

Mobile Phone: Identifying Configuration Signatures of Local Devices Absent from XRY

TOMA S. VASA
BCIS (AUT, New Zealand)

A thesis submitted to the graduate Faculty of Design and Creative Technologies
AUT University
in partial fulfilment of the
requirements for the degree of
Master of Forensic Information Technology

School of Computing and Mathematical Sciences

Auckland, New Zealand
2013

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.

.....

Toma S. Vasa

Acknowledgements

Firstly, I would like to thank God for his love, strength and wisdom that he has given me and without him, I would not have been able to complete this project. *“I can do all this through him who gives me strength”*, Philippians 4:13.

I would like to thank everyone that has supported me throughout the duration of this thesis. I would like to express my special thanks of gratitude to my supervisor Dr. Brian Cusack for his patience, guidance, encouragement, help and support for me to complete this project.

I would also like to acknowledge and thank AUT for allowing and giving me the opportunity to conduct this research. I would also like to thank Messina Shaw for her help and support as a reviewer including her excellent feedback on this project.

I would like to thank my work colleagues for their support, as well as my fellow MFIT colleagues for their support as well.

A special feeling of gratitude to my loving parents; Faamatuainu Saivaega and Moelagona Vasa for their support and words of encouragement. I would also like to thank my beloved family including my friends for their sincere love, prayers and support. They encouraged me a lot to complete this project within such a limited time. Therefore, thanks again to all who helped and supported me, without you guys I would not have been able to do this.

Lastly, I would like to dedicate this work in memories of the following people who has had such great influence in my life: Malia Seuamuli Toma, Suivaaia Vasa and Faauli & Eseta Toma-Malaesilia. May They Rest In Peace.

Abstract

Technology is rapidly expanding in to every part of daily life as evidenced by the increase in the number of new mobile phone devices appearing on the market while older models remain in use and are reused. The rapid emergence of different and new mobile devices presents challenges for mobile phone forensic investigation. Some models cannot be supported by mobile forensic tools and others have ways of preventing access. XRY is one of the best known mobile forensic tools and it is constantly updating signatures and producing new connectors to keep up with the market. However, the speed of new mobile devices' release and the emergence of new designs will always result some being overlooked.

The purpose of this research project is to conduct an investigation to identify some models on the New Zealand market that are not currently supported by XRY and to perform forensic extraction on one or two as well as a supported model. The research is to identify configuration signatures or characteristics of local mobile phone devices that are absent from the XRY database. The result was that four local mobile phone devices (test phones) that are sold and operate in New Zealand were located. Some of these models were manufactured specifically for local Network Service Providers. They were tested following a methodology derived from previous research literature including the use of practise standards and procedures for digital forensics.

The research findings determine the capability of XRY 6.5 to extract data from these local mobile phone devices. As a result, two of these test devices (Phones 2 and 4) were not officially recognised by XRY and were absent from its database. Phones 1 and 3 were in the database. XRY was able to extract data from each test phone device (logical extraction) however not all the data was extracted. Thus, some of the test devices already recognised by the tool were not fully supported. XRY was able to extract most of the data from some test devices while others had incomplete data. Most of the deleted test data was not able to be recovered.

A discussion of the findings indicates that local mobile phone devices can be supported by forensic tools such as XRY; however there are limitations due to each tool's performance criteria. These local mobile phone devices can be included in the XRY's list of supported device profiles and this research provides implications for digital forensic analysts about how these test phones can be recognised and

supported. There are also further possible aspects for future work within this research area that can focus on improving the capability of forensic tools to conduct physical analyses for these local test phones.

Table of Contents

DECLARATION	II
ACKNOWLEDGEMENTS	III
ABSTRACT	IV
LIST OF TABLES.....	IX
LIST OF FIGURES.....	IX
ABBREVIATIONS.....	X
CHAPTER ONE	1
1.0 INTRODUCTION.....	1
1.1 PROBLEM AREA	1
1.2 MOTIVATION	2
1.3 STRUCTURE OF THESIS	3
1.4 CONCLUSION	5
CHAPTER TWO	6
2.0 INTRODUCTION.....	6
2.1 MOBILE PHONE FORENSICS.....	7
2.1.1 <i>Mobile Phone Devices.....</i>	<i>7</i>
2.1.2 <i>Evidence Storage on a Mobile Phone Device.....</i>	<i>9</i>
2.2 DIGITAL FORENSIC TOOLS	11
2.3 FORENSIC TOOLS' TESTING	13
2.4 MOBILE PHONE DATA EXTRACTION	14
2.5 MOBILE PHONE MARKET IN NEW ZEALAND	16
2.5.1 <i>Local Mobile Phone Devices</i>	<i>18</i>
2.6 PROBLEMS AND ISSUES	19
2.7 CONCLUSION	20
CHAPTER THREE	22
3.0 INTRODUCTION.....	22
3.1 REVIEW OF PREVIOUS RELATED RESEARCH.....	22
3.1.1 <i>Forensic Analysis of Mobile Phones.....</i>	<i>23</i>
3.1.2 <i>Data Acquisition from Cell Phone using Logical Approach.....</i>	<i>25</i>
3.1.3 <i>Overall Assessment of Mobile Internal Acquisition Tool</i>	<i>27</i>
3.1.4 <i>Investigating Information Recover from Resold Mobile Devices.....</i>	<i>28</i>

3.1.5	<i>Windows 7: Implications for Digital Forensic Investigators</i>	29
3.2	RESEARCH DESIGN	31
3.2.1	<i>Summary of Previous Research</i>	31
3.2.2	<i>Review of Problems and Issues</i>	32
3.2.3	<i>Research Questions and Hypothesis</i>	33
3.2.3.1	Sub-Questions	33
3.2.4	<i>Research Phases</i>	34
3.2.5	<i>Data Map</i>	35
3.3	DATA ACQUISITION	35
3.3.1	<i>Collection</i>	35
3.3.2	<i>Process</i>	36
3.3.3	<i>Analysis</i>	36
3.4	LIMITATIONS	37
3.5	CONCLUSION	38
CHAPTER FOUR		39
4.0	INTRODUCTION	39
4.1	RESEARCH EQUIPMENT	39
4.2	PREVIOUS DATA	40
4.2.1	<i>XRY Device Model Features</i>	41
4.3	COLLECTION AND PREPARATION	42
4.3.1	<i>Test Phones</i>	42
4.3.2	<i>Test Data</i>	43
4.4	ACQUISITION	46
4.4.1	<i>Phone 1 - Acquisition</i>	47
4.4.2	<i>Phone 2 - Acquisition</i>	48
4.4.3	<i>Phone 3 - Acquisition</i>	49
4.4.4	<i>Phone 4 - Acquisition</i>	50
4.5	ANALYSIS	51
4.5.1	<i>Contacts and Calls</i>	52
4.5.2	<i>SMS, MMS and Email Messages</i>	52
4.5.3	<i>Pictures, Videos and Audios</i>	52
4.5.4	<i>Calendar, Tasks, Notes and Memo</i>	53
4.5.5	<i>Network Information</i>	54
4.5.6	<i>Others</i>	54
4.6	COMPARISON	54
4.7	CONCLUSION	56
CHAPTER FIVE		57

5.0	INTRODUCTION.....	57
5.1	RESEARCH QUESTIONS AND HYPOTHESES	57
5.2	DISCUSSION OF FINDINGS	62
5.2.1	<i>Mobile Phone Devices</i>	62
5.2.2	<i>Recognised and Unrecognised Device</i>	63
5.2.3	<i>Logical and Physical Extraction</i>	64
5.2.4	<i>Research Data</i>	65
5.2.4.1	Phone 1.....	65
5.2.4.2	Phone 2.....	66
5.2.4.3	Phone 3.....	66
5.2.4.4	Phone 4.....	67
5.2.4.5	Deleted Test Data	68
5.2.4.6	Extracted Device Specification.....	68
5.3	RECOMMENDATIONS	69
5.4	CONCLUSION	70
CHAPTER SIX	72
6.0	INTRODUCTION.....	72
6.1	SUMMARY OF FINDINGS	72
6.2	LIMITATIONS OF THE RESEARCH	72
6.3	FUTURE RESEARCH	74
6.4	CONCLUSION	75
REFERENCES	77
APPENDICES	82
	APPENDIX 1: PC SPECIFICATION	82
	APPENDIX 2: TEST PHONES SPECIFICATION	82
	APPENDIX 3A: PHONE 1 XRY DATA EXTRACTION	84
	APPENDIX 3B: PHONE 2 XRY DATA EXTRACTION	94
	APPENDIX 3C: PHONE 3 XRY DATA EXTRACTION	100
	APPENDIX 3D: PHONE 4 XRY DATA EXTRACTION	105
	APPENDIX 4: XRY DEVICE EXTRACTION INFORMATION SUMMARY	115

List of Tables

TABLE 1: EVIDENCE RELATED TO MOBILE DEVICE (ADAPTED FROM CASEY & TURNBULL, 2011)	11
TABLE 2: LOCAL NSP MOBILE PHONE DEVICES	19
TABLE 3: FORENSIC TOOLS USED FOR LOGICAL ANALYSIS	30
TABLE 4: DATA EXTRACTED FROM WINDOW MOBILE OS	30
TABLE 5: DATA EXTRACTED FROM W7 USING XRY	30
TABLE 6: LIST OF EQUIPMENT	40
TABLE 7: MOBILE PHONE DEVICE HARDWARE AND SOFTWARE INFORMATION	41
TABLE 8: EXPECTED DATA	41
TABLE 9: XRY LOGICAL SUPPORTED FEATURES	41
TABLE 10: TESTS PHONES NETWORK	43
TABLE 11: PHONE1 TEST DATA	44
TABLE 12: PHONE2 TEST DATA	45
TABLE 13: PHONE 3 TEST DATA	45
TABLE 14: PHONE 4 TEST DATA	46
TABLE 15: TEST PHONES RESULTS USING XRY 6.5	55
TABLE 16: MAIN RESEARCH QUESTION	58
TABLE 17: SUB-QUESTION ONE	59
TABLE 18: SUB -QUESTION TWO	60
TABLE 19: SUB-QUESTION THREE	61

List of Figures

FIGURE 1: HARDWARE CHARACTERISTICS (ADAPTED FROM JANSEN & AYERS, 2007)	8
FIGURE 2: SOFTWARE CHARACTERISTICS (ADAPTED FROM JANSEN & AYERS, 2007)	8
FIGURE 3: MOBILE PHONE EVIDENCE EXTRACTION PROCESS (ADAPTED FROM MURPHY, 2010)	15
FIGURE 4: MOBILE PHONE TOOL LEVELLING PYRAMID (ADAPTED FROM BROTHERS, 2009)	15
FIGURE 5: TELECOM, VODAFONE, 2DEGREES SUBSCRIBERS (COMMERCE COMMISSION, 2011)	16
FIGURE 6: MARKET SHARE BY SUBSCRIBER (COMMERCE COMMISSION, 2011)	17
FIGURE 7: RESEARCH APPLICATION STRUCTURE	24
FIGURE 8: DATA ACQUISITION USING JTAG	25
FIGURE 9: ACQUISITION TOOL DESIGN	26
FIGURE 10: EXPERIMENT RESULTS	28
FIGURE 11: RESEARCH PHASES	34
FIGURE 12: DATA MAP	35
FIGURE 13: PHONE 1 DEVICE PROFILE OVERVIEW	48
FIGURE 14: TELECOM R7 XT DEVICE PROFILE	49
FIGURE 15: PHONE 3 DEVICE PROFILE OVERVIEW	50

Abbreviations

2G - Second Generation

3G - Third Generation

ACPO - Association of Chief Police Officers

CDMA - Code Division Multiple Access

COTS - Commercial Off The Shelf

DM - Division Multiple

EDGE - Enhanced Data for GSM Evolution

EEPROM - Electronically Erasable Programmable Read Only
Memory

EFS - Embedded File System

EMS - Enhanced Message Service

ESN - Electronic Serial Number

FBUS - FastBus

GPRS - General Packet Radio Service

GPS - Global Positioning System

GSM - Global Systems Mobile

HSDPA - High-Speed Downlink Packet Access

ICCID - Integrated Circuit Card Identification

IEC - International Electrotechnical Commission

IM - Instant Message

IMEI - International Mobile Equipment Identifier

IMSI - International Mobile Subscriber Identity

IRMC - Infrared Mobile Communications

ISO - International Organization for Standardization

JTAG - Joint Test Action Group

MCC - Mobile Country Code

ME - Mobile Equipment

MIAT - Mobile Internal Acquisition Tool

MIN - Mobile Identification Number

MMS - Multimedia Messaging Service

MNC - Mobile Network Code

MS - Mobile Station

MSAB - Micro Systemation
MSIN - Mobile Station Identification Number
NIJ - National Institute of Justice
NIST - National Institute of Standards and Technology
NSP - Network Service Provider
OBEX - Object Exchange
OS - Operating System
PC - Personal Computer
PIM - Personal Information Manager
PIN - Personal Identification Number
PUK - Personal Unlocking Key
PUMP - Privacy and Usability Methods Pow-wow
RIM - Research In Motion Ltd
SD - Secure Digital
SIM - Subscriber Identity Module
SMS - Short Message Service
SyncML - Synchronization Markup Language
TDMA - Time Division Multiple Access
TNZ - Telecom New Zealand
UMTS - Universal Mobile Telecommunications System
USB - Universal Serial Bus
USIM - Universal Subscriber Identity Module
VFNZ - Vodafone New Zealand
WCDMA - Wideband Code Division Multiple Access

Chapter One

INTRODUCTION

1.0 Introduction

Today's mobile phone devices can do more than just dial and receive calls and send and receive text messages. Their features and capabilities can perform many operations that a laptop or home personal computer can. The amount of information these devices store is enormous including many personal details about the user and information relating to their day-to-day life. A mobile phone has become an important part of many people's daily life whether it's for personal or business needs, and lawful or unlawful activities. Therefore a mobile phone device has become an interesting source of relevant information for civil and criminal investigations. Information stored and processed on this electronic device can be significant and crucial to law enforcement and corporate agencies that are able to conduct digital forensic analyses on these devices. They use forensic tools such as XRY to extract, analyse and present relevant information (evidence) in a court of law. However not all mobile phone devices are supported by these forensic tools.

Within the Australasia region (New Zealand and Australia) there are more than a million mobile phone subscribers. This research project will identify the capability of forensic tools such as XRY to extract data from mobile phone devices that are operated and sold within New Zealand. Some local mobile phone devices or models are not fully supported by some of the world's leading forensic tools. Some of the devices sold in New Zealand are supplied by local Network Service Providers (NSPs) although a range of their models are manufactured by other companies on their behalf. A selection of these local NSPs' mobile phone devices will be the target or test devices for this research. This chapter will introduce the problem area to be researched (Section 1.1) including the motivation for this research project (Section 1.2.). The structure of the thesis is outlined in Section 1.3 which introduces and summarises the four main chapters of the research.

1.1 Problem Area

As will be discussed in Section 2.6, the problem is that not all mobile phone devices are supported by any forensic tool. New models and features of these devices make it difficult to maintain a forensic tool's support capabilities. Some cannot be supported

because each model has either different cables or connectors or a different Operating System (OS) or other dissimilar software and hardware characteristics. There are also issues regarding the type of network device a forensic tool can support whether it is a GSM, CDMA, WCDMA or others. All these issues and problems are faced by forensic specialists within this region.

Since 2011, there have been 5,020,000 mobile phones operating in New Zealand according to a Taylor Nelson Sofres (TNS) survey about mobile users' behaviours and motivations (The New Zealand Herald, 2012). This figure indicates that there are more mobile phones in New Zealand than the number of people. All these devices range from basic mobile phones to smartphones. Therefore, the capability of a forensic tool to extract information from these local devices is an interesting point for this research. There are some devices that are operated within New Zealand's mobile network and sold by local NSPs that are not supported by any forensic tool which presents a problem. Some of these devices are manufactured specifically for these NSPs which can make them unique only within New Zealand. Therefore, local law enforcement agencies such as the New Zealand Customs Service (NZCS), Electronic Forensic Unit and others have access to a wide range of high-demand forensic tools (MSAB, n.d). XRY version 6.5 will be used for this research case scenario to clarify and justify these issues and problems regarding whether some local mobile phone devices are not supported by leading forensic tools.

1.2 Motivation

A mobile phone device is very important to people who use such technology to communicate with others and to organise daily activities. Therefore it can be a very important source of information for law enforcement and corporate agencies during criminal investigations. These devices contain vital and relevant information that can be used as evidence in a court of law. According to the National Institute of Justice in the USA (2010, p.4), "*digital evidence is now used to prosecute all different kinds of crimes*". This type of evidence is admissible in a court of law as supported by the ISO/IEC International Standard (ISO/IEC 27037:2012) which will ensure the reliability and credibility of such evidence during court cases and legal disputes (Lazarte, 2012). Criminals can use such devices to organise and execute crimes such as homicide, burglary, drug dealing, money laundering, fraud, identity theft, hacking,

paedophilia, child abuse, sexual harassment and including electronic crime (e-crime) and cybercrime. According to Britz, (2008) cybercrime refers to any criminal activity that has been committed via the Internet and computer crime is any criminal activity that has been facilitated using a computer. A mobile phone device can be used to commit such crimes by using its advanced features particularly smartphones to commit malicious crimes.

Law enforcement agencies can rely on evidence extracted from these devices during civil and criminal investigations. In New Zealand the number of crimes involving electronic evidence has increased (New Zealand Police, 2010). For example a man visiting New Zealand has been jailed for importing child abuse cartoon images found on his laptop by the NZCS (TVNZ, 2013). In *The Queen vs Shawn Dean Roberts*, (2000) court case a mobile phone was used to organise the robbery of a jewellery store in Auckland by two offenders. In Australia, rape charges against a Sydney businessman dropped after deleted messages from his mobile phone were recovered which showed he did not commit the crime (Gibson, 2010). In England three teenage boys were given 40 months detention after the Greater Manchester Police found evidence of them on their mobile phones robbing a local petrol station; they had taken pictures of themselves holding the stolen cash (Collis, 2012). In August 2011 a riot in the United Kingdom more than 3,000 people were arrested. The local Police used some of the rioters' mobile phones to convict them (BBC, 2011). Two men were successfully convicted by police of killing two tourists in Antigua in the West Indies, due to one of the men inserting his SIM card in the victim's mobile phone after committing the crime (Hall, 2011). These are some of the ways mobile phone devices have been involved in illegal activities particularly in using them to organise and facilitate a criminal act. Hence crucial information can be stored on their mobile phone device relevant to a crime investigation.

1.3 Structure of Thesis

This thesis is divided in to six chapters: Chapter One – Introduction, Chapter Two - Literature Review, Chapter Three – Methodology, Chapter Four – Findings, Chapter Five – Discussion, and Chapter Six – Conclusion. The introduction to this study identifies a problem area for investigation and the motivation for this research project.

Chapter Two involves a literature review of the selected areas of this research project including the problem area. The literature review topics are: Mobile Phone Forensics (Section 2.1) which includes a review on mobile phone devices and their evidence storage areas. Forensic Tools (Section 2.2) includes Forensic Tool Testing (Section 2.3), and Mobile Phone Data Extraction (Section 2.4). The Mobile Phone Market in New Zealand is also considered (Section 2.5) including Local Mobile Phone Devices and concludes with Problems and Issues (Section 2.6).

Chapter Three defines the methodology for this research project including the research question and hypothesis. Section 3.1 reviews previous studies and research that have similar objectives to this project. The research design (Section 3.2) is based on these previous works and the areas reviewed in Chapter Two. Chapter Four presents the research question and a sequence of hypotheses to be tested to determine the outcome of this research project once the data have been collected. As part of the research design, four research phases have been created to guide the collection of data. Section 3.3 defines how the collected data will be processed and analysed. Chapter Three concludes with the limitations of this research project (Section 3.4).

Chapter Four follows the proposed methodology as defined in Chapter Three and reports on the research findings and results. The equipment that will be used is identified and discussed (Section 4.1) and the data expected to be collected based on the literature reviewed in Chapters Two and Three (Section 4.2). The test mobile phone devices that will be used in this research experiment are identified and the test data in these test devices established (Sections 4.3). Sections 4.4 and 4.5 report each procedure before and during the forensic analysis experiment, and the results and findings from the experiment and their analysis. Chapter Four concludes with comparing the findings with previous work and test data results.

Chapter Five is the final chapter of this research which discusses the findings presented in Chapter Four. This chapter begins with answering the research question including sub-questions and hypotheses that were tested and considered in Section 5.1. The entire findings context from Chapter Four will be thoroughly discussed in Section 5.2 while reviewing the problem area as discussed in Section 2.6. Chapter Five concludes with any recommendations that might arise and their implications to minimise and solve the current problems and issues relating to this project's findings. Chapter Six summarises the findings and considers their possible limitations including further areas for future work (Section 6.3).

1.4 Conclusion

Mobile phone devices are very useful not only for an individual owner but also for law enforcement agencies in solving and crime. These agencies use forensic tools to conduct digital forensic investigations on these devices. The problem is not all mobile phone devices are supported by the current forensic tools. Many different models are operated and sold within New Zealand. Some are uniquely manufactured for some of the local NSPs. Therefore, this research project aims to ensure that local law enforcement and corporate agencies are able to carry out their responsibilities without any hesitation in terms of acquiring and analysing digital data from local mobile phone devices using forensic tools such as XRY. XRY is one of the most frequently used mobile forensic tools in the market and its capability will be tested with local mobile phone devices as identified in Sections 1.1 and 2.6.

The motivation for this research is about the critical importance of mobile phone evidence for our local law enforcement agencies to track down illegal activities including day-to-day criminal activity and electronic crime. Sections 1.2. and 1.3 outline the structure of this research based on the literature review of the related research topics. The proposed methodology will be followed to collect the data and to then discuss any results to establish a successful outcome for this research project.

Chapter Two

LITERATURE REVIEW

2.0 Introduction

Mobile phones are the most commonly used electronic communication devices in today's society. People use a mobile phone every day not just for convenience, but also because it is one of the fastest ways to communicate. Mobile phones have been upgraded from simple communication devices and have become smart phones, capable of running several features like a personal or desktop computer. Law enforcement and investigating agencies highly depend on information contained in these devices during criminal or civil crimes' investigations. Forensic tools such as XRY will enable forensic analysts to extract and analyse relevant information from these devices to provide potential evidence in a court of law.

Chapter 2 reviews a selection of the literature that defines and clarifies different topics related to this research. Section 2.1 defines Digital Forensics as a whole, and its procedures including its relationship to the Mobile Phone Forensics field. Section 2.1.1 gives a fundamental overview on a mobile phone device while Section 2.1.2 describes what information can be contained on these mobile phone devices and where they can be found.

Section 2.2 reviews the forensic tool XRY which is used in this research and is one of the top used and most sophisticated Mobile Phone Forensics tools on the market. XRY has been cited, tested and used in previous research such as (Le, 2012, McCarthy, 2005, Distefano & Me, 2008, NIJ, 2010, Ayers, Jansen, Moenner, & Delaitre, 2007, Walls, Learned-Miller, & Levine, 2011, Casey & Turnbull, 2011, Jansen & Ayers, 2007) and others. Section 2.3 validates and verifies XRY's accuracy based on the results of previous research.

Section 2.4 is the review of standard procedures or guidelines to follow when conducting a Digital Forensics investigation. This procedure will cover the four main processes of Digital Forensics; collection, acquisition, analysis and reporting. Section 2.5 outlines the three main Network Service Providers (NSPs) within New Zealand and the mobile phone services they provide while Section 2.5.1 identifies the target mobile phone devices supplied by these NSPs that will be tested in the research.

Finally, Section 2.6 identifies issues and problems facing the Digital Forensics industry particularly with local government law enforcement and corporate agencies. The problem is some forensic tools aren't able to support all mobile phone devices, in terms of extracting all information contained in them. New Zealand is one of the few countries in the world that has already established and developed a digital forensic practice. Local law enforcement and corporate agencies use several forensic tools such as XRY. The question here is whether XRY is able to fully support mobile phones that are sold and supplied locally within the New Zealand market by local NSPs.

2.1 Mobile Phone Forensics

Digital Forensics requires identifying all digital evidence including computer forensics which is mainly about identifying evidence on a computer (Reith, Carr, & Gunsch, 2002). Digital Forensics focuses on a broad range of forensic investigations of digital technology including computers and electronic devices such as mobile phones. Reith et al, (2002) defines Digital Forensics as scientifically proven methods used to preserve, collect, validate, identify, analyse and report digital evidence from any digital source.

