimes.com/> (visited 0 times)

Index: 25  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "ESPN" <http://espn.com/> (visited  
0 times)

Index: 26  
Module: ANDROID  
Status: Success  
Time: 11:32:09 PM  
Message: Browser bookmark "Amazon" <http://www.amazon.com/>  
(visited 0 times)

Index: 27  
Module: ANDROID  
Status: Success  
Time: 11:32:10 PM  
Message: Browser bookmark "Weather Channel"  
<http://www.weather.com/> (visited 0 times)

Index: 28  
Module: ANDROID  
Status: Success  
Time: 11:32:10 PM  
Message: Browser bookmark "BBC" <http://www.bbc.co.uk/>  
(visited 0 times)

Index: 29  
Module: ANDROID  
Status: Success  
Time: 11:32:10 PM  
Message: Disconnecting

Index: 30  
Module: ANDROID  
Status: Success  
Time: 11:32:14 PM  
Message: Kill command failed, code: 1

Index: 31  
Module: MAIN  
Status: Success  
Time: 11:32:17 PM  
Message: ANDROID (5.1) completed successfully

Index: 32  
Module: MAIN  
Status: Success  
Time: 11:32:17 PM  
Message: Starting process of DISKSTOR (5.1)

Index: 33  
Module: DISKSTOR  
Status: Success  
Time: 11:32:17 PM  
Message: Connecting

Index: 34  
Module: DISKSTOR  
Status: Success  
Time: 11:32:17 PM  
Message: Analyzing F:\

Index: 35  
Module: DISKSTOR  
Status: Success  
Time: 11:32:17 PM  
Message: Reading update.zip

Index: 36  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\LOST.DIR

Index: 37  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\Playlists

Index: 38



Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\Albums

Index: 39  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\dcim

Index: 40  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\dcim\thumbnails

Index: 41  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Reading .thumbdata3--1967290299

Index: 42  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Reading .thumbdata3-1763508120

Index: 43  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\.quickoffice

Index: 44  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\.quickoffice\temp

Index: 45  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\nandroid

Index: 46  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\nandroid\adb recovery

Index: 47  
Module: DISKSTOR

Status: Success  
Time: 11:32:24 PM  
Message: Analyzing F:\nandroid\adbrecovey\BwCcDMS-  
20110422-2105

Index: 48  
Module: DISKSTOR  
Status: Success  
Time: 11:32:24 PM  
Message: Reading boot.img

Index: 49  
Module: DISKSTOR  
Status: Success  
Time: 11:32:22 PM  
Message: Reading misc.img

Index: 50  
Module: DISKSTOR  
Status: Success  
Time: 11:32:27 PM  
Message: Reading bpsw.img

Index: 51  
Module: DISKSTOR  
Status: Success  
Time: 11:32:29 PM  
Message: Reading system.img

Index: 52  
Module: DISKSTOR  
Status: Success  
Time: 11:34:00 PM  
Message: Reading data.img

Index: 53  
Module: DISKSTOR  
Status: Success  
Time: 11:34:26 PM  
Message: Reading cache.img

Index: 54  
Module: DISKSTOR  
Status: Success  
Time: 11:34:26 PM  
Message: Reading cust.img

Index: 55  
Module: DISKSTOR  
Status: Success  
Time: 11:34:26 PM  
Message: Reading nandroid.md5

Index: 56  
Module: DISKSTOR

Status: Success  
Time: 11:34:26 PM  
Message: Analyzing F:\OpenRecovery

Index: 57  
Module: DISKSTOR  
Status: Success  
Time: 11:34:26 PM  
Message: Analyzing F:\OpenRecovery\app2sd

Index: 58  
Module: DISKSTOR  
Status: Success  
Time: 11:34:26 PM  
Message: Analyzing F:\OpenRecovery\app2sd\bin

Index: 59  
Module: DISKSTOR  
Status: Success  
Time: 11:34:26 PM  
Message: Reading ext2.ko

Index: 60  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading mot\_boot\_mode

Index: 61  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading parted

Index: 62  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Analyzing F:\OpenRecovery\app2sd\bin\boot\_script

Index: 63  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading 51\_app2sd.sh

Index: 64  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading 51\_app2sd\_sl.sh

Index: 65  
Module: DISKSTOR  
Status: Success

Time: 11:34:27 PM  
Message: Analyzing F:\OpenRecovery\bin

Index: 66  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading .nobashcolors

Index: 67  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading adbd\_start.sh

Index: 68  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading adbd\_stop.sh

Index: 69  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading app2sd.sh

Index: 70  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading bash\_disable\_colors.sh

Index: 71  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading bash\_enable\_colors.sh

Index: 72  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading build.sh

Index: 73  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading busybox.sh

Index: 74  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM

Message: Reading change\_keyboard\_layout.sh

Index: 75  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading enable\_adb\_usbmode.sh

Index: 76  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading flac.sh

Index: 77  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading init\_recovery.sh

Index: 78  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading jit.sh

Index: 79  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading memhack.sh

Index: 80  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_app2sd.sh

Index: 81  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_app2sd2.sh

Index: 82  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_bash.sh

Index: 83  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_busybox.sh

Index: 84  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_got.sh

Index: 85  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_keyboard\_layout.sh

Index: 86  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_misc.sh

Index: 87  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_nandroid.sh

Index: 88  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_nandroid\_backup.sh