A digital source refers to any technological device that stores and/or processes data such as mobile devices (e.g. thumb drive, memory sticks and others including mobile phones) (Punja & Mislan, 2008). Globally mobile phone devices are everywhere, and people are reliant on the features and capabilities of these devices (Zareen & Baig, 2010). People use such devices for communication either for making phone calls or sending text messages (i.e. SMS, MMS, IM) including web browsing, Personal Information Management (PIM) applications, entertainment (i.e. audio, video and photos) and much more (Ayers, Jansen, Moenner, & Delaitre, 2007). They treat these devices as having an important function in their lives. Personal, professional or sensitive information can be stored on these devices similar to the way they are stored in a personal computer (PC) (Owen, Thomas, & McPhee, 2010).

2.1.1 Mobile Phone Devices

According to Punja and Mislan, (2008), mobile phone devices are also known as cellular phones (mobile) including Personal Digital Assistants (PDA) and smartphones. Mobile phones have their own fundamental hardware and software

characteristics. These devices appear in different platforms that range from an old basic or classic mobile phone to a smartphone (Jansen & Ayers, 2007). Jansen and Ayers (2007) define the characteristics of a mobile phone device to be between a basic, advanced, or smart device.

	Basic	Advanced	Smart
Processor	Limited Speed	Improved Speed	Superior Speed
Memory	Limited Capacity	Improved Capacity	Superior Capacity, Built-in Hard Drive Possibility
Display	Grayscale	Color	Large size, 16-bit Color (65,536 colors) or Higher
Card Slots	None	MiniSD or MMCmobile	MiniSDIO or MMCmobile
Camera	None	Still	Still, Video
Text Input	Numeric Keypad	Numeric Keypad, Soft Keyboard	Touch Screen, Handwriting Recognition, Built-in QWERTY-style Keyboard
Cell Interface	Voice and Limited Data	Voice and High Speed Data	Voice and Very High Speed Data
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi
Battery	Fixed, Rechargeable Lithium Ion Polymer	Removable, Rechargeable Lithium Ion Polymer	Removable, Rechargeable Lithium Ion

Figure 1: Hardware Characteristics (adapted from Jansen & Ayers, 2007)

	Basic	Advanced	Smart
OS	Proprietary	Proprietary	Linux, Windows Mobile, RIM OS, Palm OS, Symbian
PIM	Simple Phonebook	Phonebook and Calendar	Reminder List, Enhanced Phonebook and Calendar
Applications	None	MP3 Player	MP3 Player, Office Document Viewing
Messaging	Text Messaging	Text with Simple Embedded Images and Sounds (Enhanced Text)	Text, Enhanced Text, Full Multimedia Messaging
Chat	None	SMS Chat	Instant Messaging
Email	None	Via Network Operator's Service Gateway	Via POP or IMAP Server
Web	None	Via WAP Gateway	Direct HTTP
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi

Figure 2: Software Characteristics (adapted from Jansen & Ayers, 2007)

Firstly, the hardware or physical components of a mobile device include the processor, memory, display, camera, wireless, text input, and battery. Jansen and Ayers (2007) identify changes and improvements to mobile phone devices from basic to advanced and advanced to a smart device which is now known as a smartphone. Secondly, the software or the logical components of the device, start from the

operating system (OS) i.e. Apple iOS, Google Android, RIM Blackberry and others, Personal Information Manager (PIM), applications, email, messaging, web, chat and others. Figures 1 and 2 display two types of a mobile phone device's characteristics.

Punja and Mislan (2008) point out that these tools cover all features of a mobile phone device. They not only have radio capability but can also store personal data, access the Internet, send text messages known as Short Message Service (SMS) and Multimedia Messaging Service (MMS) or Enhanced Message Service (EMS), make video and audio calls, email, chat or instant message (IM), take pictures, have calendar and time functions, download/upload data and more. A mobile phone device can do much the same as a personal computer (PC) or laptop, on a much smaller and more practical device.

2.1.2 Evidence Storage on a Mobile Phone Device

Digital Forensics has a dedicated field for investigation and the extraction of data or information from a mobile phone device called Mobile Phone Forensics. It is defined as the scientific recovery of digital evidence from mobile phones using proven and accepted methods (Jansen & Ayers, 2007). According to Owen et al, (2010) Mobile Phone Forensics is one of the toughest and the most challenging fields of Digital Forensics. Information contained on mobile devices can be useful and important to law enforcement agencies when conducting an investigation in either civil or criminal proceedings.

Gonzalez, Hung, and Friedberg (2011) classify the basic information that can be retrieved and used as potential evidence from a mobile phone device. This information can be Call logs, text messages (SMS and/or MMS), contacts, calendar activities, multimedia, memorandums, notes, email, Internet browsing history, voicemails, applications, videos, map histories, geographic location information (such as Global Positioning System (GPS)) and wireless connectivity access logs. Additionally, the more difficult function of recovery of information that has been deleted from the device.

Casey and Turnbull, (2011) illuminate different locations where data can be found on a mobile phone device; embedded memory (also known as the handset), removable memory or Secure Digital (SD) memory cards and the Subscriber Identity Module (SIM) card. According to Punja and Mislan, (2008), the Network Service Provider and Universal Subscriber Identity Module (USIM) cards are other locations of information and evidence for a mobile phone device. SIM cards are normally used

on mobile phone devices that are operated under the Global Systems Mobile (GSM) network (Punja & Mislán, 2008).

A mobile phone device handset or embedded/internal memory is also referred to as board flash memory which stores and executes the data/software/programs on a mobile phone device. There are two types of flash memory: NAND and NOR. NAND is normally used on USB drives and memory cards that only store data. NOR can both store and execute software/programs that are normally used on mobile phones. Mobile phone devices can also be implemented with a hard drive memory (Punja & Mislán, 2008).

Jansen and Ayers, (2007) explain that beneath the GSM network a mobile phone device is referred to as a Mobile Station (MS) with two components: the SIM and Mobile Equipment (ME). The MS cannot function without the two components attached together. The SIM contains the subscriber's or the owner of the mobile phone device's information. It authenticates the owner's device through the network (GSM) to get access to subscribed services. Punja and Mislán (2008) also describe how the SIM card contains evidence such as Calls, Contacts, SMS, Locations and other services' information. A USIM card is used when a user needs more than one phone number assigned to his/her mobile phone device which is mainly for the 3G mobile network.

According to Jansen and Ayers, (2007), SIM cards have a Personal Identification Number (PIN) to allow access to the handset or to boot the mobile phone device. A SIM card is a smart card that contains an Electronically Erasable Programmable Read Only Memory (EEPROM). Usually only three attempts to enter the PIN are allowed before the SIM is locked. A Personal Unlocking Key (PUK) code will be used to unlock the SIM card.

Every mobile phone device that runs under the GSM network should have the following characteristics. Firstly, an International Mobile Equipment Identifier (IMEI) which is a unique 15 digit code that identifies the device within the network including manufacturer, type, model, and country of approval for the handset. Secondly, a SIM card and an Integrated Circuit Card Identification (ICCID) which is a unique 18 to 20 digit code that identifies the SIM card. Lastly, an International Mobile Subscriber Identity (IMSI) which is a unique 15 digit number stored on the SIM card. This number is made up of three codes: Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Station Identification Number (MSIN).

A memory card such as a SD card contains information such as pictures, audios, videos and documents. Basic or older model mobile phone devices do not have card slots for memory cards. The Network Service Provider (NSP) provides a source of information about a mobile phone device in terms of the subscriber's information, call history and text messages' records including location (geographic positions of the device). Table 1 describes the type of evidence that can be expected to be found on a mobile phone device.

Table 1: Evidence Related to Mobile Device (adapted from Casey & Turnbull, 2011)

Baseline phone	Hardware	Handset date and time; International Mobile Equipment Identity (IMEI)
	User-created information	Address book; SMS; calendar, memos; to-do lists
	Phone-created information	Call register (received, sent, missed)
Smart phone	User-created information	Photographs (including EXIF data); video/audio; maps, MMS; GPS waypoints; stored voicemail; files stored on system; connected computers
	Internet-related information	Online accounts; purchased media (often discoverable in embedded metadata); e-mail; Internet usage; social networking information
	Installed third-party applications	Alternate messaging and communication systems; additional capabilities; malware applications; penetration testing; other applications—anything can help provide alibi or tie to an individual
SIM card	Identifiers	Subscriber identifier (IMSI); SIM card identifier (ICC-ID)
	Usage information	SMS; abbreviated dial names/numbers; last dialled numbers; location areas

2.2 Digital Forensic Tools

A Mobile Phone Forensics investigation of a mobile phone depends on forensic tools to extract evidence or information (Jansen & Ayers, 2007). The most important characteristic of a forensic tool is its ability to preserve the integrity of the original data that has not been tampered with while extracting the data from its digital source. Forensic tools must ensure the integrity of the data and have not been changed during

extraction from a mobile phone device (Jansen & Ayers, 2006). Integrity of the data refers to the verification, validation, and authentication of the extracted digital data and it not being altered during the examination (Hildebrandt, Kiltz, & Dittmann, 2011). There are mobile forensic tools that have been specifically developed to extract evidence from mobile phone devices. Some of the popular forensic tools for acquiring data from a normal PC or laptop are “EnCase” provided by Guidance Software and “FTK” provided by Access Data (Zareen & Baig, 2010). EnCase and FTK can also be used to extract data from mobile phone devices. However, this research case scenario will use one of the world’s leading and sophisticated mobile forensic tools, XRY.

XRY is a mobile forensic tool which is used to recover evidence or data from mobile devices such as mobile phones and smart phones. XRY was developed in Sweden by Micro Systemation (MSAB). It has been awarded by the Forensic 4Cast Awards as the “Best Phone Forensic Software 2011” (MSAB, 2011). XRY has been used by law enforcement, military, and other agencies throughout the world (MSAB, n.d). It has been also involved in numerous of crimes’ investigation such as; drug dealing (Kavanagh, 2013), counter terrorism (BreakingNews IE, 2012) including real life Police television shows tracking drug trafficking in France and the death of two school girls in Korea (MSAB, 2012). XRY is more commonly used by law enforcement, government and corporate agencies throughout the world including New Zealand (MSAB, n.d).

XRY recovers data ranging from the Subscriber Identity Module (SIM) card to smart phone PIM applications (e.g. Gmail, Facebook, Skype). It supports different ranges of Operating Systems (OS) such as Windows, Android, Apple, Palm and others. It recovers data from three different locations of a mobile phone device: the **SIM card**, **Handset** (memory chip) and the **Secure Digital** (SD) memory card. It extracts and analyses data from a mobile device using two methods of extraction: logical and physical. XRY use the term “device profiles” instead of “phone supported” to determine whether a mobile phone devices is supported by XRY. For an example: Phone ‘A’ can have two device profiles supported by XRY meaning both by logical and physical extraction. However, if it’s only supported the logical analysis then one device profile of Phone ‘A’ is supported by XRY instead of saying Phone ‘A’ is supported by XRY.

XRY has been used particularly as mobile phone devices can contain important information that can be used as evidence in criminal and civil investigations (McCarthy, 2005). However, some mobile phone devices that operate or are sold within New Zealand are not supported by some forensic tools. Law enforcement agencies and some organisations are faced with difficulties and challenges during an investigation relating to particular mobile phone devices. XRY is one of the best tools available for investigating criminal evidence that involves a mobile phone device.

2.3 Forensic Tools' Testing

According to the National Institute of Justice's report (NIJ, 2010), the old version of XRY 5.0.2 was tested on some mobile devices such as HTC Touch, Samsung, Nokia, Blackberry and iPhone. Some models of these mobile phone devices like HTC were not supported by XRY. The purpose of the testing was to ensure XRY provides accurate analytic results from the data extracted on these devices. Clearly there are reasons why some models of HTC are not supported by XRY as is the case with some mobile phones in New Zealand.

Many researchers and investigators use XRY with other forensic or non-forensic tools for their research such as analysis of mobile phones (McCarthy, 2005). However, there have been criticisms regarding the performance of XRY and other mobile forensic tools (Zareen & Baig, 2010). Currently there are mobile phones on the market that cannot be supported by XRY (Walls, Learned-Miller, & Levine, 2011). Mobile phone forensic tools and toolkits are still underdeveloped in dealing with new and advanced mobile phone devices on the market (Ahmed & Dharaskar, 2008; McCarthy, 2005).

There are no standard methods for examining digital data from mobile phones (McCarthy, 2005) and validated frameworks and techniques to acquire data from mobile phone devices do not exist (Ahmed & Dharaskar, 2008). Thus, XRY is not guaranteed to work in maintaining the integrity of digital data on the device during acquisition (Mokhonoana & Olivier, 2007). However, there are guidelines provided by the Association of Chief Police Officers (ACPO) in the United Kingdom for forensic specialists, to ensure correct practices are undertaken (ACPO, n.d). In addition, the National Institute of Standards and Technology (NIST) in the USA have

its own guidelines which help to enhance policies and procedures and prepare staff with new forensic challenges (Owen et al, 2010).

Jansen and Ayers, (2007) provide some basic information about the preservation, acquisition, examination, analysis and reporting of digital data contained on mobile phone devices. Additionally they provide an understanding of the different characteristics of mobile and smart phones including cellular network capabilities. Jansen and Ayers, (2007) claim that the basic information about the capabilities of some forensic tools including XRY, have been tested to accurately acquire data or evidence from some mobile phone devices. These devices are operated on GSM, CDMA and TDMA cellular networks including recovering different task information.

2.4 Mobile Phone Data Extraction

Murphy (2010) explored and developed a process for examining mobile phone devices. Figure 3 outlines a basic overview of the process for extracting data including documentation from mobile devices. Murphy (2010) outlines the process for extracting data from mobile devices. The most critical phases relevant to this research are identification, preparation, isolation, processing, verification and documentation or reporting. Murphy, (2010) and Brothers, (2009) define different levels of logical and physical analysis which are displayed in Figure 4. **Manual Extraction** – is the physical analysis of the phone involving manual manipulation of the keyboard and photographic documentation of the data displayed on the screen. **Logical Analysis** - Connect data cable to the handset and extract data which is provided by XRY. **Physical Analysis** (Hex Dump) pushes a boot loader into the phone, dumps the memory from the phone and analyses the resulting memory dump which is also provided by XRY. **Physical Analysis** (Chip-Off) – Removes the memory from the device and reads it using another phone, EEPROM reader or another tool such as Flasher Box. **Physical Analysis** (Micro Read) - Uses an electron microscope to view state of memory.

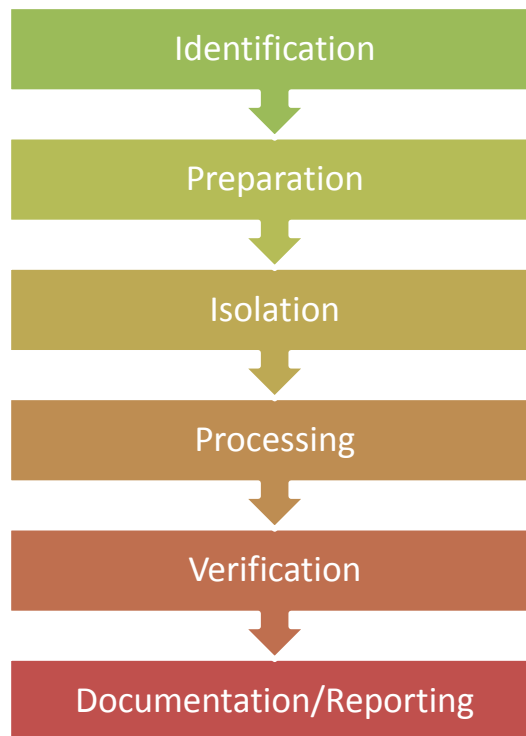


Figure 3: Mobile Phone Evidence Extraction Process (adapted from Murphy, 2010)

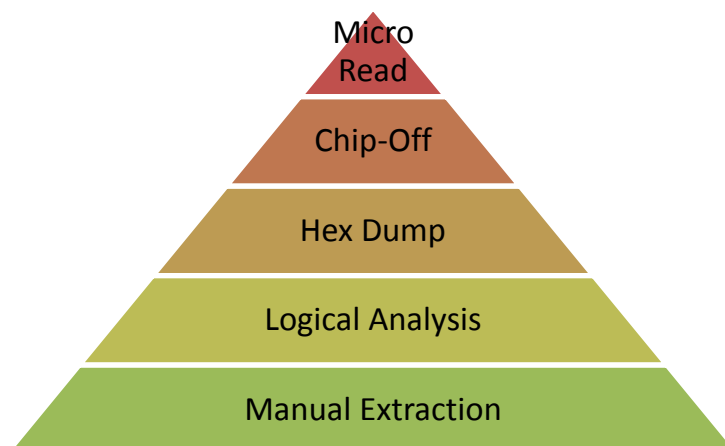


Figure 4: Mobile Phone Tool Levelling Pyramid (adapted from Brothers, 2009)

Logical and Physical (Hex Dump) analysis will be used in this research. Kim, Hong, Chung, and Ryou, (2007) define different methods to collect data from a mobile phone device's flash memory or handset. Firstly, they suggest the logical analysis of the device. However some mobile phones manufactured in Korea are not supported by forensic tools. Physical analysis was used in three methods; Flasher boxes, Joint Test Action Group (JTAG) and a chip reader. Kim et al, (2007) compare the results

from these tests with their own logical acquisition tool they created to extract data from a CDMA device. They suggest that the JTAG tool is a good method to extract data from the flash memory. This research will define the capability of XRY using both methods of extraction.

2.5 Mobile Phone Market in New Zealand

New Zealand has three main Network Service Providers (NSPs); Vodafone New Zealand (VFNZ), Telecom New Zealand (TNZ) and 2degrees and they all offer services using a different cellular network to provide their services (Keall, 2011). According to the Commerce Commission, (2011) VFNZ and 2degrees operate a 2G **Global System for Mobile** (GSM) network which is mostly used by the majority of New Zealanders and the **General Packet Radio Service** (GPRS). TNZ used to operate **Code Division Multiple Access** (CDMA) or cdmaOne network after switching from the Time Division Multiple Access (TDMA) network but have changed to **Wideband CDMA** (WCDMA) also known as the XT network. 2degrees operates the **Enhanced Data for GSM Evolution** (EDGE) network. The three NSPs also operate a **Universal Mobile Telecommunications System** (UMTS) and **High-Speed Downlink Packet Access** (HSDPA) networks.

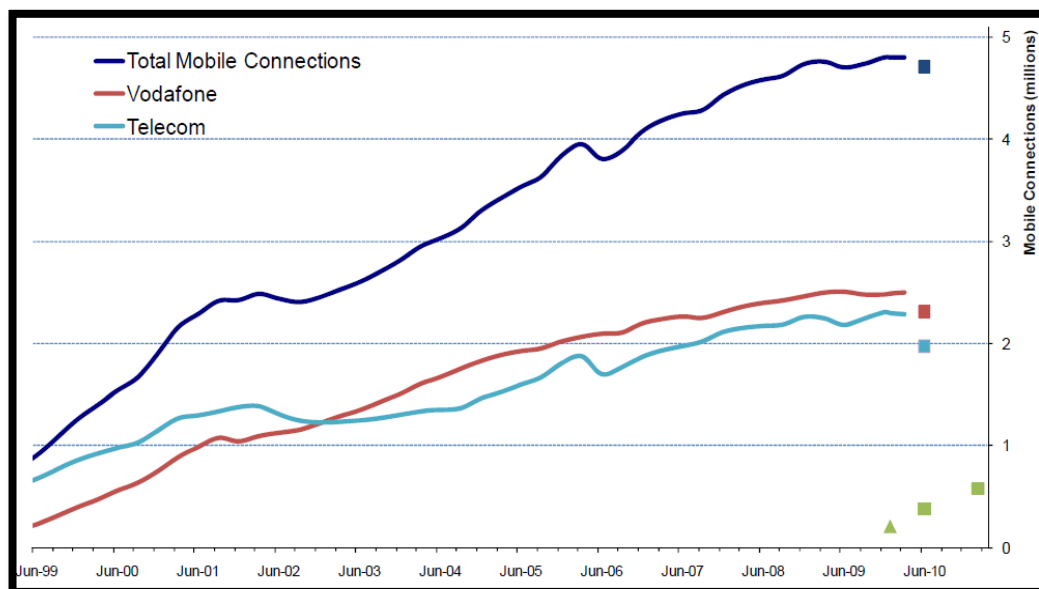


Figure 5: Telecom, Vodafone, 2degrees subscribers (Commerce Commission, 2011)

According to Commerce Commission (2011) as at June 2010 there were 4.7 million mobile subscribers in the New Zealand market dominated by VFNZ as shown in

Figure 5. Figure 6 shows the market share by subscriber between the three NSPs since 2010.

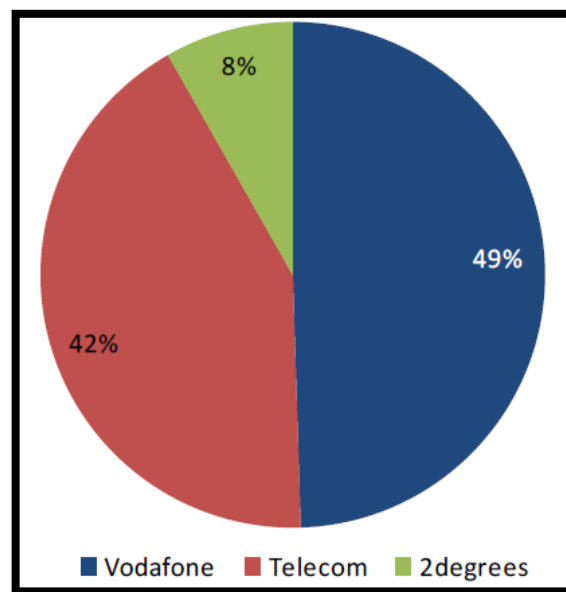


Figure 6: Market share by subscriber (Commerce Commission, 2011)

Punja and Mislán, (2008) reveal that GSM is the most dominant mobile phone network. According to Jansen et al, (2007) XRY only supports devices that operate using GSM and CDMA network cellular. Therefore, most mobile phones supplied by these three local NSPs should be supported by any mobile forensic tools. Some aspects of a mobile phone device such as brand/make, model or operating system (OS) can also determine whether such device will be supported or not by a forensic tool such as XRY based on previous work. This research will identify if the selected local mobile phone devices from each of the three NSPs will either be **fully** supported, **partially** supported or **not supported** by the latest version of XRY under the GSM or WCDMA network protocol.

TNZ is the only NSP using the WCDMA also known as the XT network (Consumer, 2012). There is another company using TNZ XT network to distribute their phone service around the country which is called Skinny mobile. Skinny mobile phone services mainly focus on pre-pay plans which are cheaper than contract plans (Consumer, 2012).

Local NSPs provide an important service within the country with a wide range of mobile phone devices to choose from. However, these mobile phone devices supplied and operated in New Zealand is questionable whether they are all able to

supported by forensic tools or not. According to Schottle, (2009) ignoring the examination of unsupported mobile phone devices will be negligent and the cause of incomplete investigations. There are alternatives in using other methods but they depend on whether such forensic or non-forensic tools are necessary for digital forensic investigation. The research will identify if the selected local mobile phone devices found in New Zealand are fully supported by mobile forensic tools such as XRY.

2.5.1 Local Mobile Phone Devices

Local NSPs supply and distribute different ranges of mobile phone device brands/makes and models. According to Vodafone NZ, (2013), it supplies a range of different types of mobile phone devices, such as classic, slide, flip, QWERTY keypad, and rugged to touch screen. VFNZ sells well-known brands such as Apple, Blackberry, HTC, Huawei, LG, Nokia, Samsung, Sony, and Vodafone. The Vodafone branded mobile phone devices are mobile phones manufactured by other companies such as Alcatel on behalf of Vodafone. Table 2a displays an example of a classic Vodafone 155 mobile phone device. According to GSMARENA, (2013), Vodafone 155 is a 2G of the GSM network.

TNZ also supplies other well-known brands including Motorola (Telecom NZ, 2013). It has its own mobile phone devices branded Telecom. Like VFNZ this kind of device is manufactured and/or supplied by other companies such as ZTE, Alcatel and others. The companies that manufacture TNZ devices can vary as it uses a number of suppliers depending on the need. Figure Table 2c displays an example of a flip mobile phone device called Telecom R1.