Index: 89  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_nandroid\_delete.sh

Index: 90  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_nandroid\_restore.sh

Index: 91  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_overclock.sh

Index: 92  
Module: DISKSTOR  
Status: Success  
Time: 11:34:27 PM  
Message: Reading menu\_restore.sh

Index: 93  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading menu\_scripts.sh

Index: 94  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading menu\_updates.sh

Index: 95  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading nandroid-delete\_adbrecovery.sh

Index: 96  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading nandroid-mobile\_adbrecovery.sh

Index: 97  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading overclock.sh

Index: 98  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading restore.sh

Index: 99  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading root.sh

Index: 100  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading scriptrunner

Index: 101  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading switch.sh

Index: 102

Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading theme.sh

Index: 103  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading wipe\_dalvik\_cache.sh

Index: 104  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Analyzing F:\OpenRecovery\etc

Index: 105  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading fstab

Index: 106  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading profile

Index: 107  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Analyzing F:\OpenRecovery\GOT

Index: 108  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading wallpaper

Index: 109  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Analyzing F:\OpenRecovery\GOT\apps

Index: 110  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading AlarmClock.apk

Index: 111  
Module: DISKSTOR



Status: Success  
Time: 11:34:28 PM  
Message: Reading CalendarProvider.apk

Index: 112  
Module: DISKSTOR  
Status: Success  
Time: 11:34:28 PM  
Message: Reading DownloadProvider.apk

Index: 113  
Module: DISKSTOR  
Status: Success  
Time: 11:34:29 PM  
Message: Reading Facebook.apk

Index: 114  
Module: DISKSTOR  
Status: Success  
Time: 11:34:31 PM  
Message: Reading GenieWidget.apk

Index: 115  
Module: DISKSTOR  
Status: Success  
Time: 11:34:33 PM  
Message: Reading LatinIME.apk

Index: 116  
Module: DISKSTOR  
Status: Success  
Time: 11:34:35 PM  
Message: Reading Launcher.apk

Index: 117  
Module: DISKSTOR  
Status: Success  
Time: 11:34:36 PM  
Message: Reading Mms.apk

Index: 118  
Module: DISKSTOR  
Status: Success  
Time: 11:34:36 PM  
Message: Reading Music.apk

Index: 119  
Module: DISKSTOR  
Status: Success  
Time: 11:34:37 PM  
Message: Reading Phone.apk

Index: 120  
Module: DISKSTOR  
Status: Success

Time: 11:34:37 PM  
Message: Reading Settings.apk

Index: 121  
Module: DISKSTOR  
Status: Success  
Time: 11:34:38 PM  
Message: Reading YouTube.apk

Index: 122  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Analyzing F:\OpenRecovery\GOT\bin

Index: 123  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading mot\_boot\_mode

Index: 124  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading mot\_boot\_mode.backup

Index: 125  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Analyzing F:\OpenRecovery\GOT\bin\boot\_script

Index: 126  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading 61\_memhack.sh

Index: 127  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading 71\_overclock.sh

Index: 128  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading readme.txt

Index: 129  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM

Message: Analyzing F:\OpenRecovery\GOT\fonts

Index: 130  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading Clockopia.ttf

Index: 131  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading DroidSans-Bold.ttf

Index: 132  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading DroidSans.ttf

Index: 133  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Analyzing F:\OpenRecovery\GOT\framework

Index: 134  
Module: DISKSTOR  
Status: Success  
Time: 11:34:39 PM  
Message: Reading framework-res.apk

Index: 135  
Module: DISKSTOR  
Status: Success  
Time: 11:34:41 PM  
Message: Reading services.jar

Index: 136  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Analyzing F:\OpenRecovery\GOT\jit

Index: 137  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Analyzing F:\OpenRecovery\GOT\jit\system

Index: 138  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Analyzing F:\OpenRecovery\GOT\jit\system\bin

Index: 139  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Reading dalvikvm

Index: 140  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Reading dexopt

Index: 141  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Reading logcat

Index: 142  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Analyzing F:\OpenRecovery\GOT\jit\system\lib

Index: 143  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Reading libcutils.so

Index: 144  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Reading libdl.so

Index: 145  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Reading libdvm.so

Index: 146  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Reading liblog.so

Index: 147  
Module: DISKSTOR  
Status: Success  
Time: 11:34:42 PM  
Message: Reading libm.so

Index: 148  
Module: DISKSTOR  
Status: Success  
Time: 11:34:43 PM  
Message: Reading libnativehelper.so

Index: 149  
Module: DISKSTOR  
Status: Success  
Time: 11:34:43 PM  
Message: Reading libz.so

Index: 150  
Module: DISKSTOR  
Status: Success  
Time: 11:34:43 PM  
Message: Analyzing F:\OpenRecovery\GOT\lib

Index: 151  
Module: DISKSTOR  
Status: Success  
Time: 11:34:43 PM  
Message: Analyzing F:\OpenRecovery\GOT\lib\modules

Index: 152  
Module: DISKSTOR  
Status: Success  
Time: 11:34:43 PM  
Message: Reading overclock.ko

Index: 153  
Module: DISKSTOR  
Status: Success  
Time: 11:34:43 PM  
Message: Analyzing F:\OpenRecovery\GOT\ocflac

Index: 154  
Module: DISKSTOR  
Status: Success  
Time: 11:34:43 PM  
Message: Reading framework.jar

Index: 155  
Module: DISKSTOR  
Status: Success  
Time: 11:34:46 PM  
Message: Reading libFLAC.so

Index: 156  
Module: DISKSTOR  
Status: Success  
Time: 11:34:46 PM  
Message: Reading libmediaplayerservice.so

Index: 157

Module: DISKSTOR  
Status: Success  
Time: 11:34:46 PM  
Message: Reading libopencore\_player.so

Index: 158  
Module: DISKSTOR  
Status: Success  
Time: 11:34:46 PM  
Message: Analyzing F:\OpenRecovery\GOT\sbin

Index: 159  
Module: DISKSTOR  
Status: Success  
Time: 11:34:46 PM  
Message: Reading busybox

Index: 160  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Analyzing F:\OpenRecovery\init

Index: 161  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Analyzing F:\OpenRecovery\keychars

Index: 162  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading azerty

Index: 163  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading euro\_qwerty

Index: 164  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading qwerty

Index: 165  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading qwertz

Index: 166  
Module: DISKSTOR

Status: Success  
Time: 11:34:47 PM  
Message: Analyzing F:\OpenRecovery\modules

Index: 167  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading ext2.ko

Index: 168  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Analyzing F:\OpenRecovery\res

Index: 169  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading .nomedia

Index: 170  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Analyzing F:\OpenRecovery\res\images

Index: 171  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading icon\_error.png

Index: 172  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading icon\_firmware\_error.png

Index: 173  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading icon\_firmware\_install.png

Index: 174  
Module: DISKSTOR  
Status: Success  
Time: 11:34:47 PM  
Message: Reading icon\_installing.png

Index: 175  
Module: DISKSTOR  
Status: Success

Time: 11:34:48 PM  
Message: Reading indeterminate1.png

Index: 176  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading indeterminate2.png

Index: 177  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading indeterminate3.png

Index: 178  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading indeterminate4.png

Index: 179  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading indeterminate5.png

Index: 180  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading indeterminate6.png

Index: 181  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading progress\_bar\_empty.png

Index: 182  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading progress\_bar\_empty\_left\_round.png

Index: 183  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading progress\_bar\_empty\_right\_round.png

Index: 184  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM



Message: Reading progress\_bar\_fill.png

Index: 185  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading progress\_bar\_left\_round.png

Index: 186  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading progress\_bar\_right\_round.png

Index: 187  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Analyzing F:\OpenRecovery\root

Index: 188  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading su

Index: 189  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading Superuser.apk

Index: 190  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Analyzing F:\OpenRecovery\sbin

Index: 191  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading adbd\_recovery

Index: 192  
Module: DISKSTOR  
Status: Success  
Time: 11:34:48 PM  
Message: Reading bash

Index: 193  
Module: DISKSTOR  
Status: Success  
Time: 11:34:49 PM  
Message: Reading busybox

Index: 194  
Module: DISKSTOR  
Status: Success  
Time: 11:34:50 PM  
Message: Reading dump\_image-arm-uclibc

Index: 195  
Module: DISKSTOR  
Status: Success  
Time: 11:34:50 PM  
Message: Reading flash\_image-arm-uclibc

Index: 196  
Module: DISKSTOR  
Status: Success  
Time: 11:34:50 PM  
Message: Reading mkyaffs2image-arm-uclibc

Index: 197  
Module: DISKSTOR  
Status: Success  
Time: 11:34:50 PM  
Message: Reading open\_rcvr\_stone

Index: 198  
Module: DISKSTOR  
Status: Success  
Time: 11:34:50 PM  
Message: Reading toolbox

Index: 199  
Module: DISKSTOR  
Status: Success  
Time: 11:34:51 PM  
Message: Reading unyaffs-arm-uclibc

Index: 200  
Module: DISKSTOR  
Status: Success  
Time: 11:34:51 PM  
Message: Analyzing F:\OpenRecovery\scripts

Index: 201  
Module: DISKSTOR  
Status: Success  
Time: 11:34:51 PM  
Message: Reading test.sh

Index: 202  
Module: DISKSTOR  
Status: Success  
Time: 11:34:51 PM  
Message: Analyzing F:\OpenRecovery\updates

Index: 203  
Module: DISKSTOR  
Status: Success  
Time: 11:34:51 PM  
Message: Reading test-update-nosign.zip

Index: 204  
Module: DISKSTOR  
Status: Success  
Time: 11:34:51 PM  
Message: Analyzing F:\ilightr

Index: 205  
Module: DISKSTOR  
Status: Success  
Time: 11:34:51 PM  
Message: Reading title.mp4

Index: 206  
Module: DISKSTOR  
Status: Success  
Time: 11:34:51 PM  
Message: Disconnecting

Index: 207  
Module: MAIN  
Status: Success  
Time: 11:34:51 PM  
Message: DISKSTOR (5.1) completed successfully

## **Appendix D**

### **SIM Card Extraction Logs**

## **Summary**

*Summary and history of this report*

Date Created: 4/27/2011 9:45:27 PM

Locked: No

Extraction Media: SIM Card Reader

XRY Version: 5.2

Is Subset: No

Is Encrypted: No

## **General Information**

*General information about the device (8 items)*

Device Name: SIM Card

Sub Model: SIM

Phase: 2 (PD)