2degrees is one of the newest NSPs in New Zealand. 2degrees also has its own brand called 2degrees manufactured by Huawei and some of its models are manufactured by Alcatel and others. Table 2b displays an example of a touch screen smart phone called 2degrees Smart Touch (2degrees, 2013). Skinny mobile supplies one of the Huawei mobile phone devices such as Huawei U2800 as displayed in Table 2d.

The three major NSPs have their own brands and these devices are totally equipped differently in terms of different characteristics especially the OS. Well-known OS such as Android is used in one of the examples given, the 2degrees Smart Touch. The research will identify whether the targeted local mobile phone devices

selected in Chapter 4 are fully supported by the selected forensic tool (XRY) despite the make/brand, model or OS of each device.

Table 2: Local NSP Mobile Phone Devices

 <p>(a) Vodafone 155 Classic (image from www.gsmarena.com)</p>	 <p>(b) 2degrees Smart Touch (image from www.2degreesmobile.co.nz)</p>
 <p>(c) Telecom R1 (image from www.telecom.co.nz)</p>	 <p>(d) Huawei U2800 Green (image from www.skinny.co.nz)</p>

2.6 Problems and Issues

Forensic tools are highly regarded and necessary in any digital forensic field such as Mobile Phone Forensics, however there is no single tool that can perform all the required functions in a given task or case (Logan, 2011). Not all forensic tools can support all mobile phone devices or are able to extract all possible information from a device. Therefore, these forensic tools are very useful in conducting digital forensic investigations especially when many mobile devices are not fully supported by these tools.

There is a wide range of new mobile devices. Zareen and Baig (2010) believe the fast change of technologies is evident in the many models of mobile phones now available. Some mobile phones have different designs in terms of improvements to existing models and the new mobile phones introduced to the market (Jansen & Ayers, 2007).

A new generation of cellular phone technologies has been introduced; however each mobile phone model has its own cable connector from within the same brand (Punja & Mislán, 2008). Each cable per model can cause an increase in the number of different cables used by forensic investigators to conduct analysis of different mobile phone devices. Different sorts of OS used by manufacturers require different sorts of device drivers which can also be another challenge in terms of connecting between the mobile phone device and the forensic tool. Therefore, many mobile phone devices are not supported by all forensic tools like XRY (Jansen & Ayers, 2007).

Devices typically have limitations in both the width of the device supported and the depth of evidence recovered from such a device. Some investigators use non-forensic tools such as “Flasher Box” which customises the device or alters the data on the device during extraction (Jansen & Ayers, 2007). Some use it because it can extract data that mobile forensic tools cannot. Al-Zarouni (2007) suggests such a tool can be used for digital forensic investigations with some precautions and considerations. The associated problems are complicated and challenging especially in the field of mobile phone forensics as many mobile phones devices are not supported by forensic tools.

These tools are commonly used in the USA, Europe and other countries around the globe. This research is about mobile phone devices sold and provided by local NSPs in New Zealand. XRY is available in New Zealand and the expected outcome of this research is the addition of unsupported phones in the XRY database for New Zealand and the Australasia region. Suggestions for further developmental improvements of forensic tools such as XRY will also be made.

2.7 Conclusion

Chapter 2 provides a comprehensive literature review on the selected areas of this research project. Firstly, it reviews the background of Digital Forensics and how it links to Mobile Phone Forensics including the lifecycle and standard procedures of a

Digital Forensic investigation. According to the literature, XRY has been proven as one of the leading mobile forensic tools available and is the main mobile forensic tool that will be used for this research. Digital Forensics has its own issues and problems that have already been identified. Local forensic agencies deal with cases where mobile phone devices are not fully supported by forensic tools such as XRY. Therefore, mobile phones will be tested using XRY; with each brand provided by the three main local Network Service Providers.

Chapter 3 will outline the methodology for how the research will be conducted. Methods and results of previous relevant and similar research will be reviewed to design a suitable approach for this research. Research questions and sub-questions will be identified including generating a set of hypotheses to determine the research outcome. Furthermore the limitations of the research will be discussed and standard Digital Forensic investigation procedures and techniques will be used while examining the selected mobile phone devices (logically and physically) using XRY.

Chapter Three

METHODOLOGY

3.0 Introduction

Chapter 2 focused on reviewing relevant literature and identified the main areas and topics for this research project. It explained and clarified specific areas including the current problems and issues within the Mobile Phone Forensics field.

Chapter 3 is about ways and means to conduct this research by establishing a method to undertake a forensic analysis experiment, and identifying solutions or alternatives, to prevent, ease, and possibly solve these problems and issues. It is about how to extract data from a mobile phone device using forensic tools such as XRY. As mentioned in Chapter 2 XRY uses both logical and physical analysis methods to extract data from a mobile phone device. Therefore, this chapter will explain in detail how such data can be extracted from a mobile phone device.

Section 3.1 reviews previous related research about what methods have been used during their experiments. Sections 3.1.1 to 3.1.5 is a review of five previous relevant research projects, their methods used, and the results.

Section 3.2 is the research design which includes a summary of Section 3.1: it reviews current problems and issues for this research including clarifying the research question(s) and hypotheses to determine the outcome of the main research question. The research design combines ideas such as methodologies, digital forensic processes, standards, and procedures adapted from previous research.

Section 3.3 is about the data requirements in terms of what data are collected, how they are processed and analysed during the forensic analysis stage of the project. Finally, limitations for the research are outlined in Section 3.4.

3.1 Review of Previous Related Research

There is literature relating to previous research that is valuable for this project in terms of research that has used a similar approach. The following articles provide thorough analysis of mobile phone devices, evaluation of forensic tools and the challenges for forensic investigators working in mobile phone forensics on a daily basis. McCarthy (2005) developed a new method or tool to extract data from a mobile phone device. Likewise, Kim, Hong, Chung, and Ryou, (2007) also came up with a new method to extract data from a Korean CDMA mobile phone device's

internal memory (handset). Integrity of the extracted data is very important during the digital forensic analysis of a device. Thus, Distefano and Me, (2008) developed a non-forensic tool and compared its performance against one of the world's leading forensic tools. Punja and Mislán, (2008) outlined a simple research design about how to prepare and undertake a forensic analysis experiment. New mobile devices come with new features that are difficult for current forensics' tools to extract data from. Le (2012) tested the capability of the forensic tools for extracting data from a new version of Windows mobile phone devices.

3.1.1 Forensic Analysis of Mobile Phones

McCarthy, (2005) provided an overview on how to acquire information or data from a mobile phone device in a forensic manner. Acquiring data from a mobile phone device must have as little impact as possible on the device's memory to ensure the data (evidence) is not being altered during the extraction process. McCarthy, (2005) states clearly that there are no fully-accepted procedures for acquiring data from mobile phones. However, there is a wide range of software applications to extract information in a forensic way that have yet to be verified and validated.

McCarthy, (2005) discusses different methodologies for mobile phone forensic analysis including a forensic analysis model proposed by Svein Yngvar Willassen which is about the process of examining a phone. It involves firstly turning off the phone, get PINs and Password from the owner, analyse the SIM card, analyse removable memory and analyse the phone memory. There are two ways to extract data from a SIM card, either via a smart card chip reader or software application such as SIM Manager, or through the mobile phone device itself. McCarthy, (2005) explains two methods of extracting data from a mobile phone memory according to Willassen. Firstly, take the phone apart and access the memory chip directly or tap the motherboard to access the memory chip. Thus, the JTAG interface method was used to access the chip directly but it's a complicated method due to its nature.

The most feasible method for data extraction from a mobile phone device is the phone's software interface. Software such as Nokia PC Suit, Sony Ericson Sync Station, and Sony Ericson File Manager are typically phones to PC interaction via USB cables or infrared connectivity. They use a different range of protocols to access data on a mobile phone device. Protocols such as AT commands or Hayes commands assist in accessing information such as messages (SMS), call logs, contacts, model, brand, IMEI and IMSI within the GSM network. The Object

Exchange (OBEX) protocol is designed for infrared devices to gain access to data such as images, audio, ringtones and downloaded applications. Synchronization Markup Language (SyncML) is one of the protocols used to replace the old Infrared Mobile Communications (IRMC) protocol which extracts data such as contacts and calendar. Nokia FastBus (FBUS) is only used on Nokia mobile phone devices which allow access to retrieve data from the device.

The application used to extract data was primarily written in Java including C. A virtual serial connection to the mobile phone was required for communication. The following mobile phone devices were used for testing; Sony Ericsson f500i, Nokia 3220 (GSM) and Nokia 6225 (CDMA). Figure 7 displays the architecture of the application used.

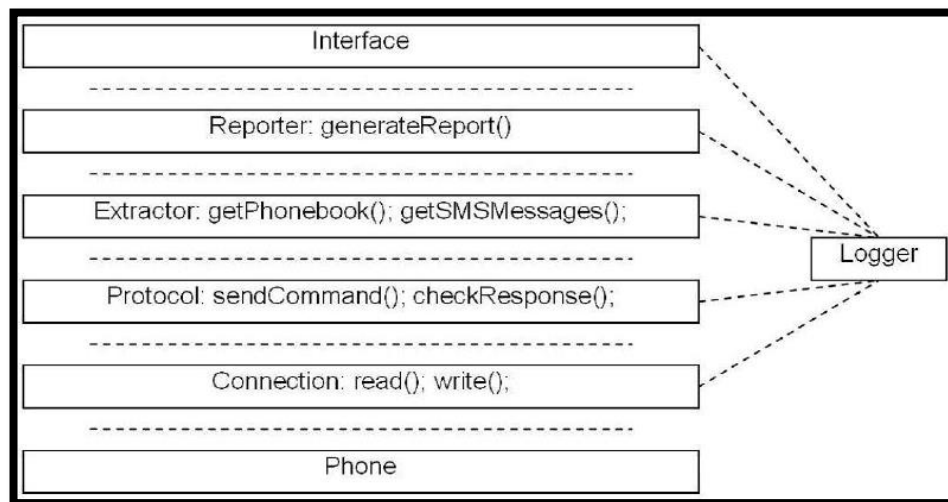


Figure 7: Research application structure

There were results after obtaining data from each of the mobile phones. Ericsson f500i retrieves phone information such as manufacturer, model, IMEI, IMSI and hardware/software version. Contacts were extracted from both the phone memory and the SIM card including SMS messages and dialled numbers. Missed and received calls were extracted from the memory including a limited portion of media files. Nokia 3220 retrieved the same results as the Ericsson f500i using the same FBUS method. Data was extracted such as missed and received calls both from the memory and SIM card. Calendar entries were able to be obtained from the phone's memory (unable to retrieve such information from the Ericsson f500i) including a limited portion of system files (media files). The Nokia 6225 (CDMA) does not require a SIM card, cannot support AT commands, nor other methods to obtain data

from the device. However, most of the data was acquired from each device apart from the deleted data and OS files.

McCarthy, (2005) believes these methods are forensics' foundations in acquiring data. Forensic software applications such as XRY, Paraben Forensic Cell Seizure, Oxygen Phone Manager II, PhoneBase, Cell Seizure, Envisage System's PhoneBase, TULP2G, and Compelson Labs' Mobiledit use the same software interfaces as non-forensic applications and all are based on the given methods. However, a concern about such methods is the integrity of the data and the lack of standardization from one mobile phone model to another.

3.1.2 Data Acquisition from Cell Phone using Logical Approach

As already mentioned in Chapter 2, there are two ways to extract data from a mobile phone; Logical and Physical analyses. Kim, Hong, Chung, and Ryou, (2007) describe a forensic tool used to acquire data from a mobile phone device flash memory or internal memory using a logical level approach. According to Kim et al., (2007) the logical method acquires files and directories from the file system of the mobile phone's memory. In Korea, most of the CDMA network mobile phones use the NAND memory which has a different method to acquire data based on the manufacturer and model of the device. CDMA phones do not have many forensic tools to support them. Mobile forensic tools are not applied to mobile phones used and supplied by Korean NSP.

According to Kim et al., (2007) most of the forensic tools analysed by NIST used the logical method (phone to PC host). However, this does not apply to all mobile phones.

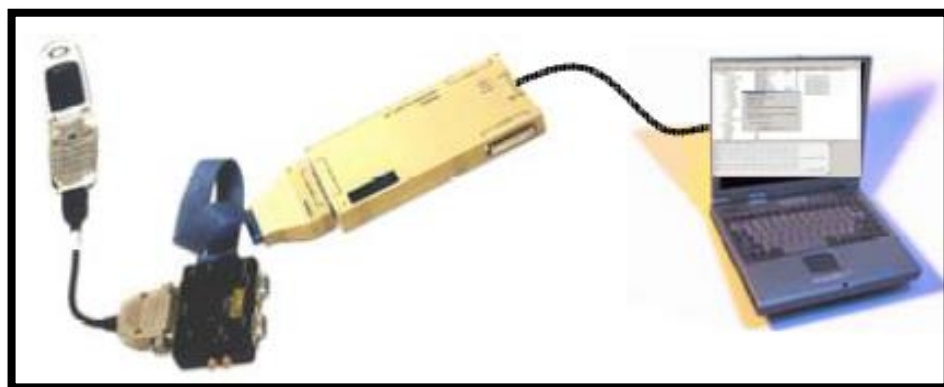


Figure 8: Data Acquisition using JTAG (adapted from Kim et al., 2007)

The physical method can be conducted using a flash boxer which is used by manufacturers for debugging and diagnosing phones and accessing data on the

phone's memory. Flash boxer tools are Twist flasher and D500 OneHAND, however not all flash boxers can access a phone's memory. A JTAG test can also be used even though it's complicated due to some mobile phone devices conceal their JTAG pins. JTAG can create a complete memory dump (raw data) from the mobile phone's memory to conduct a forensic analysis (as shown in Figure 8).

Kim et al., (2007) designed a forensic tool to acquire data from another mobile phone device (as shown in Figure 9). The tool works on a PC (Windows OS) which interacts with the target phone (Samsung SCH-E 470 and SCH-V330) via a RS-232C serial interface. The file system access and memory peek have been designed to logically acquire data from the mobile phone memory. Kim et al., (2007) focus on acquiring data such as contacts, call logs, SMS, photos including the mobile phone hardware and software information e.g. IMSI, Mobile Identification Number (MIN) and Electronic Serial Number (ESN). These data are normally stored in the phone's NAND and NOR flash memory.

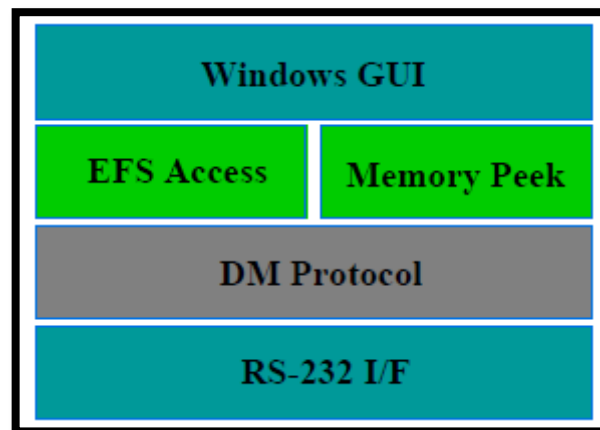


Figure 9: Acquisition Tool Design

The Embedded File System (EFS) is a file system to create, store, and manage files in a CDMA mobile phone's memory. Memory Peek acquires data by accessing an arbitrary address of the flash memory while the Division Multiple (DM) protocol which processes a request from EFS Access and Memory Peek then acquires data from the flash memory and returns acquired data to EFS Access and Memory Peek.

As a result, the Kim et al., (2007) tool was able to extract contacts, call logs, SMS, and photo data using the logical method but was not enough to retrieve deleted data from the two devices. The tool cannot be applied to all mobile phone devices. Therefore, Kim et al., (2007) believe JTAG is the best way to extract data from all kinds of mobile phone devices' memory.

3.1.3 Overall Assessment of Mobile Internal Acquisition Tool

Mobile phones have been upgraded to smart phones. Distefano and Me, (2008) introduced a new ME acquisition paradigm called the Mobile Internal Acquisition Tool (MIAT). The tool targets the smartphone market for how to acquire data from smartphone devices in a forensic manner. MIAT was put to the test by retrieving all data from a Symbian OS. Symbian is a mobile operating system developed by Symbian Ltd, previously owned by Nokia and now under Accenture (Lunden, 2011). This research will test the performance of the proposed tool (MIAT) with other Commercial Off The Shelf (COTS) forensic tools such as Paraben Device Seizure and an open source application called P3nfs.

According to Distefano and Me, (2008), MIAT acquires data directly from the internal memory slot with the acquisition application stored in the memory card. The acquisition process must be in read-only mode to ensure the integrity of the data. The mobile device should be off and all external cards removed (SIM and memory). The data from the internal memory should be copied on to an external memory card (SD card) which contains two split files; executeable and installation files for Symbian OS (.SIS file). There is no need for cables to be plugged from the device to the PC to perform the acquisition. The only forensic workstation is the device equipped with a SD card (copy of the internal memory) and the MIAT installed on the device.

The method was tested on the following mobile phone devices; the Nokia N70 and the 6630. The process steps include; firstly the extraction by MIAT, secondly the extraction by the other two tools, thirdly the extraction by MIAT again and finally the extraction by either of the two tools. The repetition of the extraction is to ensure that the integrity of the data has been maintained by the previous tool extraction process. MIAT uses Symbian S60 OS with local access to the device, Paraben uses Windows XP OS with remote access to the device via a USB cable, and P3nfs uses Ubuntu 7.04 OS with remote access to the device via Bluetooth.

The result was the MIAT was able to retrieve all elements from the target phones' memories. Figure 10 displays the results in terms of time and size of the data extracted by the three tools. There were files or data that may have changed during the acquisition process by the Paraben and the MIAT on the Nokia N70. Paraben had the most corrupt files or changes that happened to the data during the extraction process. However, the three tools were not able to retrieve deleted data from either

device. Overall, the MIAT reached the level of performance use by Paraben which is a well- known forensic tool in the industry. The MIAT should also be recognised within the industry according to Distefano and Me, (2008).

Exp	Tool	Time (min)	Size (MB)
1	MIAT	≈ 12	6.65
	Paraben	≈ 8	7.28
2	MIAT	≈ 12	6.65
	P3nfs	≈ 6	5.42
3	MIAT	≈ 50	5.73
	Paraben	≈ 15	8.86

Figure 10: Experiment results

3.1.4 Investigating Information Recover from Resold Mobile Devices

The article by Storer, Glisson, and Grispos, (2010) regards an experimental design for an ongoing investigation about the data contents of resold mobile phones device. Resold means a device that has been used before and is sold again as a second- hand phone for a cheaper than new price. The aim of the investigation is to find out the amount and type of data retained on a resold device and how consistent the recovery of such data is using forensic tools. Data on a mobile phone can be very important but are also difficult to retrieve especially deleted data due to factory restoration processes, battery removal or resetting the device. Storer et al., (2010) reveiwed two types of forensic analysis; logical and physical as well as a number of forensic applications for acquiring data from a mobile phone device.

Storer, et al., (2010) describe experimental designs for aquiring data from resold devices. Two hypotheses to guide the investigation on the devices are, H-Confidentiality: data is retained on resold devices including deleted data, and H-Consensus: different tools produce different forensic results. The experiment starts by acquiring tested resold devices (GSM network) and are checked against the forensic tools' list of devices for whether it's supported or not. The following tools were used for the experiment; the Cellebrite Universal Forensic Extraction Device; the XRY Forensics Examination Kit; and the Radio Tactics Aceso.

The tested resold mobile devices were analysed using the three tools for record informatioin such as IMEI, serial number, manufacturer, colour and model. Photos of each mobile device were taken including the SIM cards. The SIM card was removed and IMSI and ICCID recorded before extracting data i.e. contacts and

SMS messages. A physical and logical analysis using the three tools was conducted and the device's contents were manually analysed via user interface. The final approach is to analyse the recovered data such as SMS messages, emails, contacts, and call logs and classify them for potential sensitivity and/or evidence in a court of law. The results of the experiment were not available in the article but were presented at the Privacy and Usability Methods Pow-wow (PUMP), a workshop held in September 2010 about evaluating methodologies and models for studying the privacy aspects of computing systems.

3.1.5 Windows 7: Implications for Digital Forensic Investigators

Yung Anh Le (Le, 2012) conducted a forensic analysis for his master's thesis research on Windows Phone 7 (W7) mobile phone devices. W7 is a mobile phone Operating System (OS) that was released by Microsoft in 2010. According to Le (2012), it was redesigned differently compared to previous Windows' mobile OS in terms of both hardware and software. Due to the changes, forensic tools might not be able to extract data from W7. The purpose of this research is to identify what data or information can be extracted from W7 by current forensic tools and techniques.

The research was conducted in five phases. Phase one was the selection of the forensic tools that can extract data from a Windows' Mobile (WM) OS based on previous research and what data can be extracted. Phase two was about using previous results (data extracted from a WM phone) from other research to form a template of data that was loaded on to the tested W7 mobile phone. Phase three was the extraction process (logical and physical) using the selected forensic tools to extract data from the test W7 mobile phone. Phase four involved comparing results from phase three with the results from previous research. Phase five was evaluating the performance of each forensic tool based on the results from phase four.

The W7 phone HTC HD7 was the selected test phone. The double forensic analyses method was used; logical and physical. Table 3 lists the six forensic tools that were used for the logical acquisition including XRY. Table 4 displays the data that can be extracted from a WM mobile phone based on previous research results. XRY, Device Seizure and Riff Box were used for the physical acquisition. XRY and Device Seizure have the capability for physical data acquisition of WM phones and the Riff Box tool used the JTAG method extraction data.

Table 3: Forensic tools used for logical analysis

Tool (Previous Works)	Tool (Current Version)	Notes
PDA Seizure / Cell Seizure	Device Seizure 4.6	Trial
GSM .XRY / XACT	XRY Complete 6.0.1	Full Version
Oxygen PM	Oxygen Forensic Suite 2012 3.7.0.1	Trial
MOBILedit! Forensic	MOBILedit! Forensic 6.0.0.1397	Trial
Secure View	Secure View 3.4.0T	Trial
Encase	Encase 7.01.01	Academic Training

Table 4: Data extracted from Window Mobile OS

Data Type	Device Seizure	XRY	Oxygen Forensic	MOBILedit! Forensic	Secure View	Encase
Call Log	X	X	X			X
Messages (SMS/MMS)	X	X	X	X		X
Emails	X	X				X
Contacts	X	X	X	X	X	X
Calendar	X		X	X	X	X
Browsing History						
User Files	X	X	X	X	X	X
Registry	X	X				
Deleted Data	X	X				

As a result, XRY was the only tool that was able to extract data from the W7 test phone during the logical acquisition which is user image and video files. XRY should be able to extract data such as call logs, messages, emails and similar from WM based on previous results. According to Le, (2012), “*XRY provides a forensically sound method of extracting data as well as other features useful to a forensic investigation such as logging and reporting capabilities*” (p.76). Table 5 shows the range of data that can be extracted from the test phone using XRY.

Table 5: Data extracted from W7 using XRY

Data Type	XRY For WM	XRY For WP7
Call Log	X	
Messages (SMS/MMS)	X	
Emails	X	
Contacts	X	
Calendar		
Browsing History		
User Files	X	X
Registry	X	
Deleted Data	X	

During the physical acquisition of the test phone, Device Seizure was unable to retrieve data. Riff Box was able to acquire the physical acquisition (memory dump); however the

integrity of its acquisition is unpredictable due to the method used (JTAG). Overall, only one tool – XRY, was able to extract a small amount of data from the test phone (image and video files). Most of the forensic tools were not able to extract data from a W7 mobile phone device.

3.2 Research Design

Section 3.2 summarises previous research as discussed in Section 3.1 including a summary of the problems and issues this research will focus on. These problems raise many questions including the research question in Section 3.2.3. This section also clarifies how the research design is divided into four phases including the use of the traditional digital forensic process to analyse the data from the test mobile phone devices. The limited research scope could affect the outcome of this research.

3.2.1 Summary of Previous Research

McCarthy, (2005) points out that the one motive of this type of research is the importance of digital evidence from mobile phone devices for criminal and civil crime investigations. The overall purpose of each research study is to find out what data can be extracted from a specific mobile device. Also important is what other methods can be used to extract data alongside the few popular forensic tools like XRY that have been used in previous research. Integrity is another purpose which is about how accurate are the data because they can be changed during the acquisition process (Distefano & Me, 2008). Kim, Hong, Chung, and Ryou, (2007) suggested that JTAG is the best tool to retrieve data from any mobile phone device, however other researchers do not agree because it is not a forensic approach and evidence can be challenged in a court of law.