SIM Identification (ICCID): 8964240001007600585

Language Preference: English

Service Provider Name: 2degrees

Subscriber Id (IMSI): 530240100760058

Network Code (from IMSI): 2degrees, New Zealand (53024)

## **Contacts**

*Contacts stored in the device, on the SIM card or on removable media (5 items)*

Name: 2degrees

Index: 1

Tel: \*100#

Name: Customer Care

Index: 2

Tel: 200

Name: Directory Enquiries

Index: 3

Tel: 018

Name: Topup  
Index: 4  
Tel: 201  
Name: Voicemail  
Index: 5  
Tel: +64222022002

### **Network Information**

*Information related to the network (14 items)*

Ciphering Key (Kc): 017A863292AAB32B02  
Temporary Identity (TMSI): 56D02E9A  
Last Network (LAI-MCC/MNC): 2degrees, New Zealand (53024)  
Last Area Code (LAI-LOC): 2712  
Location Update Status: Updated  
Packet Temporary Identity (P-TMSI): C4C943C8  
P-TMSI Signature Value: B53B89  
Routing Area Network (RAI-MCC/MNC): 2degrees, New Zealand (53024)  
Routing Area Location (RAI-LAC): 2712  
Routing Area Code (RAI-RAC): 2  
Routing Area Update Status: Updated  
PLMN Selector: 2degrees, New Zealand (53024); Vodafone New Zealand GSM Mobile Network, New Zealand (53001)  
Forbidden PLMNs: Unknown Network, Unknown Country (45005); China Unicom, China (46001); China Mobile, China (46000); Telecom New Zealand, New Zealand (53005)  
SMS Parameters: 2degrees SCA:+64220227672 PID:00 DCS:0C VP:FF

### **Log**

*Log of extraction process created by XRY (33 items)*

Index: 1  
Module: MAIN  
Status: Success  
Time: 9:45:27 PM  
Message: Initiating Process at 21:45

Index: 2  
Module: MAIN  
Status: Success  
Time: 9:45:27 PM  
Message: XRY Version 5.2

Index: 3  
Module: MAIN  
Status: Success  
Time: 9:45:27 PM  
Message: Selected views: [All]

Index: 4  
Module: MAIN  
Status: Success  
Time: 9:45:27 PM  
Message: Processing device [SIM Card] connected to ACS  
CCID USB Reader 0 []...

Index: 5  
Module: MAIN  
Status: Success  
Time: 9:45:27 PM  
Message: Starting process of SIM (5.2)

Index: 6  
Module: SIM  
Status: Success  
Time: 9:45:27 PM  
Message: Connecting

Index: 7  
Module: SIM  
Status: Success  
Time: 9:45:27 PM  
Message: Connected with T0 Protocol

Index: 8  
Module: SIM  
Status: Success  
Time: 9:45:27 PM  
Message: Detecting SIM type

Index: 9  
Module: SIM  
Status: Success  
Time: 9:45:27 PM  
Message: Identified as SIM Card

Index: 10  
Module: SIM  
Status: Success  
Time: 9:45:27 PM  
Message: PIN code disabled

Index: 11  
Module: SIM  
Status: Success  
Time: 9:45:28 PM  
Message: Analyzing MF folder

Index: 12  
Module: SIM  
Status: Success  
Time: 9:45:28 PM  
Message: Reading General Information

Index: 13  
Module: SIM  
Status: Success  
Time: 9:45:28 PM  
Message: Reading General Information

Index: 14  
Module: SIM  
Status: Success  
Time: 9:45:28 PM  
Message: Analyzing GSM Folder

Index: 15  
Module: SIM  
Status: Success  
Time: 9:45:28 PM  
Message: Reading General Information

Index: 16  
Module: SIM  
Status: Success  
Time: 9:45:28 PM  
Message: Reading Network Information

Index: 17  
Module: SIM  
Status: Success  
Time: 9:45:28 PM  
Message: Reading Network Information PLMN Selector

Index: 18  
Module: SIM  
Status: Success  
Time: 9:45:28 PM  
Message: Reading Network Information Forbidden PLMNs

Index: 19  
Module: SIM  
Status: Success  
Time: 9:45:29 PM  
Message: Analyzing Telecom Folder

Index: 20



Module: SIM  
Status: Success  
Time: 9:45:29 PM  
Message: Reading SMS

Index: 21  
Module: SIM  
Status: Success  
Time: 9:45:30 PM  
Message: Read 30 positions, 0 used

Index: 22  
Module: SIM  
Status: Success  
Time: 9:45:30 PM  
Message: Reading General Information (MSISDN numbers)

Index: 23  
Module: SIM  
Status: Success  
Time: 9:45:30 PM  
Message: Read 3 positions, 0 used

Index: 24  
Module: SIM  
Status: Success  
Time: 9:45:30 PM  
Message: Reading Network Information

Index: 25  
Module: SIM  
Status: Success  
Time: 9:45:31 PM  
Message: Reading Contacts

Index: 26  
Module: SIM  
Status: Success  
Time: 9:45:37 PM  
Message: Read 250 positions, 5 used

Index: 27  
Module: SIM  
Status: Success  
Time: 9:45:37 PM  
Message: Reading Calls (last dialled)

Index: 28  
Module: SIM  
Status: Success  
Time: 9:45:37 PM  
Message: Read 10 positions, 0 used

Index: 29  
Module: SIM

Status: Success  
Time: 9:45:37 PM  
Message: Attempting to read 02 IMEI

Index: 30  
Module: SIM  
Status: Success  
Time: 9:45:37 PM  
Message: No IMEI Found

Index: 31  
Module: SIM  
Status: Success  
Time: 9:45:37 PM  
Message: Looking for iDEN data

Index: 32  
Module: SIM  
Status: Success  
Time: 9:45:37 PM  
Message: No iDEN data found

Index: 33  
Module: MAIN  
Status: Success  
Time: 9:45:37 PM  
Message: SIM (5.2) completed successfully

## **Appendix E**

### **WiFi Connection Report**

# Device data report

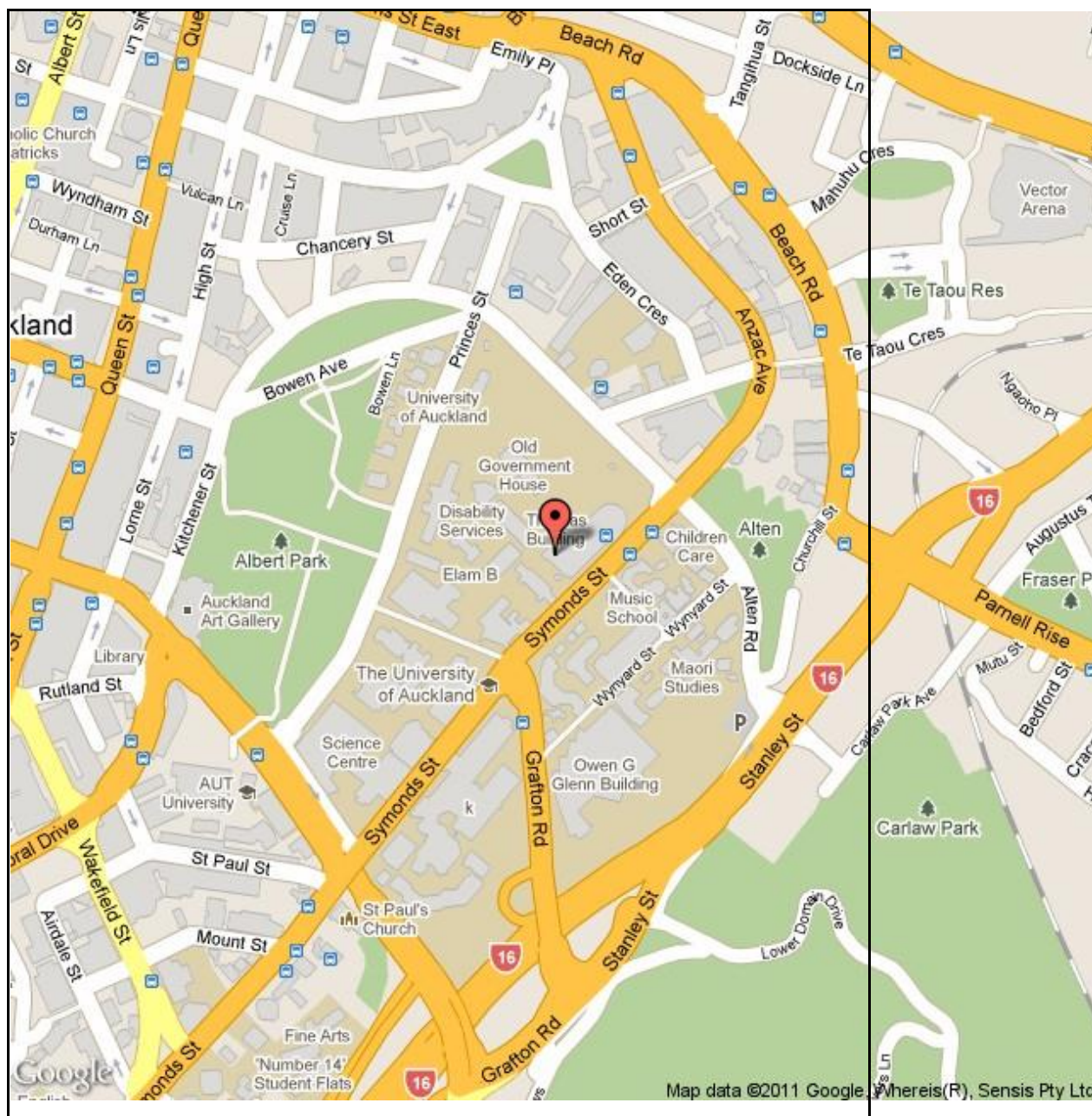
Device details	
Retail name	Apple iPhone 3G
Manufacturer	Apple
Model	iPhone 3G
SW revision	4.2.1
Boot loader	iBoot-931.71.16
IMEI	011771005941037
Device alias	New device (iPhone 3G)
Device owner numbers	
WiFi MAC address	00:23:6c:d0:e9:f1
Bluetooth MAC address	00:23:6c:d0:e9:f0
iTunes display name	Andrew
Phone number	
IMSI	530240100760058
ICCID	8964240001007600585
Device model	MB489X/A
Time zone	Pacific/Auckland
Serial number	8784265JY7H
Identificator	1163f433662d9c0f7854a2625e19dfb5da967352
Sim status	kCTSIMSupportSIMStatusNotReady
Jail Break	No
Case details	
Extracted by version	3.2.0.180
Case assigned	04
Evidence Number	04
Device notes	real
Extraction date	27/04/2011
Extraction time	1:45:03 AM
Device owner	Andrew
Extraction made by	User
Report details	
Generation date	22/06/2011
Generation time	10:04:15 AM
Extraction made by	User