The review of previous research presents different ideas and techniques that contribute to the research method and approach for this project. The experimental design provided by Storer et al., (2010) presents a simple design for how to prepare for and how to approach this type of research. Firstly, acquire the test or target devices, extract and analyse data using logical, physical and manual approaches and finally compare results which is similar to the four-phase research design that was used by Le, (2012).

All the researchers agree on the two main forensic analyses for extracting data from a mobile phone device - logical and physical. McCarthy's (2005) approach for a forensic analysis of a mobile phone device is; start by turning the device off,

remove the SIM card and analyse it separately from the device (handset). This method is also supported by Storer et al., (2010). The first three research studies in Section 3.1 proposed and designed their own tools to extract data from a mobile phone device. Storer et al., (2010) and Le (2012) used forensic tools such as XRY.

The results of the data extracted from these studies are very important for this research in terms of understanding the idea of what sort of data can be extracted from a mobile phone device and in particular what sort of data can XRY extract, which was covered by Le's (2012) research. However, none of the studies have any results relating to extracting deleted data from a mobile phone device. Kim et al.'s (2007) research has similarities with this research although it is a different NSP, region (country), mobile network (CDMA) and mobile phone device. Storer et al., (2010) also targeted resold mobile phones and only selected mobile phones operating within the United Kingdom. The mobile phone devices that were used in these studies were mostly manufactured by well-known brands such as Nokia, Samsung, Ericsson and HTC.

3.2.2 Review of Problems and Issues

Not all forensic tools are capable of extracting data from mobile phone devices. Many mobile phone devices are not fully supported by forensic tools. Some problems occur with some mobile phones operated and sold in New Zealand. A mobile phone device can be an interesting source of evidence (potential legal evidence) stored and processed as digital data. Local law enforcement and corporate forensic agencies rely on forensic tools such as XRY for its capabilities during investigations.

Some mobile phones are not supported due to hardware and software differences. Based on previous research, some mobile phone devices are not supported due to a lack of cable availability for the device's brand or model. Mobile phone models manufactured by the same company can each have its own cable. Different mobile OS used by manufacturers require different sorts of device drivers which presents another challenge. Some forensic tools only support a mobile phone device based on its OS.

Different mobile phone networks (i.e. GSM, CDMA and others) require different applications used by some phone mobile devices. Therefore some forensic tools such as XRY are developed to support specific mobile network devices like GSM and CDMA devices.

Local NSPs such as TNZ, VFNZ and 2degrees manufacture their own mobile phones (see Chapter 2). Mobile phone device models manufactured, supplied and operated by these manufacturers are not supported by some forensic tools such as XRY. The majority of New Zealanders use or buy mobile phones (see Section 2.5.1). These types of devices provided and sold by the local NSPs are the target devices for this research.

3.2.3 Research Questions and Hypothesis

The main research question for this research is generated from previous studies and their findings and concerns the significant problems and issues faced by local law enforcement and corporate forensic agencies. The main question is:

Q₀ “What is the capability of XRY for extraction of data from a mobile phone device that is sold and operated in New Zealand?”

The main question is about identifying the capability of XRY for extraction of data or information from the research study’s target or test mobile devices. These devices are specifically manufactured for the local NSPs such as TNZ, VFNZ and 2degrees. The research will also aim to identify what digital signatures or characteristics are missing or are required from the device to be able to be supported by XRY. By answering the main question will test its null hypothesis which is: H_0 “*XRY is not fully capable of supporting the selected local mobile phone device profiles*”.

3.2.3.1 Sub-Questions

The following sub-questions will be used to discover whether XRY fully supports these devices in terms of the hardware and software characteristics of the device (i.e. cable connector, device OS, mobile network, and others.) as discussed in Chapter 2. *Q₁ “Does XRY fully support these mobile phone device profiles?”* The null hypothesis for Q_1 is: H_1 “*XRY does not fully support the selected local mobile phone device profiles*.”

According to previous research literature and Micro Systemation, XRY is capable of extracting data using both logical and physical analyses of the target devices within the GSM and CDMA mobile network. Therefore: Q_2 is: *Is XRY capable of conducting logical and physical analyses on the selected local mobile phone device profiles?* If not then H_2 is: “*XRY is not capable of conducting logical and physical analyses on the selected local mobile phone device profiles*”.

In terms of data that can be retrieved from the selected devices this sub-question aims to identify; Q_3 “*What data can be extracted from the local mobile*

phone device profiles?” Data acquisition will be conducted on the device’s handset (using logical and physical analyses) including SIM and memory card if applicable. However, if unsuccessful by any means then; H₃ “XRY was not able to extract any data during the logical and physical analyses of the selected local mobile phone device profiles.” The research outcome (recommendation and future work) will be based on the results determined by the research question(s) and hypotheses given.

3.2.4 Research Phases

The research consists of four phases as shown in Figure 11. Phase 1 is the collection and preparation stage of the research to identify the target devices including their features, hardware and software characteristics. The data storage area will be identified for each device where data can be found or stored. In addition, a sample of test data (evidence to mimic a reality forensic investigation analysis) will be generated and loaded on to these devices.

Phase 2 is the acquisition stage where XRY will be applied to these devices to extract data using the logical and physical acquisition approach. The logical acquisition will be conducted first prior to the physical acquisition. SIM and memory card (if applicable) acquisition will be conducted separately using the SIM id-cloner and memory card reader provided by XRY. Phase 3 is the analysis stage to analyse and examine data that has been extracted from each device during Phase 2. Phase 4 is the evaluation and comparison stage to assess and compare results from Phase 3 to previous research results including test data. The last stage will provide recommendations about the outcome of the research based on the results and how it affects the research questions and hypotheses.

The research method and design has been adopted from previous research studies and includes the use of the traditional digital forensic process as discussed in Chapter 2. Digital forensic guidelines and principles provided by NIST and ACPO will also guide this forensic investigative analysis research to ensure the accuracy and integrity of the data extraction from the target mobile phone devices.



Figure 11: Research Phases

3.2.5 Data Map

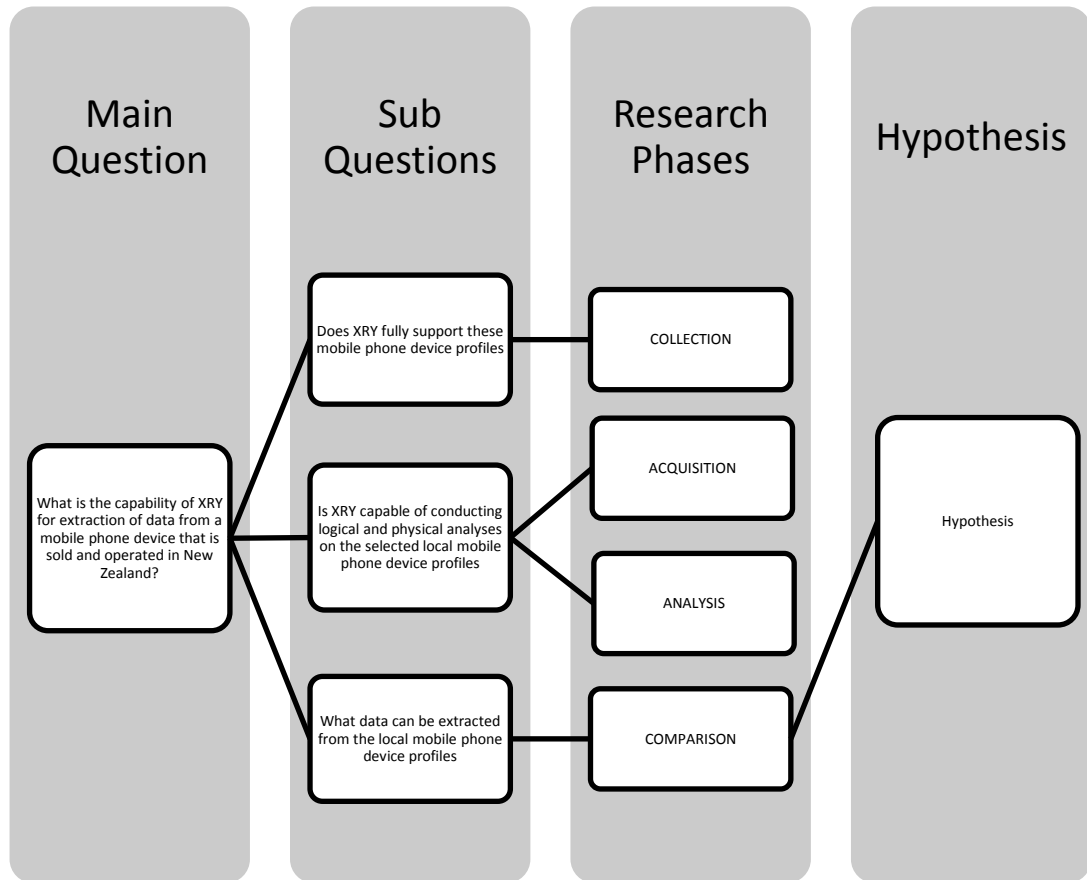


Figure 12: Data Map

3.3 Data Acquisition

Three types of data will be used in this research. First are the types of data that were extracted by XRY from previous research results. Second, test data that will be loaded manually on to the target mobile phone devices. Thirdly, the data extracted by XRY from the target mobile phone devices. These data will be collected, processed and analysed during the research phases.

3.3.1 Collection

The types of data extracted from a mobile phone device using XRY will be collected from previous research results as discussed in Chapter 2 and Section 3.1. These types of data are expected to be collected from XRY from the target devices of the research. However, XRY 6.5.1 which is the latest version might extract new types of data which have not been extracted or discovered before in previous research results.

Sample test data will be generated based and data are contact details, SMS and EMS messages, calendar entries, call logs, pictures and others. The sample test data is for the purpose of this research which will be manually imputed on the target mobile phone devices.

The last set of data will be collected from the target devices during the acquisition and analysis phase of the research using XRY. Phase four will compare the three sets of data that have been collected to determine whether XRY can extract all data from the target devices or not.

3.3.2 Process

A process will not be required for the first set of data, because it has been processed previously in other research. The list of data extracted from XRY as listed by NIST will be used including other types of data that will be expected to be extracted from a mobile phone device.

As discussed earlier test data will be entered manually into the device. The device will execute the data using data transmission (via a mobile network). Data will be transmitted among the three target devices. Test data will be logged and documented in a journal (log book) after loading it on to the device to ensure that the integrity of the data expected to be extracted from the device (third set of data) is maintained and not changed during the extraction process. Furthermore, XRY will ensure the truthfulness of the data by calculating the Message Digest (MD5) hash value to ensure each data has not been tampered with.

The last set of data will be processed using XRY by extracting it from the test device. Then it will be analysed and compared with previous results to identify what data XRY extracted and what was not. The data process will also be documented in the log book.

3.3.3 Analysis

The data will be analysed and compared during Phases Three and Four of the research. Previous research including previous XRY results has already identified the type of data that can be extracted from a mobile phone device. A list of different types of data is already known to this research. The data analysis of this research is to compare results (data) extracted by XRY from the target devices. The analysis process is to find out what data has been extracted and what data has not and then differentiate the extracted data to see what type of data can be extracted by XRY and

whether it can be located on the list of previous results (type of data) from other research studies such as NIST and Le (2012). Not all mobile phone devices will provide new features that might introduce a new type of data for the analysis process. Data analysis will determine XRY's capability of extracting data from the target devices based on the research question(s) and hypotheses.

3.4 Limitations

The main purpose of the research is to identify whether XRY is capable of extracting data from local mobile phone devices that are sold and operated in New Zealand by local NSPs.

According to previous research and guidelines, XRY can only extract data from GSM and CDMA devices. This research will target mobile network devices only from those provided by local NSPs despite other mobile network devices operating in New Zealand.

The selected target devices are branded by each of the local NSPs. Thus, the research is not focusing on other brands/makes/models sold by these three NSPs. The brands Telecom, Vodafone and 2Degrees will be used. These brands are also manufactured by other companies such as Huawei and LG which both manufacture mobile phone devices on behalf of Vodafone NZ. The selected target devices will be purchased from local NSPs' stores. The target devices will be new mobile phone devices that have not been used before.

One of the limitations is the availability of resources by XRY such as cable connectors for the selected target devices, in spite of the use of wireless or Bluetooth connection. Based on previous research this is one of the most significant problems with some mobile phone devices where each device has its own unique cable.

In New Zealand there are security measures or criteria that a mobile device must meet for the protection of data contained on these devices. GCSB, (2011) released a New Zealand Information Security Manual (NZISM) which is the national baseline technical security policy. The report describes the baseline and minimum mandatory technical security standards for government departments and agencies. Section 19.1 of this report covers information about the technical security of mobile devices including mobile phones and smartphones. The objective of the section is protecting classified information on mobile devices from unauthorised access. Thus, the target devices for this research are not covered by the NZISM report because it

only applies to government departments and agencies. Such a policy can be a factor in preventing forensic tools such as XRY extracting data from a mobile phone device.

The results (data) extracted from the target devices using XRY will be analysed. No other forensic tools will be used to extract data from the target devices. There will be recommendations about other alternative tools or methods to extract data based on previous research literature.

3.5 Conclusion

Previous research has used either different forensic tools (XRY) or non-forensic tools (JTAG) to extract data from a mobile phone device. Different methods and techniques used to extract data tended to use the logical and physical analyses' approach. The research questions and hypotheses for this research study have been formed based on reviews from other research studies including the problems and issues for this research to address. The research method has been designed and adopted from previous studies and will be conducted over four different phases; Collection, Acquisition, Analysis, and Comparison. The first step is to acquire four test local mobile phone devices and input test data, extract data from these target devices using XRY, analyse the extracted data and compare with other research results including test data. Data requirements have been discussed and it is important to ensure data has been collected, processed and analysed in a forensic manner. Limitations for this research might affect the outcome of this research. Not all mobile phone devices are supported by forensic tools in all cases.

Chapter 4 will report on the experiment's results and findings in terms of data methods specified and the methodology of this Chapter 3.

Chapter Four

RESEARCH FINDINGS

4.0 Introduction

There are different ways or methods that people use to access data i.e. pictures, audio or videos on a mobile phone device. Generally people can connect such devices to their personal computers via a USB cable and access such information. Within the Digital Forensic field there are certain methods and techniques that are used to access or extract data from any electronic device. Mobile forensic tools are made specifically to extract data from a mobile phone device in a forensic manner. These tools are capable of extracting data but not necessarily all of the data. As discussed in Chapter 2, XRY is one of these forensic tools that are used to extract data from a mobile device.

Chapter 4 is about using of XRY 6.5 to extract data from a list of selected mobile phone devices. Chapter 3 established the methodology for extracting, processing and analysing data from a mobile phone device. These extracted data will be reported as the findings or results of this research. Section 4.1 will then discuss the equipment and tools that will be used to extract data from the mobile phone devices. Previous data from other research studies and the type of data that can be extracted from a mobile phone device will be discussed in Section 4.2. Section 4.3 is the collection and preparation phase of the research where the test phones will be identified including the creation of the test data for each test phone.

The extraction process of each test phone device will be discussed in Section 4.4 while Section 4.5 will present the analysis of the raw data from each device as findings or results. These results will then be compared with previous results from other research studies together with the test data in Section 4.6. The findings from the experiment in this chapter will be discussed in Chapter 5 to determine the outcome of this research according to the research question(s) and hypotheses defined in Chapter 3.

4.1 Research Equipment

The equipment used during the research includes four mobile phone devices, a mobile phone forensic tool and a personal computer. The list of equipment is summarised in Table 6. The four mobile phone devices will be referred to as “test

phones”. These test phones were purchased locally as new and in good condition. The specifications and characteristics for each device will be discussed in Section 4.3.1.

The mobile forensic tool is the latest version of XRY as discussed in Chapter 2. XRY version 6.5 will be used for this case scenario to acquire data from the test phones using both logical and physical analyses. The XRY toolkit also provides the SIM and memory card reader device to acquire data from SIM cards used by each test phone including the memory card if applicable.

A personal computer (PC) will be used in this research and is located inside the Masters of Forensic Information Technology laboratory at the Auckland University of Technology. XRY 6.5 has been installed on the PC and the mobile forensic toolkit will be connected to the PC via USB cable. The PC specification is listed in Appendix 1. More information about the test phones will be discussed in Section 4.3.1.

Table 6: List of Equipment

Item	Name	Serial/Model Number	OS
PC	Standalone	Nil	Windows 7 Professional 32 Bit SP1
Forensic Tool	XRY 6.5	Nil	Nil

4.2 Previous Data

As discussed in Chapter 3, previous data will be used in this research to identify what types of data can be extracted from a mobile phone device. Chapters 2 and 3 present previous research results in terms of data extraction. Previous studies have used quite similar methods for extracting data from a mobile phone device using a wide range of forensic tools. In this research case scenario, previous results or types of data extracted from a mobile phone device using the mobile forensic tool XRY will be used to generate the type of data that will be the focus of this research. These types of data have been discussed in Chapters 2 and 3.

Table 7 outlined basic hardware and software information of the mobile phone device when establishing connections with the forensic tool. Table 8 summarises the types of data that can be extracted from the mobile phone device using XRY based

on previous research results. These types of data will be expected to be extracted from a mobile phone device using the XRY 6.5 toolkit.

Table 7: Mobile Phone Device Hardware and Software Information

Device Name	Serial Number
Model	ESN
Manufacture	MIN
IMEI	PUK
IMSI	SIM Number
Operating System	ICCID

Table 8: Expected Data

Contacts	Videos
Messages (SMS/MMS)	Pictures
Call Logs	Internet Browsing History
Emails	Notes
Calendar	Tasks
Audios	Deleted Items
File Systems	User Files

4.2.1 XRY Device Model Features

According to MSAB, (2011) XRY can extract data such as Bluetooth information,

Table 9: XRY Logical Supported Features

SIM Contacts	Files
SIM Calls	MMS
SIM SMS	E-mail
Contacts	Calendar
Calls	Tasks
SMS	Notes
Pictures	Memory Card
Audio	Cable
Video	Bluetooth

Maps and Global Positioning System (GPS) locations, Smartphone applications such as Facebook, Gmail, Skype, and database file systems such as bookmarks, searches and others. Table 9 displays common features of a mobile phone device that are supported by the XRY toolkit during the logical analysis.

Once the target device establishes connection with the XRY toolkit via cable, Bluetooth or infrared, then XRY will determine whether the following features of the target device are able to be supported in terms of extracting data. SIM features are data that can be extracted from the device's SIM card, while the Memory Card feature is the extraction of data contained inside the device's memory card if applicable. The Cable and Bluetooth features are about whether the device can be connected to the XRY via cable or Bluetooth.

4.3 Collection and Preparation

Phase One is the most critical phase of this type of research (Murphy, 2010) as it includes establishing identification, preparation and isolation of the device before progressing to Phase Two. Inside Phase One is the collection and selection of the target mobile phone devices or test phones as well as the creation of the test data by preparing and generating test data that will be manually inputted into each test phone. Each test phone device is then segregated and the research environment including equipment that will be needed for the forensic analysis experiment is set-up.

4.3.1 Test Phones

There were 25 mobile phones devices that were considered for this research as discussed in Chapter 3. However, four new mobile phone devices were purchased and selected from a list of local mobile phone devices which were available through local electronic stores. These test phone devices must at least operate within the GSM mobile network provided by the local NSPs. Table 10 illustrates the four selected test phones including the type of mobile phone as discussed by Jansen and Ayers (2007), the NSP and the type of network that the device will be able to operate under, the manufacturer and the OS. Full specification and features for each test phone can be found in Appendix 2.

Table 10: Tests Phones Network

Test Phone	Type	OS	Network	NSP	Manufacture
Phone 1	Smartphone	Android	GSM & HSDPA	VFNZ	Huawei
Phone 2	Advanced	Native	GSM & UMTS	TNZ	ZTE
Phone 3	Basic	Native	GSM & WCDMA	TNZ	Samsung
Phone 4	Smartphone	Android	GSM & UMTS	2degrees	Huawei

4.3.2 Test Data

Test data have been created and inputted onto each test phone and are based on the expected data type listed in Table 8. Three test phones have GPS or Assisted-GPS (AGPS) features, with data created for such features in terms of searching for a location using the GPS navigation if applicable. Table 11-14 summarises the test data that was created on to each test phone as well as deleted data.

Before inputting data on to each test phone some of the devices needed to be registered within the network. The NSP requires a PIN to activate the device for verification and authentication to the network, as well as to verify its owner or user. Each test phone was successfully activated through its dedicated network. These devices are in as-new condition and there is no need to reset each device or restore factory settings. The date and time on each device needs to be set up according to New Zealand Standard Time which is Auckland/Wellington UTC/GMT +12 hours.

The type of data has been divided into two parts; **actual data** and **deleted data**. The ‘actual data’ are data that has not been deleted from the test phones and can still be viewed on the device. The ‘deleted data’ are data that has been deleted from the device and cannot be viewed. Data has been intentionally deleted for the purpose of establishing whether the forensic tool is able to recover such data.

The test data has been created based on the features available on the device. There are test data that is not applicable to be created on some of the test phones devices. **Contacts** have been created and stored inside the SIM Card and phone. **Calls** have been divided into three categories; dialled, received and missed. There two types of messages created; **SMS** and **MMS** which has been categorised as received and sent. Data such as Calls, Contacts and SMS can be stored on the device’s SIM card. **Files** refer to data created by the user such as **Pictures**, **Audios** and **Videos** including the device’s system or OS files. Some files can be directly loaded or saved on the device’s **Memory Card**. **Events** has been created using the

Calendar feature on each device including **Tasks**, **Notes** and **Memorandum**. Phone 1 and Phone 4 can access the Internet while connecting to a Wi-Fi and access the Internet which creates **Internet Browse History**. All test phones have **Bluetooth** connections to pair up with other devices to exchange data. An **E-mail** account has been set up on Phones 1, 2 and 3 for the purpose of sending and receiving email between the three devices. Not all devices have the same features and each has to be treated differently. For instance, only Phones 1 and 4 have the **GPS location** feature. Data have been deleted from each device intentionally to observe whether the same data will be recovered.

Table 11: Phone1 Test Data

Type of Data	Actual Data	Deleted Data
Contacts	9 x Contacts (5 SIM + 4 Ph)	3 x Contacts
Calls	12 x Dialed Calls 4 x Missed Calls 2 x Received Calls	1 x Dialed Call 1 x Missed Call 1 x Received Call
SMS	4 x Received SMS 1 x Sent SMS	1 x Received SMS 1 x Sent SMS
Pictures	2 x Pictures*	2 x Pictures
Audio	1 x Audio*	1 x Audio
Video	7 x Videos	1 x Video
MMS	3 x Sent MMS 1 x Received SMS	1 x Sent MMS 1 x Received MMS
E-mail	Set as a Gmail account. Username: mfit.aut@gmail.com 1 x Sent email 7 x Received email	NA
Calendar	1 x Event	1 x Event
Notes	1 x Note	1 x Note
SIM Card	5 x Contacts	1 x Contact
Memory Card	6 x Folders containing files 6 x Pictures 1 x Video	NA
Internet Browse History/Search	Web search – auto Web search – aut Visited: www.aut.ac.nz	NA
GPS Location	Navigation from 44 Matapan Road, Panmure to 55 Wellesley St East, Auckland	NA
Network Information	Connected: TNCAP99529F (private Wi-Fi)	NA

Table 12: Phone2 Test Data

Type of Data	Actual Data	Deleted Data
Contacts	9 x Contacts (6SIM + 3Ph)	1 x Contact
Calls	3 x Dialed 3 x Received 4 x Missed	1 x Dialed 1 x Received 1 x Missed
SMS	3 x Received (1SIM) 1 x Sent	1 x Received 1 x Sent
Pictures	3 x Pictures*	1 x Picture
Audio	2 x Audios*	1 x Audio
Video	1 x Video	1 x Video
MMS	1 x Received 1 x Sent	1 x Received 1 x Sent
E-mail	1 x Outbox	NA
Calendar	1 x Event	1 x Deleted
SIM Card	6 x Contacts 1 x Received SMS	NA
Internet Browse History	Visited: Yahoo Telecom nz.m.yahoo.com	NA

Table 13: Phone 3 Test Data

Type of Data	Actual Data	Deleted Data
Contacts	14 x Contacts (9 SIM + 5 Ph)	2 x Contacts (Ph)
Calls	7 x Dialed 2 x Received 4 x Missed	2 x Dialed 2 x Received 3 x Missed
SMS	3 x Received (2 SIM) 1 x Sent	1 x Received 1 x Sent
Pictures	3 x Pictures	1 x Picture
Audio	2 x Audios	1 x Audio
Video	1 x Video	1 x Video
MMS	1 x Received 2 x Sent	1 x Received
E-mail	Set as a Gmail account. Username: mfit.aut@gmail.com 9 x Received email	NA
Calendar	2 x Events	NA
Tasks	2 x Tasks	NA
Memo	2 x Memos	NA
SIM Card	9 x Contacts 1 x Received SMS	NA
Internet Browse History	Visited: Yahoo Telecom nz.m.yahoo.com and www.aut.ac.nz.	NA

Table 14: Phone 4 Test Data

Type of Data	Actual Data	Deleted Data
Contacts	12 x Contacts (8SIM + 4Ph)	1 x Contact
Calls	18 x Dialed 2 x Received 5 x Missed	1 x Dialed 1 x Received 1 x Missed
SMS	6 x Received 1 x Sent	1 x Received 1 x Sent
Pictures	2 x Pictures*	1 Picture
Audio	2 x Audios*	NA
Video	2 x Videos	NA
MMS	2 x Received 1 x Sent	1 x Sent
E-mail	Set as a Gmail account. Username: mfit.aut@gmail.com 1 x Sent email 9 x Received email	NA
Calendar	2 x Events	NA
Notes	2 x Notes	NA
SIM Card	8 x Contacts	NA
Memory Card	Pictures, Audios and Videos	NA
Internet Browse History/Search	Web search: www Web search: aut Visited: www.aut.ac.nz Web search: xry msab Visited: www.msab.com	NA
Network Information	Connected: TNCAP99529F (private Wi-Fi)	NA

4.4 Acquisition

Phase Two is the extraction or acquisition stage of the research. XRY 6.5 was used to extract data as discussed in Section 4.3 as well as to identify whether the forensic toolkit is able to extract data from the test phone devices using both logical and physical acquisition.

XRY 6.5 has been installed on the PC and the forensic toolkit synchronised with the PC before the extraction process begins. The test phone device needs to be identified by the forensic toolkit by either automatic detection or by using the “device finder” option to ensure that such devices have been listed within XRY’s list of untested and tested or supported device profiles. There are three ways the device can be connected to XRY, either via cable, Bluetooth or infrared. For this research study the cable and Bluetooth methods were used. Once the device is identified by XRY then either the logical or physical extraction process will begin.

MSAB advises that when the device is not supported or not being identified by the toolkit, use alternatives to choose a similar device profile using the device finder. The device finder will look for similar types of phone examples; types of devices, manufacturer and OS, and will use such a device profile to identify and extract data from the test phone device.

XRY 6.5 was able to extract data from each test phone device by logical acquisition only. Some test phone devices were not able to be identified and neither supported by XRY. Therefore, another method was used (another similar device's profile) to extract data. Section 4.4.1 to 4.4.4 will discuss in more detail each test phone device's acquisition process using XRY 6.5.

4.4.1 Phone 1 - Acquisition

XRY was able to identify Phone 1 by using the device finder and the device name as suggested by MSAB. Phone 1 was connected to XRY via cable. However, the "USB Debugging" option on the device had to be enabled. The "USB Debugging" was made for development purposes and can be used to exchange or copy data between the device and the computer. Therefore, this option needed to be enabled to ensure the connection between XRY and Phone 1. These settings needed to be activated for all test phones before synchronising.

XRY recognises Phone 1 as "Vodafone 858 Smart" referred as DP1. The device overview shows that the "Vodafone 858 Smart" device profile is supported by XRY and has been tested. According to the device overview provided by XRY, not all features can be supported or in other words not all data can be extracted from the Phone 1 device profile and were marked as either: full, partial or not supported. Figure 13 shows an overview of Phone 1 device's profile as identified by XRY. A **Logical Extraction** was conducted on Phone 1 with the intention to extract the test data that have been generated in Table 11. The logical extraction process was successful and XRY was able to extract data from Phone 1. The entire status of the extraction was successful. Appendix 3A shows the logical extraction process log of Phone 1.

Device Overview : Vodafone 858 Smart		
Network		GSM
OS		Android
Logical		
Connectivity		
Cable	✓	microUSB Cable
Bluetooth	✗	Not Supported
Recommended Media		Cable
Features		
Contacts Sim	✓	Full Support
Calls Sim	✗	Not Supported
SMS Sim	✓	Full Support
Contacts	✓	Full Support
Calls	✓	Full Support
SMS	✓	Full Support
Pictures	✓	Partial Support
Audio	✓	Partial Support
Video	✓	Partial Support
Files	✓	Partial Support
MMS	✓	Full Support
E-mail	✓	Partial Support
Calendar	✓	Full Support
Tasks	✗	Not Supported
Notes	✗	Not Supported
Memory card	✓	Full Support

Figure 13: Phone 1 Device Profile Overview

The **Physical extraction** method was not available for the Phone 1 device profile. XRY can only support logical extraction for the Phone 1 device profile. Therefore, the physical extraction for Phone 1 cannot be completed. Another device profile was also used to extract data from Phone 1. The device profile was “Huawei U8160” referred as DP1U which is equivalent to the Phone 1 model number which apparently can be the same mobile phone device. However, the device profile has not been tested by XRY. Thus, a logical extraction was conducted using this device profile to extract data from Phone 1. XRY was able to extract data from Phone 1 using the “Huawei U8160” device profile. However, even this device profile cannot complete a physical extraction of Phone 1. Finally, data was successfully extracted from Phone 1 and processed using logical extraction under a tested and untested device profile. Both device profiles were not able to conduct a physical extraction on Phone 1. The extracted data from Phone 1 is analysed in Section 4.5.

4.4.2 Phone 2 - Acquisition

Phone 2 is not supported by XRY. The device cannot be found in the device finder or detected automatically when establishing connection with XRY using a cable and Bluetooth. As discussed in Section 4.4, another similar device profile can be used to extract data from the test phone device. Another device profile was used to extract data from Phone 2. When choosing a suitable device profile to use, the similarity was based on the manufacturer (ZTE), OS (Native) and type of phone (flip), therefore a

“Telecom R7 XT” referred as DP2 device profile was used in this case. Figure 14 shows an overview of the device profile that was used to extract data from Phone 2.

The selected device profile was able to conduct a **logical extraction** of Phone 1. The extraction process was successful however XRY encountered some problems extracting data from Phone 2 and advised that data may not be complete. Appendix 3B displays the logical extraction log of Phone 2 with some unknown device errors. Such errors may have caused the problems during the extraction process. However, XRY successfully processed and decoded the extracted data that was able to be taken out from Phone 2. XRY is not able to complete a **physical extraction** of the data under the selected device profile. It only supports logical extraction which is the same as the Phone 1 device profile. Therefore, the physical extraction for Phone 2 cannot be completed. Finally, data have been extracted from Phone 2 using a different device profile because XRY does not support Phone 2. The extracted data from Phone 2 is analysed in Section 4.5.

Network	GSM
OS	Brew
Logical	
Connectivity	
Cable	✓ ZTE Cable 2
Bluetooth	✗ Not Supported
Recommended Media	Cable
Features	
Contacts Sim	✓ Full Support
Calls Sim	✓ Full Support
SMS Sim	✓ Full Support
Contacts	✓ Full Support
Calls	✓ Full Support
SMS	✓ Full Support
Pictures	✓ Full Support
Audio	✓ Full Support
Video	✓ Full Support
Files	✓ Partial Support
MMS	✗ Not Supported
E-mail	✗ Not Supported
Calendar	✓ Full Support
Tasks	— Not Available
Notes	— Not Available
Memory card	✓ Full Support

Figure 14: Telecom R7 XT Device Profile

4.4.3 Phone 3 - Acquisition

XRY was able to identify Phone 3 via a cable and Bluetooth connection. It recognised Phone 3 under the “Samsung GT-E3210” referred as DP3 device profile. Figure 15 shows an overview of the device profile of Phone 3. The device has been tested and supported by XRY. However, according to the overview not all features are supported and some are either fully or partially supported.

Device Overview : Samsung GT-E3210		
Network		GSM
OS		Proprietary
Logical		
Connectivity		
Cable	✓	microUSB Cable
Bluetooth	✓	Supported
Recommended Media		Cable
Features		
Contacts Sim	✓	Full Support
Calls Sim	✗	Not Supported
SMS Sim	✓	Partial Support
Contacts	✓	Partial Support
Calls	✓	Partial Support
SMS	✓	Partial Support
Pictures	✓	Full Support
Audio	✓	Full Support
Video	✓	Full Support
Files	✓	Full Support
MMS	✗	Not Supported
E-mail	✗	Not Supported
Calendar	✓	Partial Support
Tasks	✓	Full Support
Notes	✗	Not Supported
Memory card	✓	Full Support

Figure 15: Phone 3 Device Profile Overview

Data was able to be extracted from Phone 3 using **logical extraction** supported by the device profile. The entire logical extraction process was completed successfully without any errors. Appendix 3C displays the logical extraction log of Phone 3. However, as with the other device profiles the Phone 3 device profile does not support **physical extraction** of the device. The extracted data was decoded and processed by XRY and the results are analysed in Section 4.5.

4.4.4 Phone 4 - Acquisition

A device profile for Phone 4 was not found nor identified by XRY. As with Phone 2, another device profile can be used to identify and extract data from Phone 4. Two device profiles were selected and only one was able to extract data from Phone 4. The first device profile selected for its similarity with Phone 4 is “Huawei C8600” referred as DP4 device profile based on the manufacturer, the OS and type of phone. However, the device profile does not have the same type of network device as Phone 4. Phone 4 is a GSM type of device network yet the device profile selected is for CDMA which might explain why XRY cannot identify Phone 4 under the DP4 device profile.

The second selected profile which was used is DP1U and was based on its similarities with Phone 4 as well. It was the same device profile that was used to extract data from Phone 1. However, this device profile has not been tested by XRY

but it was able to extract data successfully from Phone 1 using the logical method. Therefore, it was used to extract data from Phone 4. The selected device profile overview is presented in Figure 1.

A **logical extraction** was able to be conducted on Phone 4 under the selected device profile. XRY successfully extracted data from Phone 4 but according to the results' extraction log presented in Appendix 3D, there were system data that were forbidden or failed to be extracted from Phone 4. However, data have been extracted using the logical extraction method. As discussed in Section 4.4.1 the selected device profile cannot support physical extraction. Therefore, **physical extraction** for Phone 4 cannot be completed. The previous device profile DP4 supports physical extraction but it cannot identify Phone 4. Finally, data have been extracted from Phone 4 using a different device profile because XRY does not support Phone 4. The extracted data from Phone 4 is analysed in the next section.

4.5 Analysis

Phase Four is the analysis of the data that have been extracted from each test phone device as discussed in Section 4.4. Only the logical analysis method was able to be conducted, so this chapter will analyse data from the extraction method. Phones 1 and 3 were able to be identified and supported by XRY and the other two test phone devices were identified and supported under a different device profile. Data have been successfully extracted from these two devices using their own device profile. Data was also extracted from Phones 2 and 4 by using different device profiles.

General information about each device including IMEI, Model, NSP and other details have been compared against the full specifications of each test phone device in Appendix 1. Device information recovered by XRY is matched to the device specifications for verification. The only exception from the general information for each device on the extraction log is for Phones 2 and 4, because two different device profiles were used. However, other information should be identical with other general specifications of the device.

The following sections will identify and describe the data type that has been extracted from each device using the logical extraction method as well as whether the test data was fully recovered including deleted data. Extracted data from each test phone device are described in Appendices 3A to 3D.

4.5.1 Contacts and Calls

XRY was able to extract the list of **contacts** for each of the test phones. Contacts stored on the SIM card and the device itself was recovered. XRY was able to recover one deleted Contact from Phone 2 which was stored on the SIM card. However, deleted Contacts on the other three test phone devices have not been recovered by XRY. All received, missed and dialled **Calls** have been recovered from Phones 1, 3 and 4. There was inconsistency with Phone 3's Calls test data. The numbers were not correctly displays. However, no deleted calls have been recovered from each of the test phone devices.

4.5.2 SMS, MMS and Email Messages

SMS messages were recovered from Phones 1, 3 and 4. These messages were stored on the SIM card (such as Phone 3) and on the device itself. XRY was able to recover **MMS** messages from Phones 1 and 4. No **MMS** messages were recovered from Phones 2 and 3. According to the device profile overview of Phone 3 and the device profile overview used by Phone 2, they do not support or recover **MMS** messages. There were no deleted, sent or received **SMS** or **MMS** recovered from the four devices.

XRY was able to recover **Email** information such as an email address and email messages from Phone 1. The email address was "*mfit.aut@gmail.com*" with the password. Email information from Phones 2, 3 and 4 were not able to be extracted by XRY. The only information to be identified was whether each test phone device used the Email feature where user activities are recorded as system files in the extraction data (see Appendix 3B to 3D). These files record information when the user creates or uses the Email feature of the device, however, the actual email details such as account or message are not held. Therefore, the device profile used by Phones 2 and 3 cannot support Email. The Phone 4 device profile was not able to recover Email.

4.5.3 Pictures, Videos and Audios

User files such as pictures, videos and audios were successfully recovered from each of the test phone devices apart from Phone 4. No Videos were able to be extracted from Phone 4. XRY was able to recover every user file that was stored on the device and the memory card (removable media). All the test data pictures were recovered including default user files that come with the device including files that were sent or

received as MMS messages. According to each device profile that was used, XRY can support or extract such data however no deleted user files were recovered.

4.5.4 Calendar, Tasks, Notes and Memo

Phones 1, 3 and 4 were able to recover **calendar** events that were created on each device. There was a Phone 1 event called “*Birthday*”, Phone 3 events called “*Birthday*” and “*Anniversary*” and a Phone 4 event called “*Birthday*”. Calendar events for Phone 2 were not extracted but were recorded within the system files that were extracted from the device. As previously mentioned these files do not show specific details of an event just the date of the event and other metadata. The Phone 2 calendar event is displayed in a system file called “*calendar20130720800_0.vcs*”.

Test data have been created for the **Tasks** and the **Memo** features and are only applicable to Phone 3. A list of tasks has been recovered from Phone 3 such as “Go Party” and “Go Holiday” but no Memo data recovered. Test data for the **Notes** feature was created for Phones 1, 2 and 4 and there were no apparent notes recovered from each device. System files identified Notes that have been created on Phone 1 - “31-05-2013 5:31:36 AM UTC” with the file name “*note_pad.db*”, and on Phone 4 but with no specific details. There were no deleted calendar events recovered on any of the devices. Web History, Searches and GPS Locations

Internet history was recovered from Phone 4 with two regularly visited websites “*www.aut.ac.nz*” and “*www.msab.com*” featuring and **web searches** of the word “*www*”. However, web search results did not include the other two words “*aut*” and “*msab*”. For Phone 1 only web searches were recovered but no web history. Web searches of the word “*auto*” and “*aut*” were recovered but not for the visited website “*www.aut.ac.nz*”. No web history was recovered from Phones 2 and 3.

XRY was able to extract **GPS location** data from Phone 1 which was the only device using the navigation feature. The location was to get directions from 44 “*Matapan Road, Panmure, Auckland*” to “*55 Wellesley St East, Auckland*”. There was no test data created for Phone 4, neither for Phones 2 and 3 because they do not have Navigation or GPS features. Other data from a Google Map Navigation feature were also recovered. These data was GPS coordinates of pictures that have been taken with the device’s built-in camera. These coordinates indicate the whereabouts of the picture (see Appendix 3A).

4.5.5 Network Information

Phones 1 and 4 were able to connect to private Wi-Fi called “TNCAP99529F”. XRY was able to recover the network details of the Wi-Fi connection including its password from Phone 1 only. There was no network information recovered from Phone 1 which might be something to do with the untested device profile that was used by Phone 4. Phone 1’s information was also extracted using the same untested device profile and did recover network information. The problem might therefore be caused by the device itself where some part of the extraction process of Phone 4 blocked XRY from extracting certain files. Phones 2 and 3 do not have the feature to connect to Wi-Fi.

4.5.6 Others

Data such as User Files, Contacts and SMS were retrieved from both SIM and Memory cards. Some Contacts on the four test phone devices were able to be extracted from the SIM cards including SMS messages only from Phone 3. Phones 1, 3 and 4 have the capability of using a memory card but only 1 and 4 did. Mostly user data was recovered from Phones 1 and 4 memory cards or removable media.

System files mentioned earlier are recorded as unrecognised files. These files will generate a log about the file such as name, path, created time, storage and other information. There are some occasions in this section that these files were able to determine the existence of the data. It shows data was created but cannot be retrieved. Therefore, these files can be related to such data.

4.6 Comparison

Phase Four is about comparing this study’s results to previous studies’ results about the type of data that can be extracted from a mobile phone device. The XRY 6.5 forensic toolkit was used in this research and retrieved most of the data including some variation with the results. Most of the expected type of data (see Table 11 to 14) was able to be recovered in this research. There are also data that were not supported or extracted by the forensic toolkit. However, compared to the results of extraction data from previous research studies, new types of data have also been recovered.

Table 15 presents the type of data that was extracted from each of the test phone devices. The ‘x’ represents actual data that was successfully extracted from the device and ‘xd’ represents both actual and deleted data was successfully

extracted from the device. The ‘*’ sign means there were variations in the test data in terms of missing data or other ways to read the test data as discussed in Section 4.5. The ‘NA’ means the particular type of data is not applicable to the test phone device. The ‘-’ icon means the particular type of data cannot be extracted or supported by the forensic tool.

Table 15: Test Phones Results using XRY 6.5

Type of Data	Phone 1	Phone 2	Phone 3	Phone 4
Contacts	x	xd	x	x
Calls	x	-	x*	x
SMS	x	-	x	x
MMS	x	-	-	x
E-mail	x	_*	_*	-
Pictures	x	x	x	x
Audio	x	x	x	x
Video	x	x	x	-
Calendar	x	_*	x	x
Tasks	NA	NA	x	NA
Memo	NA	NA	-	NA
Notes	_*	-	NA	-
SIM Card	x	x	x	x
Memory Card	x	NA	NA	x
Web History/Search	x*	-	-	x*
GPS Location	x	NA	NA	NA
Network Information	x	NA	NA	-

XRY was able to extract data from each device using the logical extraction method only. None of the devices used were able to extract data using the physical extraction method. The type of data recovered from each device was based on the capability of the test phone devices. Phones 1, 3 and 4 were able to recover most of their test data with some variation in the results. Phone 2 used a different device profile to Phone 4 which was enabled to be supported by XRY and extract data. Phones 1 and 3 were more successful in extracting test data because both are supported by XRY. Although Phones 2 and 4 are not supported by XRY, Phone 4 was able to recover most of its data because the device profile used is quite similar to its model although it has not been tested by XRY. Phone 2 retrieved the least amount of data extracted due to the factor that both Phones 2 and 4 are supported by XRY.

4.7 Conclusion

Extracted data from a mobile phone device can be vital to a forensic investigation. The data could be relevant to the case and potentially used as evidence in a court of law. Therefore, the integrity of such data is very important. Forensic tools such as XRY use the logical and physical extraction methods and the extracted data should be accurate and complete. However, not all devices are supported by the tool and/or not all data can be extracted due to the tool's limitations in retrieving data from a specific device.

XRY 6.5 was used in this forensic experiment to extract data from the four selected mobile phone devices (see Section 4.3.1). Test data was created and inputted in to each device as part of the experiment. These test data was generated in Section 4.3.2 based on previous research studies outlined in Section 4.2, and Chapters 2 and 3.

Data was extracted from each device using the XRY 6.5 logical extraction method outlined in Section 4.4. The physical extraction method was not able to support the test phone devices. Data was extracted from each device with some variation. These findings were processed and analysed in Section 4.5. Section 4.6 compares the findings and results with previous studies' results including the test data. Most of the test data was recovered from some of the devices including from other storage areas such as the SIM and Memory Card. Unfortunately, most of the deleted data was not recovered.

Chapter 5 will evaluate and discuss the findings from Chapter 4 to answer the research question(s) and appraise the hypotheses. There will be more discussion in the next chapter on the findings and the capability of the selected forensic tool including recommendations and future work.

Chapter Five

DISCUSSION OF FINDINGS

5.0 Introduction

Chapter Five will discuss the research findings that were reported in Chapter Four. These findings will establish a research outcome in terms of discussing the scope of the research. The discussion identifies both the strengths and weaknesses of the research including its limitations. It will explain and discuss why such devices cannot be supported, what data was extracted, what method was used, and what new ideas can be derived from the extracted data. Within the discussion reference will be made to relevant previous sections to audit the accountability of the research based on problems and issues stated in Chapter Two including comparisons with previous work as reviewed in Chapter Three. Section 5.1 uses these results to answer the main research question and the sub-questions, and also tests each hypothesis for whether it can be accepted or rejected.

The findings discussion has been divided into four parts; Section 5.2.1 will discuss the test phone devices. Section 5.2.2 talks about which devices were able to be recognised or officially supported by XRY 6.5. There were two methods that were expected to extract data however only the logical method was available which is discussed in Section 5.2.3. Data that were extracted from each test phone device are discussed in Section 5.2.4 including deleted data in Section 5.2.4.5. Interesting information about one particular device profile is discussed in Section 5.2.4.6. Finally, recommendations are made in Section 5.3 on how to improve the capability of mobile forensic tools to be able to support not only this study's test phone devices but others also.

5.1 Research Questions and Hypotheses

The research question(s) and hypotheses were derived based on the literature review in Chapter Two. The main research question captured the entire scope of this research. The research sub-questions were developed to ensure that all parts of the main research question were systematically covered. Chapter Three presented the methodology used in Chapter Four to collect data from the test phone devices.

The findings reported in Chapter Four will be used to answer the main and sub research questions as well as to test the hypotheses as discussed in Section 3.2.3.

The research questions and hypotheses will be presented in Tables 16-19 with arguments ‘for’ and ‘against’ to the given questions and their associated hypothesis including a conclusion at the end. ‘For’ will support (accepts) the argument, ‘Against’ does not support (rejects) the argument and ‘Indeterminate’ means the findings were unable to prove or disprove the hypothesis.

Table 16: Main Research Question

Research Question (Q0): <i>What is the capability of XRY for extraction of data from a mobile phone device that is sold and operated in New Zealand?</i>	
Hypothesis (H0): <i>XRY is not fully capable of supporting the selected local mobile phone device profiles.</i>	
For <p>Phones 2 and 4 device profiles have not been tested by XRY or included in the list of supported devices.</p> <p>Not all the test data was able to be extracted by XRY from each of the mobile phone devices. Most of the deleted data was not extracted from each of the test phones.</p> <p>None of the test phone devices were able to have data extracted using the Physical analysis method.</p>	Against <p>XRY 6.5 was able to extract data from each of test phones devices.</p> <p>Phones 1 and 3 were already supported by XRY. Their device profiles had already been tested by XRY and were included in the list of supported devices.</p> <p>Logical analysis was the only method that was able to extract data from the four test phones.</p>
Conclusion: <p>Based on the findings reported in Chapter Four, XRY partially supported each of the test phone devices. In other words XRY was able to extract data from each device using the logical analysis method. Two device profiles (DP1 and DP3) for Phones 1 and 3 were identified and supported by XRY. Phones 2 and 4 used different device profiles (DP2 and DP1U) to extract data because both test devices cannot be identified or supported by XRY.</p>	

Most of the deleted test data was not able to be extracted from each device. The logical analysis was the only method that could extract data from the devices based on the device profiles that were used. The physical analysis is not available nor does it support any of the used device profiles.

Therefore, XRY supports each device based on its device profile whether it is supported and tested. Some device profiles supported both logical and physical analyses. However, in this case only a few data was extracted from each device using the logical analysis method only. The integrity of the extracted data is very important however based on the findings there were other different device profiles that were used to extract data from Phone 2 and 4 devices because they could not be identified by XRY.

Table 17: Sub-Question One

Sub Question (Q1): <i>Does XRY fully support these mobile phone device profiles?</i>	
Hypothesis (H1): <i>XRY does not fully support the selected local mobile phone device profiles.</i>	
For <p>XRY was not able to identify Phones 2 and 4 or no such device profile was found.</p> <p>XRY was not able to support Phones 1 to 4 in terms of extracting all data including deleted data from each device.</p> <p>XRY was not able to conduct a physical analysis on each device.</p>	Against <p>XRY only supported Phones 1 and 3 in terms of identifying the device and matching its device profile before extracting data from each device.</p> <p>XRY partially supported each test device by extracting a few data using the logical analysis method.</p>
Conclusion: <p>XRY partially supported each test phone device. It only supported Phones 1 and 3 by identifying each device and matching their device profile which was tested and supported by XRY. The mobile forensic tool was not able to identify Phones 2 and 4 device profiles. Not all test data can be recovered by XRY from each</p>	

device using the logical analysis method including deleted data. XRY was able to extract data from Phones 2 and 4 by using a different device profile. The device profiles used by each test phone device cannot conduct a physical analysis of each test phone device.