## WiFi Connections

### Oxygen Forensic Suite 2011 (Trial) - 3.3.0.270

<b>SSID</b>	TP-LINK_660650
<b>BSSID</b>	00:25:86:66:06:50
<b>RSSI (dbm)</b>	-85
<b>Channel</b>	6
<b>Last joined time</b>	7/04/2011 12:52:05 AM
<b>Last auto joined time (GMT+0)</b>	10/04/2011 11:10:39 AM
<b>Geo coordinates (from Google</b>	N/A
<b>Accuracy (in meters) (from</b>	N/A
<b>Address(from</b>	N/A
<b>MD5 Hash</b>	607e54adc8485b546bc751620a87d2ca

<b>SSID</b>	UoA
<b>BSSID</b>	00:13:c3:06:b7:20
<b>RSSI (dbm)</b>	-85
<b>Channel</b>	1
<b>Last joined time</b>	29/03/2011 3:10:28 AM
<b>Last auto joined time (GMT+0)</b>	30/03/2011 3:30:39 AM
<b>Geo coordinates (from Google server)</b>	S 36.8507928, E 174.7709154
<b>Accuracy (in meters) (from Google server)</b>	51.0
<b>Address(from Google)</b>	New Zealand, Auckland, Symonds St, 44
<b>MD5 Hash</b>	fa2dee21f0a1e56336cff33739345fef
<b>Map Image</b>	



SSID	iptime
BSSID	00:08:9f:b2:22:10
RSSI (dbm)	-84
Channel	11
Last joined time	1/03/2011 1:29:54 AM
Last auto joined time (GMT+0)	4/04/2011 8:25:08 PM
Geo coordinates (from Google server)	N 37.3845511, E 126.6426153
Accuracy (in meters) (from Google server)	51.0
Address(from Google	South Korea, Incheon, Songdo-dong, 8-20
MD5 Hash	fdee439d0d2cb41a64dbd6eba7b47baa
Map Image	



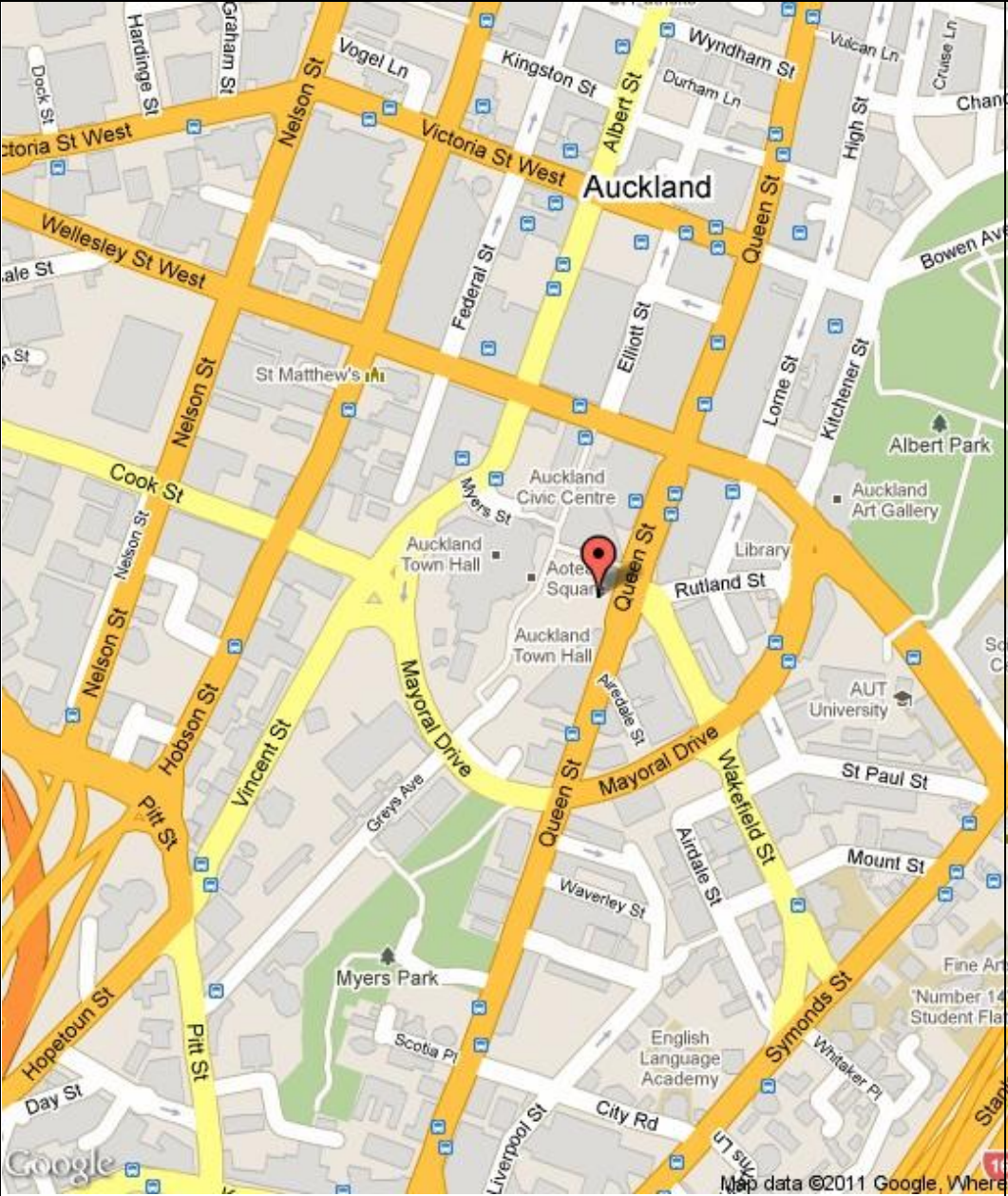
SSID	AUT-Unisurf
BSSID	00:23:eb:80:74:b4
RSSI (dbm)	-61
Channel	11
Last joined time	13/03/2011 11:25:54 PM
Last auto joined time (GMT+0)	1/04/2011 7:29:50 AM
Geo coordinates (from Google server)	S 36.8522517, E 174.76353
Accuracy (in meters) (from Google server)	49.0
Address(from Google	New Zealand, Auckland, Auckland Central, Queen St, 303