Therefore, XRY cannot fully support each device (Phones 2 and 4) but at least a few data can be extracted from each device. XRY can only define fully, partially or not supported specifically in terms of what data can be extracted from a device as presented in Section 4.4 Figure 1 to 3, but overall XRY only partially supports these devices.

Table 18: Sub -Question Two

Sub Question (Q2): <i>Is XRY capable of conducting logical and physical analyses on the selected local mobile phone device profiles?</i>	
Hypothesis (H2): <i>XRY is not capable of conducting logical and physical analyses on the selected local mobile phone device profiles.</i>	
For XRY was not able to conduct a physical analysis on each test phone device.	Against XRY was able to conduct a logical analysis on each test phone device.
Conclusion: According to Chapter Two, XRY can extract data from a mobile phone device using both logical and physical analysis methods. In this case XRY was able to extract data from the test devices using the logical analysis method only. The physical analysis cannot be conducted due to the device profile that was used in the experiment. The four device profiles that were used cannot support physical analysis or physical dumping for each test phone device. Phone 4 was tested with one of the device profiles that support physical dumping, however it was unsuccessful or failed to identify the test device. Therefore, according to the findings, XRY can only conduct logical analysis on these devices.	

Table 19: Sub-Question Three

Sub Question (Q3): <i>What data can be extracted from the local mobile phone device profiles?</i>	
Hypothesis (H3): <i>XRY was not able to extract any data during the logical and physical analyses of the selected local mobile phone device profiles.</i>	
For <p>Most of the deleted data that were created in Section 4.3 cannot be extracted.</p> <p>Some test data was not extracted because they were not supported by XRY under the device profile that was used.</p> <p>Some data was missing from the extraction.</p>	Against <p>XRY was able to extract different types of data from each test device including one item of deleted data from Phone 2.</p> <p>XRY was unable to extract the actual data but was able to identify some information about data stored on the device's extracted system files.</p>
Conclusion: <p>XRY was able to extract data from each test device. The type of data extracted from XRY is listed in Table 10. The 'Memo' type of data was not able to be extracted from Phone 3. Only one item of deleted data was able to be extracted from Phone 2. Most of the deleted data cannot be extracted using the logical analysis method. Some data was uncertain to be extracted due to the fact that some are fully, partially or not able to be extracted by XRY (see Figures 1 to 3, Section 4.4). There were some variations in the data when they were extracted and processed by XRY. Some data was missing from the actual data and some actual data was not able to be extracted although their information was found in file systems that were extracted by XRY. It will prove that such data was created on the device via an application.</p> <p>Therefore data was extracted from XRY using the logical analysis method only. However, not all data including deleted data was able to be extracted apart from one single item from one of the devices.</p>	

5.2 Discussion of Findings

Section 5.2 will discuss the results and findings from the forensic analysis experiment of the four test phone devices which are reported in Chapter Four. The discussion is based on the problems and issues that were discussed in Chapter Two. It will identify whether these local test phone devices are able to be supported by forensic tools such as XRY.

The discussion will begin with some information about the four tests phone devices then which devices are supported or not supported by XRY. Thirdly, it will discuss what data was extracted including the method used. Finally, it's about the overall performance of the mobile forensic tool during the experiment. All these aspects will be considered with reference to the problems and issues as discussed in Section 2.6.

5.2.1 Mobile Phone Devices

The four test mobile phone devices as listed in Table 10 Section 4.3.1 are operated within the following mobile network; GSM, WCDMA, HSDPA and UMTS. These devices were specifically made to function within these networks. Local NSPs provide such network services as listed in Section 2.5. These types of network devices should be supported by forensic tools such as XRY which can support GSM and CDMA network devices (Jansen & Ayers, 2007). All the test phones are recognised by XRY because they are all operated within the GSM network (see Table 10).

Mobile phone technology changes rapidly producing newer models. The four test devices were supplied and sold by local NSPs. Phones 1, 2 and 4 were manufactured by different companies on behalf of each NSP. Phone 3 was made by its own company but supplied by one of the NSPs. There are different sorts of OS used by manufacturers that require different sorts of device drivers which can also be another challenge in terms of connections between the mobile phone device and the forensic tool. Therefore, Phones 1 and 4 have the same OS while Phones 2 and 3 have a "Native" OS or an OS that comes with the device developed by its manufacturer.

Connecting to XRY via cable is very important so that both the test device and the tool are able to communicate. According to previous research, each cable per model

can cause an increase in the number of different cables used by forensic investigators to conduct an analysis of different mobile phone devices. Phones 1, 3 and 4 used the same kind of cable to connect to XRY which is called “microUSB”. Phone 2 used “ZTE Cable 2”. Therefore, at this stage the cable was not an issue because it was supplied by XRY. The next step is whether these devices can be identified or supported by XRY.

5.2.2 Recognised and Unrecognised Device

MSAB (2011) defines their support of mobile phone devices in a different way and use the term “device profile” rather than of phone support. Phones 1 and 3 were able to be identified by XRY with their device profiles. In other words XRY can identify and support these two devices using their device profile. Once they are supported XRY provides a device profile overview about what kind of data can be extracted from it using the device profile. Section 4.4 Figures 13 to 15 present an example of a device profile.

Phone 1 used its device profile called “Vodafone 858 Smart” (DP1) and Phone 3 used “Samsung GT-E3210” (DP2). Their device profiles’ overviews are shown in Section 4.4, Figures 13 and 14. According to Phone 1 device’s specifications shown in Appendix 2, its device model number is “U8160-U”. Therefore, another device profile can be used by Phone 1 which is supported by XRY called “Huawei U8160 (Untested)” (DP1U). This device profile has not been tested by XRY which means that Phone 1 can be extracted using two device profiles. Phone 1 was used to extract using DP1 and DP1U while DP2 could be used to extract data from Phone 2.

No device profile was found for Phones 2 and 4. These devices were not able to be identified by XRY. However, according to XRY if a device is not supported or not able to be identified using a similar device profile that is supported by XRY is another option. Similarity was based on the type of device, manufacturer and OS. Phone 2 device’s profile was selected on the type of device (flip flop) and manufacturer (ZTE). The OS is the same because it was developed by the same manufacturer. As a result, Phone 2 can use the device profile called “Telecom R7 XT” (DP3), another device profile similar to Phone 2. The device profile’s name represents one of the local NSPs and its mobile network. Therefore, it’s one of the local devices that have already been supported by XRY. Phone 2 was able to use DP3 to extract data.

Phone 4 has the same position as Phone 2. Phone 4 device's profile was selected on the type of device (touch), manufacturer (Huawei) and OS (Android). Two possible device profiles were considered. Firstly, a device profile called "Huawei C8600" (DP4). However, this device profile cannot identify Phone 4 due to network differences. Such a device profile is a CDMA kind of network device but Phone 4 is GSM and UMTS. Secondly, the DP1U device profile was able to extract data from Phone 4. However, it has not been officially tested by XRY but is based on the Phone 1 results using DP1U which apparently extracts the exact data using DP1.

Section 2.6 raised some issues around whether a different brand, model, OS or type of device can be a factor in it not being recognised by a forensic tool. In this research, it is not a factor as the forensic tool will be able to identify the device or use another device's aspects to make it recognised by XRY and able to extract data from Phones 1 to 4. It can be a factor if the device is a new branded model that has not been seen or dealt with before requiring further actions to be taken to make it recognised which will be discussed later in Section 5.3.

5.2.3 Logical and Physical Extraction

Chapter Two reviewed forensic tools such as XRY are able to extract data using the logical and physical methods as discussed in Section 2.2. During the experiment the results reveal that the logical and physical analyses of the device are based on the forensic tool itself. The XRY device profiles that were selected to use for Phones 1 to 4 can only support or conduct logical analysis. DP4 was the only option because it can conduct both logical and physical analyses of a device. It was applied to Phone 4 but it was unsuccessful. Therefore, the other device profiles that were used can only conduct logical extraction and analysis of each test device.

The physical analysis cannot be conducted on the test devices. XRY can only support the selected device profiles for logical analysis but not physical analysis. As mentioned earlier the logical or physical analysis of a device is based on whether the tool can support it or not. According to Chapter Two, XRY can support both logical and physical analyses. Thus, further improvements on the tool itself will be necessary especially for the device profiles that cannot conduct both logical and physical analyses.

5.2.4 Research Data

Data extracted from a mobile phone device are very important and this is one of the areas that raised some issues. According to Jansen and Ayers, (2007) devices typically have limitations in both the width of the devices supported and the **deepness of evidence recovered** from each device. Test data was created in Section 4.3.2 which was derived from previous research results about types of data that can be extracted from a mobile phone device using XRY. As a result, XRY 6.5 was able to extract at least some data from each test phone. Section 4.6 Table 15 summarises the final results of the data extracted from each test phone device.

5.2.4.1 Phone 1

XRY was able to extract most of Phone 1's test data including some bits of data about the test data created for "Notes". XRY declared that Notes is not supported based on the DP1 device profile overview (Section 4.4.1 Figure 13). However, XRY was able to identify some bits of information about the Notes test data "*Go Gymnasium Tomorrow*" was created in Phone 1 and extracted as system files (Files/Database). There was no specific information about the note that was created, but it was able to identify that there was a note created in the device according to the system files. In this case, there was no expectation that Notes would be extracted however it was valuable to understand that the device's system files (Files/Database) recorded system activities including Notes' activities that were created using the Notes application called "NotePad". The recovered system file only recorded the time the 'Notes' application was used to create the note which was "*31-05-2013 5:31:36 AM UTC*" and the name of the database file "*note_pad.db*" including other metadata about the system file. This is relevant because the date the note was created is truly correct. These pieces of information despite the actual data will prove that the user was creating notes. The data was only recovered using the logical analysis method. There might be a possibility to recover the actual data about the Notes if a physical analysis applied but not in this case.

XRY did not extract Web History data about the visited website "*www.aut.ac.nz*", but was able to extract Web Searches' data. According to the DP1 device profile overview, Web Searches/History data is not included however XRY was able to extract some bits of data from Phone 1. Relevant extracted data results from Phone 1 using DP1 and DP1U is presented in Appendix 3A. Both device

profiles extracted the same amount of data. However, DP1U has not been officially tested by XRY but was capable to extract data from Phone s 1 and 4.

5.2.4.2 Phone 2

Phone 2 is not officially supported by XRY 6.5 because it is not currently recognised and another device profile (DP2) was used to extract data from the device as discussed in 5.2.2. As a result, XRY was able to extract test data from Phone 2 using DP2 apart from Calls, SMS, MMS, Web History and Notes. There were some bits of information that were extracted about Emails' data which has been recorded as system files (Files/Unrecognised). According to Table 12, there was an "outbox" email created and system files recorded bits of information about this recorded under (Files/Unrecognized) results of the extraction data. It's the same situation with Phone 2's Notes' results where there were bits of system files' information to indicate Email activity. Likewise, the Calendar event that was created had only some bits of information recorded within the system files able to be extracted and presented under Files/Unrecognised data in Appendix 3B. According to the DP2 overview in Section 4.4.2 Figure 14, Calls, SMS, MMS and Notes are fully supported by XRY. However, XRY was not able to extract the following from Phone 2 including Web History test data.

DP2 is for a different model or device and not specifically for Phone 2. Therefore, DP2 cannot be guaranteed to fully work on Phone 2 and in this case only extracted minimal data. After considering the results from Phone 2, the test data that were extracted is very important. Although DP2 is not fully extracted of some of the most important data, some data was worth extracting. If there was a device profile it might have been a different result. Likewise with Phone 2 there might be a possibility to recover other test data if a physical analysis applied.

5.2.4.3 Phone 3

XRY was able to extract data from Phone 3 using its device profile (DP3). Like Phone 1, there were only the two devices that were identified or can be supported by XRY. According to its device profile in Figure 15, XRY should be able to extract all types of data apart from Calls on the SIM, MMS, Email and Notes. That result was correct based on the findings from Phone 3 as summarised in Table 15. However, there were inconsistencies with the Calls results in terms of the phone numbers. They were not accurate according to the test data.

Likewise, the other test phone device's results have some activities about the test data recorded within the systems' files extracted by XRY and presented as Files/Unrecognised data. These system files logged the Email application activity on Phone 3 and were able to record the time the user accessed the application. There were test data created for Web History, however XRY could not extract such information because it is not supported by XRY under the DP3 device profile. Therefore overall, most of the data that was expected to be extracted from Phone 3 was successful using the DP3 device profile. It would better if other test data created could be extracted by XRY. However, it's similar to other selected device profiles where DP3 can only conduct a logical analysis on the device. There might be a likelihood of recovering other test data if a physical analysis was available for DP3. Nevertheless, Phone 3 was able to be supported by XRY in terms of test data that were able to be extracted successfully.

5.2.4.4 Phone 4

Phone 4 had the same position as Phone 2. It is not officially supported by XRY 6.5 because it was not recognised. Thus, another device profile (DP2) was used to extract data from the device as discussed in 5.2.2. Apparently there is no device profile overview for DP1U because it has not been tested by XRY. Phone 1 was tested using DP1U and it was able to extract the same amount of data when using DP1. Thus, DP1U was used on Phone 4 because DP4 cannot be used.

According to Phone 4 results in Table 15, most of the data was extracted compared to the Phone 1 findings apart from Email and Notes. No Notes' test data was able to be extracted probably because Phone 1 used the "NotePad" application while Phone 4 used the "OI Notepad" application. Two different applications might be the reason why there were no details or bits of information about the Phone 4 Notes' test data extracted.

XRY was not able to recover Email test data from Phone 4 using DP1U. Phone 1's Email test data was able to be extracted by both content and email account details. However, the Email test data from Phone 4 were not able to be extracted including any recordings within the system files. Both Phones 1 and 4 are manufactured by the same company but have different versions of the OS. Phone 4 has the Android v2.3.6 which is newer than Phone 1s OS (see Appendix 2) and may be the cause of the problem because Phone 4 is not officially supported by XRY due to its unknown device profile.

The rest of Phone 1's Web searches' test data was able to be extracted by XRY apart from the Web History. XRY only extracted the Web History but not the rest of Phone 4's Web Searches' test data. These are the missing pieces of information from XRY for both devices. Phone 4 connects to a private network as does Phone 2 (see test data Table 11 and 14 Section 4.3.2.) XRY was able to extract such network information from Phone 2 using both DP1 and DP1U but not Phone 4.

XRY was able to extract most of the data compared to Phone 1's results using DP1U. It's vital that valuable data extracted to an investigation can be extracted successfully. Phone 4 is not supported by XRY and the selected device profile (DP1U) can address the problem by extracting most of the data. However, MSAB needs to test such a device before allowing it to become officially identified and as part of XRY's supported device profiles together with Phone 2. There might also be the possibility to recover test data from other device profiles used in this research if a physical analysis applied.

5.2.4.5 Deleted Test Data

As discussed previously, the device profiles used only support or conduct the logical analysis method. According to previous research it's very complicated to extract deleted data. There was only one item of deleted data that was able to be extracted from Phone 2, (Table 15). According to MSAB, (2013) the physical analysis method has the advantage of revealing deleted data which may not be available through a logical analysis. Thus, in this research the logical analysis method was mostly used because none of the used device profiles were able to conduct a physical analysis. However, there was a single piece of deleted data that was extracted from Phone 2 during a logical analysis, which was one of the Contacts that was stored on the device but was deleted intentionally. As a result, XRY was able to recover it from Phone 2 using a different device profile logical analysis. Overall no deleted data can be extracted using a logical analysis method by XRY. If a physical analysis applied then it would be a different result.

5.2.4.6 Extracted Device Specification

Appendix 4 summarises Phones 1 to 4 device specifications extracted by XRY 6.5. It presents information about the Device Profile, IMEI, IMSI, Network Code and others. Appendix 2 summarises each test phone device's full specification during Phase One of the research experiment as discussed in Section 4.3.1. There were some differences in some details about two of the test phone devices that were recorded

prior to the experiment, comparing what XRY extracted from the device. Phone 1's model recorded by XRY using DP1 and DP1U is called "Vodafone 858" but the model number recorded on the device (behind the battery) and inside the phone manual is "U8160-U". Thus, this model number is associated with the DP1U device profile's name. In other words, XRY has two device profiles that linked to Phone 1 as discussed in Section 5.2.2. Thus, this situation can lead to confusion when apparently DP1 and DP1U are for the same model as recorded in Appendix 2.

However, it might be that just one model is registered using two different names or model numbers. As discussed in Section 2.5.1 some of the devices supplied by local NSPs are manufactured by a different company on behalf of the NSP. That might be the reason why they call such a device using the NSP's name instead of the actual model number of the device. Phone 1 is an example where XRY recorded the model number as "Vodafone 858" but on the device itself it is "U8160-U" manufactured by Huawei. However, only one device profile is supported by XRY which is DP1 but not DP1U. It is difficult to understand what the point is in having two device profiles doing the same work for one model.

According to Appendix 4, Phone 4 has been recorded by XRY as manufactured by 2degrees which is one of the local NSPs. On the device itself it records Huawei. These raise more questions about how accurate are the information that forensic tools such XRY can extract. XRY is able to read and extract data out of these devices so a lot depends on what data it extracts. Another possible factor could relate to how the manufacturer registers/names of these devices.

The key point is not just the integrity of data that can be extracted from a device but also the device itself. Different model numbers and other device specification details which are not matched with the device itself could make their data inadmissible in a court of law. It could also cause confusion for forensic analysts when conducting forensic investigations.

5.3 Recommendations

According to the findings, only two devices were officially supported by XRY and the other two were not. However, data was still able to be recovered from each device. The unsupported devices (Phones 2 and 4) were able to be identified by XRY using other models' device profiles which allowed test data to be recovered from these devices.

The next step is how to get these devices recognised by XRY or included in the XRY list of supported device profiles. If the device is not supported by XRY then it's possible to use another similar device profile. Once the extraction process is successful with such a device profile then the vendor can be informed about such results. The vendor can mark an untested device profile but once it is tested then it will officially be supported by XRY either logically, physically or both. Phones 2 and 4 are good examples of unsupported devices.

This is another way MSAB can improve its tool capability and contribute to the digital forensic community. It is the only way to solve the problems and issues with unsupported devices with both parties working together to ensure that unsupported devices be able to be recognised by the tool. Mobile phone device manufacturers are another entity that can improve forensic investigation capability of devices. It's about sharing such knowledge and ideas and working together to solve such problems and issues.

The research questions have been answered and the hypotheses were tested. Finally, local mobile phone devices that are sold and operate within New Zealand are supported by XRY but not as fully as others. According to the final results two of the test devices are supported and the others are not. However, there was still data able to be extracted from these unsupported models which make them untested supported devices.

5.4 Conclusion

The findings from the research experiment conducted in Chapter Four have been reviewed and discussed in Chapter Five. These findings determine the entire scope of this research in terms of answering the main research question and sub-questions and also test each hypothesis.

The research question(s) and hypotheses were answered and tested in Section 5.1 which reveals that all mobile test phone devices were able to be supported by XRY. Two of them are not officially supported but because XRY was able to extract data from each of them, they are untested supported devices. H_0 was accepted due to XRY 6.5 was able to extract from all devices. However some of them have not been tested by XRY. H_1 was accepted for Phones 1 and 3 but rejected on Phones 2 and 4. H_2 was rejected because XRY 6.5 cannot perform a physical analysis on the test phone devices but it was accepted because it can perform logical analyses. H_3 is

accepted due to some test data was able to be extracted. Overall, XRY 6.5 is capable of extracting data from the test devices but not all them.

Identifying the device depends on whether XRY can support such a device. Phones 1 and 3 were identified but not Phones 2 and 4. However, XRY was able to extract data from each unsupported device using other device profiles. If the device has a similar model that is already supported by XRY data can be extracted from it. Cables, make, brand and OS were not factors in making a mobile device be supported by XRY 6.5. XRY extracted most of the test data from each phone with some new information to identify these test data. However, XRY could not extract deleted test data during the logical analysis apart from one item recovered from Phone 2. There were two device profiles that were identified in XRY that can support Phone 1. XRY recorded a different model number/name for Phone 1 compared to the device specification. Therefore, such a model number/name should be unique to avoid confusion during a forensic analysis.

Recommendations have been provided to ensure that unsupported devices could be identified by XRY in the future. The input from forensic analysts about unsupported devices will assist MSAB to improve the capability of XRY to be able to support such devices and to ensure both logical and physical analyses can be conducted on each supported device profile.

Chapter Six will summarise and conclude the research about the significant findings reported in Chapter Four which has been discussed in this chapter. A summary of the research questions and hypotheses' discussions will include possible areas for further research based on the limitations discovered in the research.

Chapter Six

CONCLUSION

6.0 Introduction

The motive for this research was the potential for digital evidence from electronic devices such as mobile phones, to be investigated, in relation to many different types of crime including e-crime (see Chapter 1). However, the problem is that not all mobile phone devices are supported by forensic tools. Chapter 2 identified the problems and issues within this field of study and which has tested the capability of forensic tools such as XRY 6.5 to extract data from models that are sold and operated within New Zealand.

Chapter 3 outlined the methodology to conduct a forensic experiment on the selected local mobile phone devices. This method was derived from previous similar research studies and was used to extract data from the test devices using XRY. The results and findings from the forensic experiment were used to determine the outcome of the research in terms of answering the research question and testing the hypotheses. These findings were reported in Chapter 4 and were analysed and discussed in Chapter 5. The discussions in Chapter 5 were focused on these local devices and whether they were supported by XRY based on the extracted data and the method that was used. In addition, recommendations were made for forensic analysts around how to draft such models or kinds of devices to enable them to be supported by XRY and perhaps even other forensic tools.

This Chapter concludes this research and the summary of findings as reported in Chapter 4 including the research question (see Section 6.1). There were limitations to the research study such as areas that were out of scope (see Section 6.2). Section 6.3 identifies future research work that needs to be considered to cover other related areas.

6.1 Summary of Findings

Test data were generated and put into the four test phone devices. The types of data created based on previous research are discussed in Chapters 2 and 3. XRY 6.5 was able to extract some of the test data from each device using the logical method only. As a result for Q_0 and H_0 , XRY is capable of extracting data from each phone device, however not all data, including deleted test data. Q_1 and H_1 are rejected due to

Phones 1 and 3 being the only devices that were officially supported by XRY. Phones 1 and 3 are identified and recognised by their device profiles; DP1 and DP3 while Phones 2 and 4 used other model device profiles; DP2 and DP1U. DP1U was not tested by XRY.

The logical analysis method was used to extract data from each test phone device due to their profiles which can only conduct logical analysis. The physical method cannot be conducted because the test phone devices have device profiles that do not allow XRY to support physical dumping or analysis which rejects Q₂ and H₂; only logical analysis can be conducted on the test phone devices. However, XRY was still able to extract most of each device's test data using the logical analysis method which accepted Q₃ and H₃.

XRY was able to extract most of Phone 1's test data except the Web History data and some variation of its Notes' test data. In other words only bits of information about the data were found within the extracted system files of the device. Some test data were not extracted but bits of information about such data are recorded as system files (Files/Unrecognised). These bits of information are associated with the test data as activity logs. Phone 2 is not supported by XRY but some of its test data were able to be extracted including a deleted Contact using a different device profile (DP2). There were some variations on the Calendar and Email test data. Nothing was recovered from Calls, SMS, MMS, Web History and Notes. No deleted data from Phone 2 were able to be extracted apart from one Contact. XRY was able to recover most of Phone 2's data apart from MMS, Memo and Web History test data including the Email system files. No deleted data were able to be extracted from Phone 3. XRY was able to extract most of Phone 4's test data apart from deleted data. There were some missing Web Search test data and XRY could not extract Email, Notes and Network Information data from Phone 4. DP1U has not been tested by XRY however it was able to use and extract most of Phone 4's data.

Phone 1 was able to be recognised by XRY with two device profiles; DP1 and DP1U. Although out of the scope of this study it is interesting that both device profiles are available on XRY except DP1U which has not been tested. Both device profiles can extract the same amount of data from Phone 1. In other words one model (Phone 1) is supported by two device profiles (DP1 and DP1U) which are both the same device. This may cause confusion as they are two different devices with

different names (model numbers) but are the exact same device. These types of issues depend on how the manufacturer names/registers each device.

The test phones were selected from the list of local mobile phone devices that are sold and operated by local NSPs. Some of these devices are manufactured by other companies on behalf of local NSPs. The research reveals that these devices (Phones 1, 2 and 4) are not unique or very different from other well-known models. These devices have their NSP name with their other device characteristics (model numbers) recorded under the manufacturer. Therefore, forensic tools such as XRY should be able to support these kinds of devices based on previous models from the manufacturer that are already being supported by the forensic tool.

Due to the findings the main research question has been answered and some of the sub-questions were either accepted or rejected based on the results for each device. Some of the test phone devices were not officially supported by XRY but data was able to be extracted from them.

6.2 Limitations of the Research

The limitations in the research have been discussed earlier (Section 3.4). Most of the devices were GSM network devices. Other mobile network devices such as CDMA should probably have been included in the research because XRY can also support CDMA devices (no SIM card). The test mobile phone devices were selected from the three major NSPs and purchased only from local stores.

As discussed in Section 3.4 a limitation might include the forensic tool's resources in terms of its cable or connectors for the mobile phone devices. However, in this case the cable was not a problem at all. However the nature of the device is significant whether new or old or a XRY supported or unsupported model. The research was only tested on local mobile phone models that were manufactured by the three disclosed mobile phone manufacturing companies which developed the devices for the three local NSPs. There are other NSPs within the Asia Pacific and Australasia region which provide the same services.

XRY 6.5 was the only version available at the time the experiment was conducted. According to previous research and MSAB, XRY is capable of conducting both logical and physical analyses on a mobile phone device. During the acquisition phase of this research; only the logical analysis was able to be conducted to extract data on the test phones. Physical analysis was not able to be conducted by

XRY due to the device profiles that were used. As discussed earlier if such an analysis method was available, there might be the opportunity to extract other missing or deleted data from the test phone devices. In this case XRY 6.5 can only support the test phone devices using the logical analysis method.

6.3 Future Research

Some of the four devices' test data were able to be extracted by XRY 6.5 but not all including deleted data. Some of the devices were not officially supported by XRY. Therefore further research to improve the capability of forensic tools to support unsupported local devices is needed.

Physical analyses of mobile phone devices can be another possible research focus either using XRY or another available forensic tool. In this study only the logical analysis method was used to extract data from each test phone device. Therefore using XRY's physical analysis allow for other data missing from the findings including deleted data, to be identified and extracted.

Local CDMA network devices are another possible aspect for future work using XRY or another forensic tool. Based on previous research; both GSM and CDMA are supported by XRY. As discussed before, the test phones that were used were manufactured specifically for each NSP and operated within their GSM network.

Local NSP mobile phone devices are manufactured by other companies. This can be another interesting area of research in terms of whether the devices these companies manufacture are specifically made for these NSPs, and how they are named and registered. Based on what has been discovered in this research, Phone 1 has two different names yet was manufactured by the same company. Other models are manufactured by the same company but use different names/model numbers particularly those models manufactured on behalf of other entities (local NSPs). As example the Alcatel V860 model is also known as Vodafone Smart II (Smith, 2012).

As discussed in Section 3.4, the GCSB rereleased a security policy report (NZISM) for government departments and agencies, which contains security measures for mobile phones including the protection of sensitive information on these devices. The researcher believes that the research test phones have not been equipped in accordance with this report's specifications. Hence, this might another potential field of research to test the capability of forensic tools to support these

devices used for such security measures and to identify whether all mobile phone devices imported by local NSPs meet the security criteria. It can be an issue in terms of what forensic tools can and cannot do especially when government and other intelligence agencies' security measures are involved.

From a legal perspective, this research only tested four devices from the total number of other local mobile phones. Thus, there are still some devices that potentially have the same problems as Phones 2 and 4 in terms of not being supported by forensic tools such as XRY. Another possible research area is how to present evidence in a court of law if XRY or any other forensic tool cannot extract data (evidence) from a mobile phone device. What other methods or ways can be used by local prosecutors to present phone device evidence (if it can be physically viewed on the device) in court? Mobile phone technology may surpass forensic tool development and there might be no other tool able to extract these data, even though a mobile phone device is capable of storing so much information over time. The integrity and reliability of any current or new forensic tool are foremost priorities.

6.4 Conclusion

This research was focused on the capability of forensic tools such as XRY 6.5 to support local mobile phone devices that are operated and sold within New Zealand. The findings from the forensic experiment were analysed and discussed to appraise the ability of XRY to support these local mobile phone devices. Chapter 6 has concluded this research by re-evaluating the findings including the research question and sub-questions with the hypotheses. The research question has been answered and clearly states that XRY is capable of extracting data from the test phone devices. However, the experiment's results also find there are incomplete performances and variations with the extracted test data, and that most deleted data were not able to be extracted.

Thus, there is still more work needed to improve the capability of forensic tools such as XRY. Future work arising from this research needs to identify the areas that will improve the capability of forensic tools, especially mobile phone forensic tools for the benefit of the consumer, the manufacturer, and the Digital Forensic community. Reliable forensic tools and techniques are necessary for the integrity of any mobile phone forensic investigation.

References

- 2degrees. (2013, January 10). *Phones*. Retrieved from
2degrees:https://www.2degreesmobile.co.nz/shop?p_p_id=konakart_portlet_WAR_konakart_portlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column1&p_p_col_count=1&_konakart_portlet_WAR_konakart_portlet__spage=%2FSelectCat.do%3FcatId%3D21&_konakart_port
- ACPO. (n.d.). *Good Practice Guide for Computer-Based Electronic Evidence*. London: 7safe.
- Ahmed, R., & Dharaskar, R. V. (2008). *Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective*. Hingna Road, Nagpur: India: G. H. Rasoni Institute of Engineering & Technology.
- Akkaladevi, S., Keesara, H., & Luo, X. (2008). *Efficient Forensic Tools For Handheld Devices: A Comprehensive Perspective*. Petersburg, Virginia: USA: Virginia State University, Department of Computer Information Systems.
- Al-Zarouni, M. (2007). *Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics*. Joondalup WA: Australia: School of Computer and Information Science.
- Ayers, R., Jansen, W., Moenner, L., & Delaitre, A. (2007). *Cell Phone Forensic Tools: An Overview and Analysis Update*. Gaithersburg, USA: National Institute of Standards and Technology.
- BBC (2011, August 9). *Rioters' mobile phones could help police investigation*. Retrieved from BBC News: <http://www.bbc.co.uk/news/technology-14465546>
- BreakingNews IE. (2012, May 01). *IRA membership trial hears mobile phone evidence*. Retrieved from BreakingNews.ie:
<http://www.breakingnews.ie/ireland/ira-membership-trial-hears-mobile-phone-evidence-549779.html>
- Britz, M. T. (2008). *Computer Forensic and Cyber Crime*. New Jersey: Pearson Education Inc.
- Brothers, S. (2009). *How Cell Phone "Forensic" Tools Actually Work - Proposed Leveling System*. Chicago, Illinois: Mobile Forensics World.

- Casey, E., & Turnbull, B. (2011). Digital Evidence on Mobile Devices. In E. Casey, *Digital Evidence and Computer Crime* (3 ed., pp. 1-44). United States of America: Elsevier Inc.
- Collis, H. (2012, April 22). *Teenage robbers who raided garage caught after saving pictures of their loot on a mobile phone*. Retrieved from MailOnline: <http://www.dailymail.co.uk/news/article-2133494/Teenage-robbers-raided-garage-caught-saving-pictures-loot-mobile-phone.htm>
- Commerce Commision. (2011). *Annual Telecommunications Monitoring Report 2010*. Wellington: Commerce Commission.
- Consumer. (2012, December 03). *Telecom XT compatibility*. Retrieved from www.consumer.org.nz: http://www.consumer.org.nz/reports/mobile-phones/telecom-xt-compatibility
- GCSB. (2011). *New Zealand Information Security Manual*. Wellington: Government Communications Security Bureau.
- Gonzalez, J., Hung, J., & Friedberg, S. (2011). *Mobile Device Forensics: A Brave New World?* United States of America: Bloomberg Finance L.P.
- GSMARENA. (2013, January 06). *Vodafone 155*. Retrieved from Gsmarena: http://www.gsmarena.com/vodafone_155-4969.php
- Hall, R. (2011, July 29). *How a mobile phone broke killers' wall of silence*. Retrieved from The Independent: <http://www.independent.co.uk/news/world/americas/how-a-mobile-phone-broke-killers-wall-of-silence-2328000.html>
- Hildebrandt, M., Kiltz, S., & Dittmann, J. (2011). A Common Scheme for Evaluation of Forensic Software. *Sixth International Conference on IT Security Incident Management and IT Forensics* , 93-106.
- Jansen, W., & Ayers, R. (2007). *Guidelines on Cell Phone Forensics*. Gaithersburg: USA: National Institute of Standards and Technology.
- Kavanagh, B. (2013, January 23). *Rattigan trial hears evidence from mobile phone forensics expert*. Retrieved from Independent.ie: <http://www.independent.ie/irish-news/courts/rattigan-trial-hears-evidence-from-mobile-phone-forensics-expert-29021862.html>
- Keall, C. (2011, March 22). *2degrees big reveal: 580,112 customers*. Retrieved 08 3, 2011, from The National Business Review: <http://www.nbr.co.nz/opinion/what-2degrees-should-announce-tomorrow>

- Kim, K., Hong, D., Chung, K., & Ryou, J.-C. (2007). *Data Acquisition from Cell Phone using Logical Approach*. Korea: World Academy of Science, Engineering and Technology.
- Lazarte, M. (2012, November 15). *Guilty or not? New ISO/IEC standard for credible digital evidence*. Retrieved from International Organization for Standardization:
http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1677
- Le, Y. A. (2012). *Windows Phone 7: Implications for Digital Forensic Investigators*. Auckland, New Zealand: Auckland University of Technology
- Logan, N. (2011). Digital forensic tools. *Computer Security, Criminology and Law Enforcement*, 42.
- Lunden, I. (2011, September 30). *Symbian Now Officially No Longer Under the Wing of Nokia 2300 Jobs Go*. Retrieved from Paid Content:
<http://paidcontent.org/2011/09/30/419-symbian-now-officially-no-longer-under-the-wing-of-nokia-2300-jobs-go/>
- McCarthy, P. (2005). *Forensic Analysis of Mobile Phones*. Adelaide: School of Computer and Information Science, University of South Australia.
- Mokhonoana, P. M., & Olivier, M. S. (2007). *Acquisition of a Symbian Smart phone's Content with an On-Phone Forensic Tool*. Pretoria: Department of Computer Science, University of Pretoria.
- MSAB. (n.d.). *Law Enforcement*. Retrieved from Micro Systemation:
<http://www.msab.com/market-areas/law-enforcement>
- MSAB. (n.d). *Military*. Retrieved from Micro Systemation:
<http://www.msab.com/market-areas/military>
- MSAB. (2011, May 09). *Mobile Phone Support*. Retrieved from MSAB:
<http://www.msab.com/posts/blog/mobile-phone-support>
- MSAB. (2011, June 08). *XRY Wins Award*. Retrieved 08 1, 2011, from Micro Systemation: <http://www.msab.com/posts/news/xry-wins-award>
- MSAB. (2011, October 7). *What is XRY v6.mp4* [Video File]. Retrieved from <http://www.msab.com/xry/what-is-xry>
- MSAB. (2012, July 29). *XRY has two TV appearances*. Retrieved from Micro Systemation: <http://www.msab.com/posts/news/xry-has-two-tv-appearances>

- MSAB. (2013, May 05). *XRY Physical*. Retrieved from MSAB:
http://www.msab.com/app-data/downloads/Product_Sheets/XRY_Physical.pdf
- Murphy, C. (2010, July). *Celluar Phone Evidence Data Extraction And Documentation*. Retrieved Oct 2011, from Digital Forensics Magazine:
http://www.digitalforensicsmagazine.com/index.php?option=com_jdownloads&Itemid=0&task=view.download&cid=9
- New Zealand Police. (2010). *Electronic Crime Strategy To 2010*. Wellington: New Zealand Police
- NIJ. (2010). *Test Results for Mobile Device Acquisition Tool: XRY 5.0.2*. Washington: National Institute of Justice
- Owen, P., Thomas, P., & McPhee, D. (2010). An Analysis of the Digital Forensic Examination of Mobile Phones. *Fourth International*
- Punja, S. G., & Mislán, R. P. (2008, June). Mobile Device Analysis. *Small Scale Digital Device Forensics*, 2(1), 1-16.
- Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 1-12.
- Schottle, P. (2009). *Digital Forensics in Computer and Cellular Networks*. North Rhine-Westphalia: Germany: Ruhr University Bochum.
- Smith, M. (2012, May 31). *Vodafone UK launches Smart II: Android Gingerbread for £70 (hands-on)*. Retrieved from Hard Reset:
<http://www.engadget.com/2012/05/31/vodafone-smart-2-hands-on/>
- Storer, T., Glisson, W. B., & Grispos, G. (2010). Investigating Information recovered from Re-sold Mobile. *Privacy and Usability Methods Pow-wow (PUMP) Workshop* (pp. 1-2). Dundee: ACM: University of Abertay.
- Telecom NZ. (2013, January 07). *Mobile Phones - Our Picks*. Retrieved from Telecom NZ: <http://store.telecom.co.nz/mobile/personal/phones>
- The New Zealand Hearld. (2012, April 24). *More mobile phones in NZ than people: study*. Retrieved from The New Zealand Hearld:
http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10801183
- The Queen vs Shawn Dean Roberts, 235 (Court of Appeal of New Zealand 10 December, 2000).

- TVNZ. (2013, May 17). *Tourist jailed for child sexual abuse cartoons*. Retrieved from TVNZ: <http://tvnz.co.nz/national-news/tourist-jailed-child-sexual-abuse-cartoons-5440185>
- Vodafone NZ. (2013, January 05). *Mobile Phones*. Retrieved from Vodafone NZ: <http://www.vodafone.co.nz/shop/mobileListing.jsp?selectionKey=mobile&reset=true&categoryId=cat80064>
- Walls, R. J., Learned-Miller, E., & Levine, B. N. (2011). *Forensic Triage for Mobile Phones with DECODE*. Amherst: Department of Computer Science, University of Massachusetts.
- Zareen, A., & Baig, S. (2010). Mobile Phone Forensics Challenges, Analysis and Classification. *Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering*, 47-55.

Appendices

Appendix 1: PC Specifications

Manufacture	Gigabyte
Model	M61PME-S2P
Operating System	Windows 7 Servive Pack 1
Processor	AMD Phenom(tm) 9650 Quad-Core Processor 2.3GHz
RAM	4.0GB
System Type	32-Bit OS
Computer Name	mfit-PC
Product ID	00371-840-1995551-85861
Description	MFIT Lab Standalone PC
Serial Number	Unknown

Appendix 2: Test Phones Specification

This information adapted from the supplier's website, the device (behind the battery) and device's user manual.

	PHONE 1	PHONE 2	PHONE 3	PHONE 4
Name	Vodafone 858 Smart	Telecom R1	Samsung E3210	2degrees Smart Touch
Number	02108425854	0279516107	0279516108	0220744606
IMEI:	357147040188755	8617210101782209	358098043787383	867104010332924
Serial Number	K5F7ND1160703845	-	RF1C977VJED	CCGQKKC10170914
PUK	-	59425408	13695045	53768370

FCC ID	QISU8160-U	-	A3LGTE321OB	-
Model	U8160-U	R1	GT-E3210B	C8660NZ
Made in	China	China	Vietnam	China
Manufactured	Huawei	ZTE	Samsung	Huawei
SIM	VFNZ 128K	TNZ	TNZ	2D 128K
SIM Number	6401 1210 1187 1854	64050021782636207	64050021782636199	896424000102717485
GSM (2G)	850 / 900 / 1800 / 1900	900/1800 /1900	850 / 900 / 1800 / 1900	850/900/ 1800/1900
UMTS (3G)	NA	850/2100	NA	900/2100
HSDPA	2100	-	900 / 2100	-
OS	Android 2.2.1	Native	Native	Android 2.3.6
Memory Card	up to 32GB	NA	NA	up to 32GB
Internal Memory	130MB	130MB	36MB	100MB
GPRS	Yes	-	Yes	Yes
EDGE	Yes	-	Yes	Yes
Speed	3.6 Mbps	3.6 Mbps	3.6 Mbps	-
WLAN	Yes	Nil	Nil	Yes
Bluetooth	v2.1	v2.0	v2.1	Yes
USB	USB v2.0	USB v2.0	USB v2.0	USB v2.0
Camera	2 megapixel	0.3 megapixel	0.3 megapixel	2 megapixel
Video Recording	Yes	Yes	Yes	Yes
Messaging	SMS, MMS, Email, Push Mail, IM	MMS, SMS, Email	SMS, MMS, Email, IM	SMS, MMS, Email
Browser	HTML	WAP only	WAP 2.0/xHTML, HTML	Yes
GPS	Yes	-	No	Yes
Battery	Li-Ion battery	Li-Ion 900 mAh	Li-Ion 800 mAh battery	Li-Ion battery
Media player	Yes	Yes	Yes	Yes
Calendar	Yes	Yes	Yes	Yes

Full electronic copy of Appendix 3A-D can be downloaded by clicking this link: [Download](#)

Appendix 3A: Phone 1 XRY Data Extraction

Summary

Subject	Data
Date Created	02-06-2013 7:08:37 AM
XRY Version	6.5
Lowest Module Version	6.4
Manual Device Selection	Yes
Extraction Media	Cable
Locked	No
Is File Subset	No
Is Encrypted	No
Case Operator	Toma Vasa
Case Reference	MFIT Thesis
Exhibit Id	Phone 1
Notes	Logical extraction of Phone 1

Device General Information

Attribute	Data
Device Name	Manual Selection
Used Device Profile	Vodafone 858 Smart
Mobile Id (IMEI)	357147040188755
Subscriber Id (IMSI)	530016607871854
SIM Status	READY

Network Code (from IMSI)	53001
Service Provider Name	vodafone NZ
Manufacturer	Huawei /HUAWEI
Model	Vodafone 858
Revision	2.2.1 Vodafone858C02B617
Language Preference	en
Device Timezone	Pacific/Auckland
Device Clock	01-06-2013 6:53:37 AM UTC
PC Clock	02-06-2013 7:09:26 AM UTC+12:00, New Zealand Standard Time
Bluetooth Address	04:C0:6F:4E:71:50
Device Status	Bootmode = boot
Baseband Version	unknown

Device Network Information

SSID		Password	Deleted
TNCAP99529F		A524E83ABF	No

Device Event Log

Event Type	Time
Device Bootup	04-05-2012 8:49:26 AM UTC

Device Accounts

Application	Password	Email Address	Storage
Android Email	briancusack	mfit.aut@gmail.com	Device

Contacts

Name	Storage	Index	Mobile	Account Name
Voicemail	Device	1	+6421700700	SIM
Customer Service	Device	2	777	SIM
Directory 018	Device	3	018	SIM
Wicked Welcomes	Device	5	703	SIM
Phone3	Device	6	0279516108	Phone
Phone2	Device	7	0279516107	Phone
TV	Device	8	0212087313	Phone
TV1	Device	9	0210222729	SIM
Phone4	Device	11	0220744606	Phone

Calls

Type	Name	Time	Duration	To (Matched)	Storage	To	From (Matched)	From
Dialed	Customer Service	30-05-2013 1:38:44 AM UTC (Device)	00:02:47	Customer Service	Device	777		
Dialed	Voicemail	30-05-2013 2:57:51 AM UTC (Device)	00:00:00	Voicemail	Device	+6421700700		
Missed	Phone3	30-05-2013 3:39:34 AM UTC (Device)			Device		Phone3	0279516108
Missed	Phone2	30-05-2013 3:40:59 AM UTC (Device)			Device		Phone2	0279516107
Dialed	TV	30-05-2013 3:42:34 AM UTC (Device)	00:00:00	TV	Device	0212087313		
Dialed	Phone2	30-05-2013 3:43:06 AM UTC (Device)	00:00:00	Phone2	Device	0279516107		
Dialed	Phone3	30-05-2013 3:44:02 AM UTC (Device)	00:00:00	Phone3	Device	0279516108		
Dialed	Phone4	30-05-2013 2:47:25 PM UTC (Device)	00:00:00	Phone4	Device	0220744606		
Missed	Phone4	30-05-2013 2:53:12 PM UTC (Device)			Device		Phone4	0220744606
Missed	TV	30-05-2013 4:13:17 PM UTC (Device)			Device		TV	0212087313

Dialed	Phone4	30-05-2013 4:17:27 PM UTC (Device)	00:00:00	Phone4	Device	0220744606		
Received	TV	30-05-2013 4:23:37 PM UTC (Device)	00:00:06		Device		TV	0212087313
Received	Phone4	30-05-2013 4:25:15 PM UTC (Device)	00:00:06		Device		Phone4	0220744606
Dialed	Phone2	31-05-2013 1:15:37 AM UTC (Device)	00:00:04	Phone2	Device	0279516107		
Dialed	Phone3	31-05-2013 1:18:13 AM UTC (Device)	00:00:04	Phone3	Device	0279516108		
Dialed	Phone3	31-05-2013 1:18:34 AM UTC (Device)	00:00:03	Phone3	Device	0279516108		
Dialed	Phone4	31-05-2013 1:21:25 AM UTC (Device)	00:00:04	Phone4	Device	0220744606		
Dialed	Phone4	31-05-2013 1:22:25 AM UTC (Device)	00:00:03	Phone4	Device	0220744606		



Calendar

Subject	Location	Start	End	Timezone	Organizer		Storage
Birthday	Home	04-08-2013 2:00:00 AM UTC	04-08-2013 3:00:00 AM UTC	Pacific/Auckland	Phone		Device

SMS Messages

From	To	Message	Time	Status	Storage	Folder	Service Center	Thread ID	From (Matched)	To (Matched)
Vodafone		Great! We've added your Freebee Bonus to your account. Check your new Freebee Bonus balance at m.vodafone.co.nz/myaccount or TXT FREEBEE to 756 (free in NZ)	30-05-2013 1:39:34 AM UTC	Read	Device	Inbox	+6421601170	1		
Vodafone		Welcome to Prepay FreebeeDATA! Check your Freebee Bonus balance at m.vodafone.co.nz/myaccount on your mobile or TXT FREEBEE to 756 (free in NZ)	30-05-2013 1:39:37 AM UTC	Read	Device	Inbox	+6421601170	1		
+64212087313		Test txt1	31-05-2013 1:25:23 AM UTC	Read	Device	Inbox	+6421601170	2	TV	
+64212087313		Test txt2	31-05-2013 1:26:40 AM UTC	Read	Device	Inbox	+6421601170	2	TV	
	0212087313	Thank u	31-05-2013 1:35:46 AM UTC (Device)	Sent	Device	Sentbox		2		TV

MMS Messages

Subject	MMS	Time	Priority	Folder	Status	Storage	To	To	To	From
	<Binary data not included in export>	31-05-2013 1:47:07 AM UTC	Normal	Sentbox	Sent	Device	0279516107	0279516108	0220744606	
File Name	IMG_20120603_040345.jpg									
Size	9.85 KB									
Path	/data/data/com.android.providers. telephony/app_parts/ PART_1369964439062									
MMS										
File Name	smil.xml									
Size	367 Bytes									
Pics2		31-05-2013 1:55:12 PM UTC	Normal	Inbox	Read	Device				0279516107
MMS										
File Name	applicationsmil_1.smil									
Size	451 Bytes									
File Name	imagejpeg_2.jpg									
Size	4.95 KB									
Path	/data/data/com. android.providers. telephony/app_parts /PART_1369965320230									

Email Messages

From Address	To Address	Subject	Body	Status	Received	Storage	Folder	Application
mail-noreply@google.com Gmail Team	mfit.aut@gmail.com AUT MFIT	Get started with Gmail		Read	31-05-2013 3:27:02 PM UTC	Device	INBOX	Android Email
mail-noreply@google.com Gmail Team	mfit.aut@gmail.com AUT MFIT	Get Gmail on your mobile phone		Read	31-05-2013 3:27:02 PM UTC	Device	INBOX	Android Email
mail-noreply@google.com Gmail Team	mfit.aut@gmail.com AUT MFIT	Customize Gmail with colors and themes		Read	31-05-2013 3:27:02 PM UTC	Device	INBOX	Android Email
noreply-daa26fef@plus.google.com Google+ team	mfit.aut@gmail.com	Getting started on Google+		Read	31-05-2013 3:28:21 PM UTC	Device	INBOX	Android Email
toma.shavas@gmail.com Toma Vasa	mfit.aut@gmail.com Phone4	Re: Test		Read	31-05-2013 3:35:13 PM UTC	Device	INBOX	Android Email
mfit.aut@gmail.com Phone1	wmh2513@aut.ac.nz	Test	Hello	Read	31-05-2013 3:47:29 AM UTC	Device	Sent	Android Email
toma.shavas@gmail.com Toma Vasa	mfit.aut@gmail.com Phone1	Re: Test		Read	31-05-2013 3:49:00 PM UTC	Device	INBOX	Android Email
toma.shavas@gmail.com Toma Vasa	mfit.aut@gmail.com AUT MFIT	Test		Read	01-06-2013 4:51:36 AM UTC	Device	INBOX	Android Email

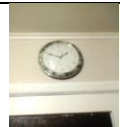

Location and Bookmarks

Application	Storage	Type	Data
Google Maps	Device	Entered	44 matapan road, panmure, auckland
Google Maps	Device	Entered	55 wellesley st east, auckland

Web Searches

Text	Time	Storage
auto	31-05-2013 4:04:48 AM UTC (Device)	Device
aut	31-05-2013 4:05:27 AM UTC (Device)	Device

Pictures

Picture	Name	Type	Size	Path	Storage	Created
	PART_1369965320230	Jpeg	4.95 KB	/data/data/com.android.providers .telephony/app_parts/PART_1369965320230	Device	31-05-2013 1:55:20 AM UTC
	PART_1369964439062	Jpeg	9.85 KB	/data/data/com.android.providers .telephony/app_parts/PART_1369964439062	Device	31-05-2013 1:40:39 AM UTC

*Other pictures that were extracted include default pictures and web view pictures which were all stored on the device and removable media (memory card).