MD5 Hash

e3b6902bf50ce01d425248238c0933c7

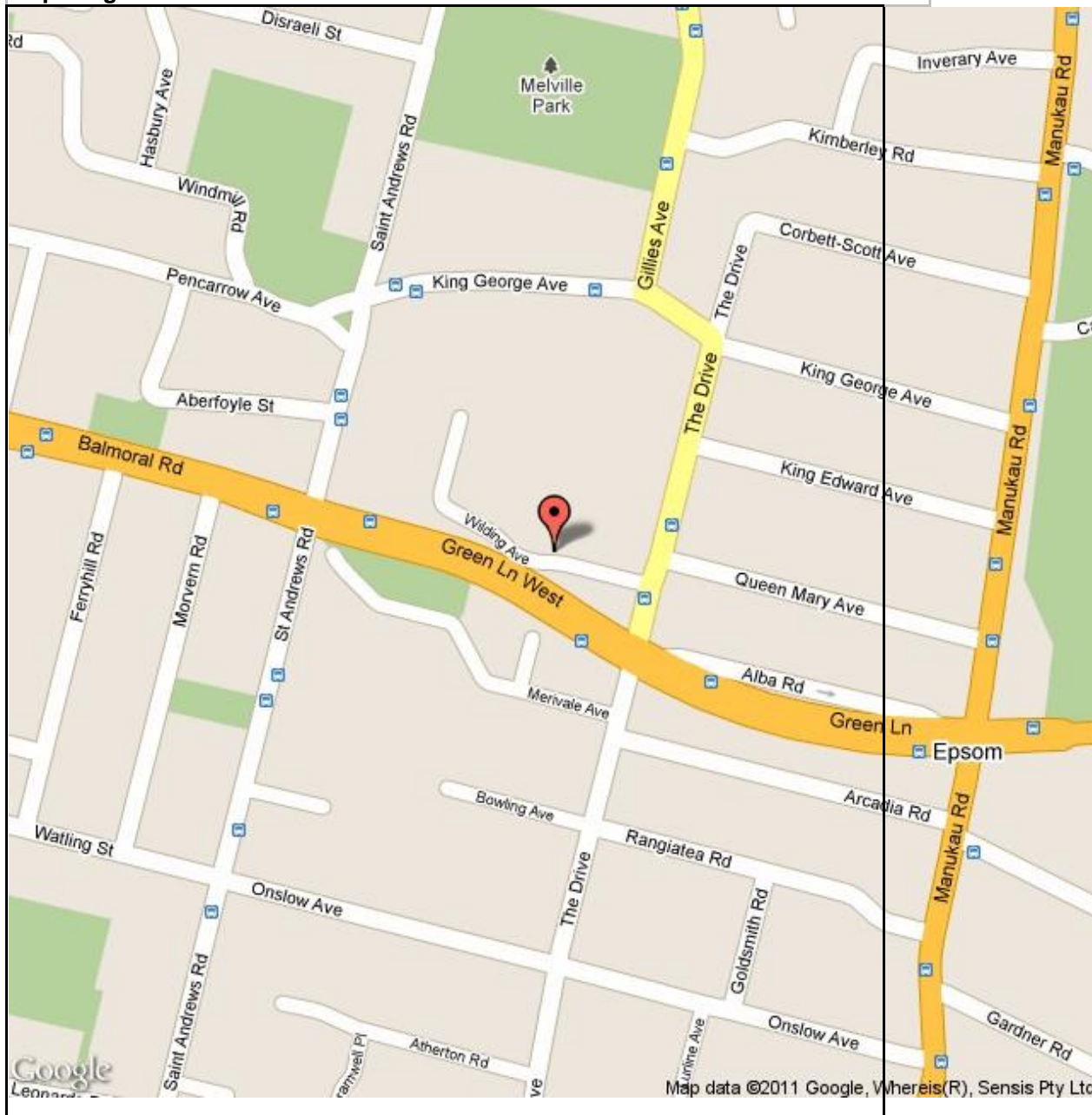
Map Image



Map data ©2011 Google, Where's(R), Sensis Pty Ltd

SSID	qiufamily
BSSID	00:1e:e5:95:b8:ca
RSSI (dbm)	-66
Channel	11
Last joined time	21/10/2010 9:02:24 AM
Last auto joined time (GMT+0)	24/10/2010 7:44:04 AM
Geo coordinates (from Google server)	S 36.8915013, E 174.7691274
Accuracy (in meters) (from Google server)	73.0
Address(from Google	New Zealand, Auckland, Epsom, Wilding Ave, 17

MD5 Hash	f83c79886f5c7272b9c6255913cf3c95
Map Image	

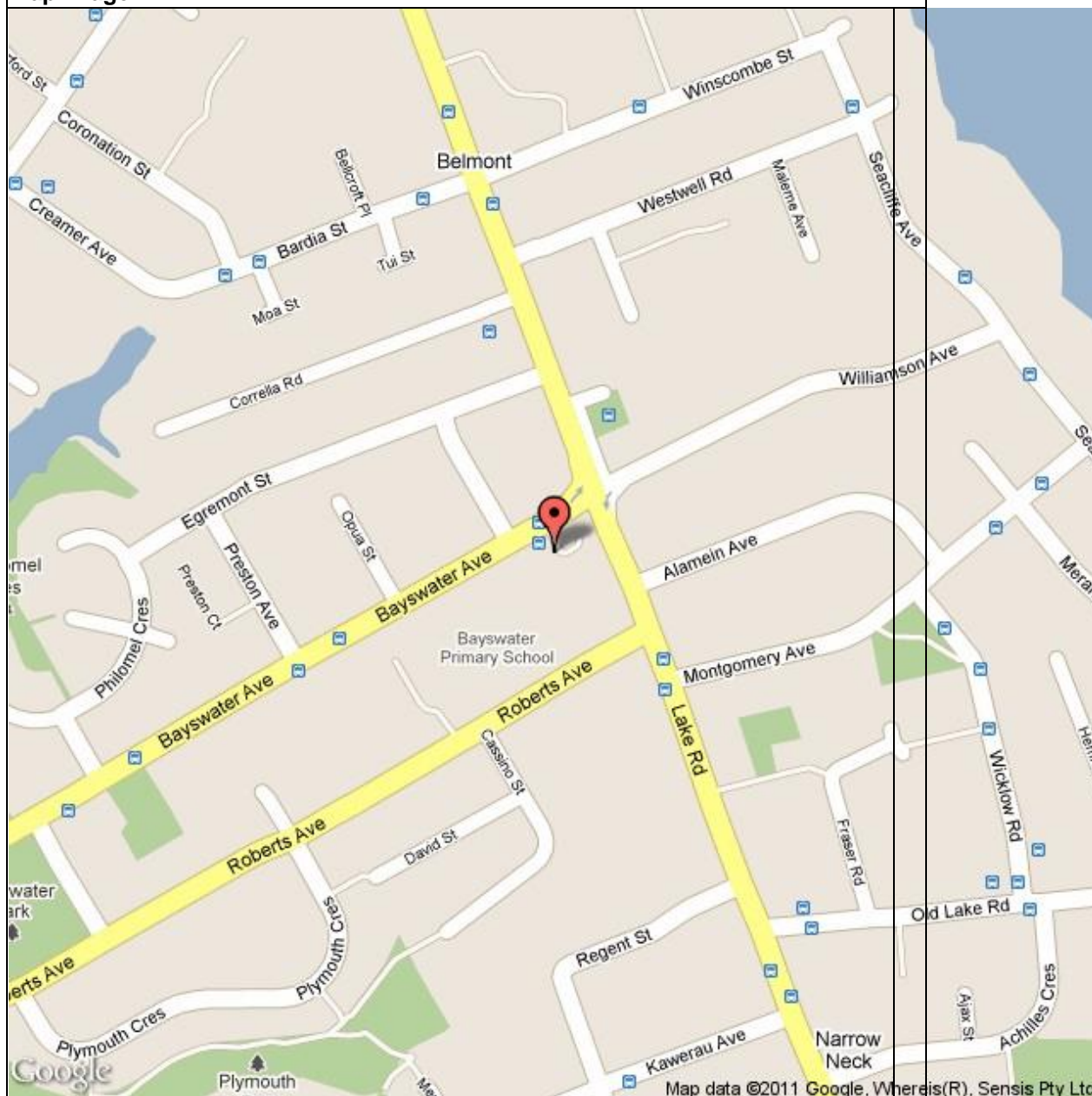


SSID	ThomsonAD82BB
BSSID	00:1f:9f:85:54:01
RSSI (dbm)	-50
Channel	6
Last joined time	1/01/2000 3:41:39 AM
Last auto joined time (GMT+0)	26/04/2011 12:36:28 PM
Geo coordinates (from Google server)	S 36.8089118, E 174.7896277



Accuracy (in meters) (from Google server)	73.0
Address(from Google	New Zealand, Auckland, Belmont, Bayswater Ave, 187
MD5 Hash	6c2b9e1952d4dc69da742f22f35185e8

#### Map Image



SSID	AUT-Unisurf-Open
BSSID	00:23:eb:62:47:a1
RSSI (dbm)	-57
Channel	11
Last joined time (GMT+0)	1/01/2000 12:06:29 AM
Last auto joined time (GMT+0)	13/03/2011 11:22:04 PM
Geo coordinates (from Google server)	S 36.8532236, E 174.7639751

Accuracy (in meters) (from Google server)	73.0
Address(from Google)	New Zealand, Auckland, Auckland Central, Airedale St, 2
MD5 Hash	7b087f9f2d798ca3a2b872bc8212ac96
Map Image	