Audio

Name	Type	Size	Path	Storage	Created	Modified	Application	MIME Type
recording20649.amr	Amr	33.01 KB	/mnt/sdcard/Recordings /recording20649.amr	Removable Media	31-05-2013 2:30:52 AM UTC	31-05-2013 2:30:53 AM UTC (Device)	Media Content Provider	audio/amr

*Other audio that were extracted includes default audio i.e ringtones which were all stored on the device and removable media (memory card).

Videos

Name	Type	Size	Path	Storage	Created	Created	Modified	Application	MIME Type
------	------	------	------	---------	---------	---------	----------	-------------	-----------

VID_20120529_033208.3gp	3gp	248.35 KB	/mnt/sdcard/DCIM/Camera/ VID_20120529_033208.3gp	Removable Media	28-05- 2012 2:32:18 PM UTC	28-05- 2012 3:32:18 PM UTC (Device)	28-05- 2012 3:32:18 PM UTC (Device)	Media Content Provider	video/mp4
VID_20120706_052452.3gp	3gp	27.10 KB	/mnt/sdcard/DCIM/Camera/ VID_20120706_052452.3gp	Removable Media	05-07- 2012 4:25:26 PM UTC	05-07- 2012 5:25:26 PM UTC (Device)	05-07- 2012 5:25:26 PM UTC (Device)	Media Content Provider	video/mp4
VID_20120708_003016.3gp	3gp	55.52 KB	/mnt/sdcard/DCIM/Camera /VID_20120708_003016.3gp	Removable Media	07-07- 2012 11:30:24 AM UTC	07-07- 2012 12:30:24 PM UTC (Device)	07-07- 2012 12:30:24 PM UTC (Device)	Media Content Provider	video/mp4
VID_20120710_022620.3gp	3gp	24.90 KB	/mnt/sdcard/DCIM/Camera/ VID_20120710_022620.3gp	Removable Media	09-07- 2012 1:26:38 PM UTC	09-07- 2012 2:26:38 PM UTC (Device)	09-07- 2012 2:26:38 PM UTC (Device)	Media Content Provider	video/mp4
VID_20100825_134301.3gp	3gp	64.30 KB	/data/HWUserData/Videos/Videocamera/ VID_20100825_134301.3gp	Device	25-08- 2010 1:43:08 PM UTC	25-08- 2010 1:43:08 PM UTC (Device)	25-08- 2010 1:43:08 PM UTC (Device)	Media Content Provider	video/mp4
VID_20110914_071217.3gp	3gp	214.75 KB	/data/HWUserData/Videos/Videocamera/ VID_20110914_071217.3gp	Device	14-09- 2011 7:12:32 AM UTC	14-09- 2011 7:12:32 AM UTC (Device)	14-09- 2011 7:12:32 AM UTC (Device)	Media Content Provider	video/mp4
VID_20110829_041639.3gp	3gp	17.86 KB	/data/HWUserData/Videos/Videocamera/ VID_20110829_041639.3gp	Device	29-08- 2011 4:16:41 AM UTC	29-08- 2011 4:16:41 AM UTC (Device)	29-08- 2011 4:16:41 AM UTC (Device)	Media Content Provider	video/mp4

Files and Database

File Name note_pad.db
Storage Device
Created 31-05-2013 5:31:36 AM UTC
Path /data/data/com.example.android.notepad/databases/note_pad.db
Type SQLite
Data <Binary data not included in export>
File Size 6.00 KB
Hash (SHA1) 53b030d0ce8ffc93d2a30717ce5f9e3973efcbd6
Hash (MD5) 0ae3ae14f55a99378757ac4fc805b6e9

Files/Unrecognized

File <Binary data not included in export>
Name NotePad.odex
Size 49.22 KB
Path /system/app/NotePad.odex
Storage Device
Created 23-04-2011 2:59:54 PM UTC
Hash (MD5) ea85cf17230e133b40bc5f6da3579f72
Hash (SHA1) 5cd8cf33d47db8a489c31172d7c45d6f8c92b224

XRY System Extraction Log using DP1

Index	Module	Status	Time	Message
1	MAIN	Success	7:08:37 AM	Initiating Process at 02-Jun-13 7:08 AM
2	MAIN	Success	7:08:37 AM	XRY Version 6.5
3	MAIN	Success	7:08:37 AM	OS: Windows 7 x86, Service Pack 1

4	MAIN	Success	7:08:37 AM	License key: 2-1388919
5	MAIN	Success	7:08:37 AM	Process options: Logical (Full read)
6	MAIN	Success	7:08:37 AM	Selected views: [All]
7	MAIN	Success	7:08:37 AM	Processing device [Vodafone 858 Smart] connected to Micro Systemation Generic ADB Port (COM5) [COM5]...
575	MAIN	Success	7:13:17 AM	THUMBNAILDECODER (6.5) completed successfully
576	MAIN	Success	7:13:17 AM	Starting process of PATHSIZEDECODER (6.5)
577	PATHSIZEDECODER	Success	7:13:17 AM	Processing image:
578	MAIN	Success	7:13:17 AM	PATHSIZEDECODER (6.5) completed successfully

*No errors during the extraction process.

Appendix 3B: Phone 2 XRY Data Extraction

Summary

Subject	Data
Date Created	02-06-2013 8:36:54 AM
XRY Version	6.5
Lowest Module Version	6.4
Manual Device Selection	Yes
Extraction Errors	Yes
Extraction Media	Cable
Locked	No
Is File Subset	No
Is Encrypted	No
Case Reference	Thesis
Exhibit Id	Phone 2
Case Operator	Toma Vasa
Notes	Logical extraction of Phone 2 using Telecom R7 XT device profile.


Device General Information



Attribute	Data
Device Name	Manual Selection
Used Device Profile	Telecom R7 XT
Manufacturer	ZTE Corporation
Model	R1
Revision	R1 T02 1 [Jun 24 2010 21:00:00]
Mobile Id (IMEI)	861721010178209
Subscriber Id (IMSI)	530052178263620
Network Code (from IMSI)	Telecom New Zealand, New Zealand (53005)

Contacts

Name	Category	Storage	Index	Tel	Mobile	Deleted
Voicemail		SIM	1	+6483083210		
Customer Info		SIM	2	*333		
Customer Service		SIM	3	*123		
Telecom Roaming Helpde		SIM	4	+6433710866		
Phone3		SIM	5	0279516108		
TV		SIM	6	0212087313		
Phone1	Unassigned		1		02108425854	
TV1	Unassigned		2		0210222729	Yes
TV2	Unassigned		3		0210272922	
Phone4	Unassigned		4		0220744606	

Pictures

Picture	Name	Type	Size	Path	Created	Modified
	Pic_0601_002.jpg	Jpeg	4.95 KB	fm/photo/album	01-06-2013 1:44:37 AM (Device)	01-06-2013 1:44:37 AM (Device)

	Pic_0601_003.jpg	Jpeg	8.04 KB	fm/photo/album	01-06-2013 1:44:51 AM (Device)	01-06-2013 1:44:51 AM (Device)
	Pic_0601_004.jpg	Jpeg	5.69 KB	fm/photo/album	01-06-2013 2:36:32 AM (Device)	01-06-2013 2:36:32 AM (Device)

*Other pictures that were extracted include default pictures which were all stored on the device.

Audio

Name	Type	Size	Path	Created	Modified
SUD_0601_001.amr	Amr	31.94 KB	fm/audio/record	01-06-2013 2:24:47 AM (Device)	01-06-2013 2:24:47 AM (Device)
SUD_0601_003.amr	Amr	31.51 KB	fm/audio/record	01-06-2013 2:00:51 PM (Device)	01-06-2013 2:00:51 PM (Device)

*Other audios that were extracted include default audio which were all stored on the device.

Video

Name	Type	Size	Path	Created	Modified
Mov_0601_001.3gp	3gp	128.62 KB	fm/video/record	01-06-2013 2:37:17 AM (Device)	01-06-2013 2:37:17 AM (Device)

Files/Unrecognized

File <Binary data not included in export>
Name calendar20130720800_0.vcs
Size 336 Bytes
Path mod/ztecalendar
Created 01-06-2013 2:53:57 AM (Device)
Modified 01-06-2013 2:53:57 AM (Device)
Hash (MD5) e90183f9885ceb1df522e7bbe9bcf480
Hash (SHA1) 691d71823ea01cfc87933c3ac3afcf3ef4500ea0

File <Binary data not included in export>
Name outbox.ind
Size 160 Bytes
Path mod/mailer/email/1/conf
Created 01-06-2013 3:41:41 AM (Device)
Modified 01-06-2013 3:41:41 AM (Device)
Hash (MD5) 30a01f415bad1260cb259fde9859d14d
Hash (SHA1) 98d0fb24dfa147f15675332206f56da0ba3264fd

File <Binary data not included in export>
Name 13216.eml
Size 227 Bytes
Path mod/mailer/email/1/outbox
Created 01-06-2013 3:41:41 AM (Device)
Modified 01-06-2013 3:41:41 AM (Device)
Hash (MD5) 1a168b6647c4abff8abda31ebeeabc24
Hash (SHA1) bfe3a9ed58c320ab2a1ced84d06bbf0b3e6e2b03

File <Binary data not included in export>
Name spaceconfig.ini
Size 66 Bytes
Path mod/mailer/conf
Created 01-06-2013 3:41:41 AM (Device)
Modified 01-06-2013 3:41:41 AM (Device)

Hash (MD5) 1a96240df8181570fe7e63ee8684a1b1
Hash (SHA1) c51ef426eaf1c1618a151bc206fd15816e7ef30d

File <Binary data not included in export>
Name emaillocal.ini
Size 1.84 KB
Path mod/mailer/email/1/conf
Created 01-06-2013 3:41:41 AM (Device)
Modified 01-06-2013 3:41:41 AM (Device)
Hash (MD5) 00153b12ba4141820e6cf8f96693a743
Hash (SHA1) 75cf57036ab310907218c18e47a25bcff3d08d95

XRY System Extraction Log using DP2

Index	Module	Status	Time	Message
1	MAIN	Success	8:36:54 AM	Initiating Process at 02-Jun-13 8:36 AM
2	MAIN	Success	8:36:54 AM	XRY Version 6.5
3	MAIN	Success	8:36:54 AM	OS: Windows 7 x86, Service Pack 1
4	MAIN	Success	8:36:54 AM	License key: 2-1388919
5	MAIN	Success	8:36:54 AM	Process options: Logical (Full read)
6	MAIN	Success	8:36:54 AM	Selected views: [All]
7	MAIN	Success	8:36:54 AM	Processing device [Telecom R7 XT] connected to ZTE Handset USB Modem [COM6]...
20	MAIN	Failed starting protocol	8:36:59 AM	BREWSYNC (6.4) completed with error
24	BREWFILE	Forbidden	8:37:00 AM	Analyzing '.efs_private', Status: 2684354863
25	BREWFILE	Forbidden	8:37:12 AM	Analyzing '.nvm', Status: 2684354863
30	BREWFILE	Forbidden	8:38:21 AM	Reading 'mod/32789/DK_AicWig.dat', Status: 2684354863
31	BREWFILE	Forbidden	8:38:21 AM	Reading 'mod/32789/DK_EARACg.dat', Status: 2684354863
32	BREWFILE	Forbidden	8:40:11 AM	Reading 'sys/download/lock', Status: 2684354863
33	BREWFILE	Forbidden	8:40:11 AM	Reading 'sys/priv/prefs.dat', Status: 2684354863
46	GSM0707	Unknown device error	8:40:13 AM	Error Failed initializing LD storage.
48	GSM0707	Unknown device error	8:40:13 AM	Error Failed initializing MC storage.
50	GSM0707	Unknown device error	8:40:13 AM	Error Failed initializing RC storage.

52	MAIN	Unknown device error	8:40:13 AM	GSM0707 (6.4) completed with error
56	MAIN	No conversion available	8:40:26 AM	GSM0705 (6.4) completed with error
73	QUALCOMMFILEDECODER	Not found	8:41:33 AM	Files not found...
75	QUALCOMMFILEDECODER	Not found	8:41:33 AM	Files not found...
99	MAIN	Success	8:41:33 AM	THUMBNAILEDDECODER (6.5) completed successfully
100	MAIN	Success	8:41:33 AM	Starting process of PATHSIZEDECODER (6.5)
101	PATHSIZEDECODER	Success	8:41:33 AM	Processing image:
102	MAIN	Success	8:41:33 AM	PATHSIZEDECODER (6.5) completed successfully

*There were errors during the extraction process.

Appendix 3C: Phone 3 XRY Data Extraction

Summary

Subject	Data
Date Created	02-06-2013 9:09:56 AM
XRY Version	6.5
Lowest Module Version	6.1
Manual Device Selection	Yes
Extraction Media	Cable
Locked	No
Is File Subset	No
Is Encrypted	No
Case Reference	MFIT Thesis
Exhibit Id	Phone 3
Case Operator	Toma Vasa
Notes	Logical extraction of Phone 3.

General Device Information

Attribute	Data
Device Name	Manual Selection
Used Device Profile	Samsung GT-E3210
Manufacturer	SAMSUNG
Model	GT-E3210B
Revision	08/02/2009
Mobile Id (IMEI)	358098 04 378738 3
Subscriber Id (IMSI)	530052178263619

Network Code (from IMSI)	Telecom New Zealand, New Zealand (53005)
Device Clock	02-06-2013 8:54:13 AM (Device)
PC Clock	02-06-2013 9:09:56 AM UTC+12:00, New Zealand Standard Time

Contacts

Name	Name	Storage	Index	Tel	Mobile
Voicemail		SIM	1	+6483083210	
Customer Info		SIM	2	*333	
Customer Service		SIM	3	*123	
Telecom Roaming Help		SIM	4	+6433710866	
Phone1		SIM	5	02108425854	
Phone2		SIM	6	0279516107	
Phone4		SIM	7	0220744606	
TV		SIM	8	0212087313	
TV1		SIM	9	0210222729	
Phone1	Phone1	Device			02108425854
Phone2	Phone2	Device			0279516107
Phone4	Phone4	Device			0220744606
TV1	TV1	Device			0210222729
TV	TV	Device			0212087313

Calls

Type	Number	Index	Name (Matched)
Missed	02108425854	1	Phone1
Missed	0279516107	2	Phone2
Missed	0212087313	3	TV
Missed	0220744606	4	Phone4
Dialed	0800323232	1	

Dialed	02108425854	2	Phone1
Dialed	0279516107	3	Phone2
Dialed	0220744606	4	Phone4
Dialed	0212087313	5	TV
Dialed	*333	6	Customer Info
Dialed	*333	7	Customer Info
Received	02108425854	1	Phone1
Received	02108425854	2	Phone1

Calendar

Subject	Categories	Start	End
Birthday	Appointment	04-08-2013 8:00:00 AM UTC (Device)	04-08-2013 8:00:00 AM UTC (Device)
Anniversary	Appointment	25-08-2013 8:00:00 AM UTC (Device)	25-08-2013 8:00:00 AM UTC (Device)

Tasks

Subject	Start	Due	Priority	Status
Go party	01-06-2013 3:00:00 AM UTC (Device)	01-06-2013 12:00:00 AM UTC (Device)	2	Needs Action
Go holiday	28-12-2013 3:00:00 AM UTC (Device)	15-02-2014 12:00:00 AM UTC (Device)	2	Needs Action




SMS Messages

Number	Message	Time	Status	Storage	Index	Service Center
003100380034	FRM Telecom: Your Top Up balance recently dropped below \$1. If you need to Top Up simply call *333 or go to Your Telecom, click FREE http://m.telecom.co.nz/yt ,0,0	01-06-2013 8:21:00 AM UTC+12:00 (Network)	Read	SIM	1	+002B0036003400320037003 7003400330038003300300030
+002B0036003400320031003 2003000380037003300310033	Test txt3,0,0	01-06-2013 1:28:00 AM UTC+12:00 (Network)	Read	SIM	3	+002B0036003400320037003 7003400330038003300300030

+002B0036003400320031003 2003000380037003300310033 0030003200310032003000380 037003300310033	Test txt2,0,0	01-06-2013 1:27:00 AM UTC+12:00 (Network)	Read	Device	1	002B0036003400320037003 7003400330039003000310030
	Thank u,3,0		Sent	Device	2	

*As displayed in red is as an example of incompleteness and inconsistency of the extracted data (Calls). Phone numbers are not correct.

Pictures

Picture	Name	Type	Size	Path	Created	Modified	Accessed
	Photo-0001.jpg	Jpeg	110.55 KB	E:\Images	01-06-2013 1:45:40 AM (Device)	01-06-2013 1:45:40 AM (Device)	01-06-2013 (Device)
	Photo-0002.jpg	Jpeg	90.38 KB	E:\Images	01-06-2013 1:45:46 AM (Device)	01-06-2013 1:45:46 AM (Device)	01-06-2013 (Device)
	Photo-0003.jpg	Jpeg	85.31 KB	E:\Images	01-06-2013 1:45:52 AM (Device)	01-06-2013 1:45:52 AM (Device)	01-06-2013 (Device)

Audio

Name	Type	Size	Path	Created	Modified	Accessed
Voice-0002.amr	Amr	15.94 KB	E:\Sounds	01-06-2013 2:40:18 AM (Device)	01-06-2013 2:40:42 AM (Device)	01-06-2013 (Device)
Touch the light.mp3	Mp3	1.09 MB	E:\Sounds\Music	26-10-2011 3:05:34 PM (Device)	26-10-2011 2:43:28 PM (Device)	01-06-2013 (Device)

Video

Name	Type	Size	Path	Created	Modified	Accessed
Video-0002.3gp	3gp	241.44 KB	E:\Videos	01-06-2013 2:38:28 AM (Device)	01-06-2013 2:38:36 AM (Device)	01-06-2013 (Device)

XRY System Extraction Log using DP3

Index	Module	Status	Time	Message
1	MAIN	Success	9:09:56 AM	Initiating Process at 02-Jun-13 9:09 AM
2	MAIN	Success	9:09:56 AM	XRY Version 6.5
3	MAIN	Success	9:09:56 AM	OS: Windows 7 x86, Service Pack 1
4	MAIN	Success	9:09:56 AM	License key: 2-1388919
5	MAIN	Success	9:09:56 AM	Process options: Logical (Full read)
6	MAIN	Success	9:09:56 AM	Selected views: [All]
7	MAIN	Success	9:09:56 AM	Processing device [Samsung GT-E3210] connected to SAMSUNG Mobile USB Modem [COM9]...
168	MAIN	Success	9:11:32 AM	THUMBNAILEDDECODER (6.5) completed successfully
169	MAIN	Success	9:11:32 AM	Starting process of PATHSIZEDECODER (6.5)
170	PATHSIZEDECODER	Success	9:11:32 AM	Processing image:
171	MAIN	Success	9:11:32 AM	PATHSIZEDECODER (6.5) completed successfully

*No errors during the extraction process.

Appendix 3D: Phone 4 XRY Data Extraction

Summary

Subject	Data
Date Created	02-06-2013 10:23:53 AM
XRY Version	6.5
Lowest Module Version	6.5
Manual Device Selection	Yes
Extraction Media	Cable
Locked	No
Is File Subset	No
Is Encrypted	No
Case Reference	MFIT Thesis
Case Operator	Toma Vasa
Exhibit Id	Phone 4
Notes	Logical extraction of Phone 4 using Huawei U8160 profile device.

Device General Information

Attribute	Data
Device Name	Manual Selection
Used Device Profile	Huawei U8160 (Untested)
Device Status	Bootmode = unknown
Baseband Version	msm
SIM Status	Ready
Subscriber Id (IMSI)	530240102717485
SIM Identification (ICCID)	8964240001027174850

Network Code (from IMSI)	53024
Service Provider Name	2degrees
Mobile Id (IMEI)	867104010332924
Manufacturer	2degrees
Model	C8660
Revision	2.3.6/GRK39F/5775
Device Clock	02-06-2013 10:10:55 AM UTC+12:00, New Zealand Standard Time (Device)
PC Clock	02-06-2013 10:26:21 AM UTC+12:00, New Zealand Standard Time
WiFi Address	88:F4:88:6A:F3:67
Bluetooth Address	88:F4:88:6A:C0:9E

Contacts

Name	Index	Mobile	Home	Account Name	Application
2degrees	1	*100#		SIM	com.android.contacts.sim
Balance	2	*100*1#		SIM	com.android.contacts.sim
Customer Care	3	200		SIM	com.android.contacts.sim
Directory 0133	4	0133		SIM	com.android.contacts.sim
Directory 018	5	018		SIM	com.android.contacts.sim
Top Up	6	201		SIM	com.android.contacts.sim
Voicemail	7	+64222022002		SIM	com.android.contacts.sim
Phone1	8		02108425854	Phone	Local
Phone2	9		0279516107	Phone	Local
Phone3	10		0279516108	Phone	Local
TV	11	0212087313		SIM	com.android.contacts.sim
TV2	13		0210272922	Phone	Local

Calls

Type	Time	Duration	To	To	Storage	From	From
Dialed	31-05-2013 2:51:31 AM UTC (Device)	00:00:00	0279516107	Phone2	Device		
Dialed	31-05-2013 2:53:25 AM UTC (Device)	00:00:00	02108425854	Phone1	Device		
Dialed	31-05-2013 2:54:13 AM UTC (Device)	00:00:00	0279516108	Phone3	Device		
Dialed	31-05-2013 2:54:33 AM UTC (Device)	00:00:00	0279516108	Phone3	Device		
Missed	31-05-2013 2:58:25 AM UTC (Device)				Device	0212087313	TV
Dialed	31-05-2013 3:09:16 AM UTC (Device)	00:00:00	0210222729		Device		
Dialed	31-05-2013 3:13:26 AM UTC (Device)	00:00:00	0210272922	TV2	Device		
Missed	31-05-2013 3:23:46 AM UTC (Device)				Device	0279516108	Phone3
Dialed	31-05-2013 4:14:41 AM UTC (Device)	00:00:00	0210272922	TV2	Device		
Dialed	31-05-2013 4:15:18 AM UTC (Device)	00:00:00	0279516107	Phone2	Device		
Missed	31-05-2013 4:17:20 AM UTC (Device)				Device	0212087313	TV
Missed	31-05-2013 4:17:57 AM UTC (Device)				Device	02108425854	Phone1
Dialed	31-05-2013 4:18:48 AM UTC (Device)	00:00:00	02108425854	Phone1	Device		
Dialed	31-05-2013 4:19:20 AM UTC (Device)	00:00:00	0279516108	Phone3	Device		
Missed	31-05-2013 4:21:52 AM UTC (Device)				Device	0279516108	Phone3
Dialed	31-05-2013 4:22:12 AM UTC (Device)	00:00:00	0212087313	TV	Device		
Dialed	31-05-2013 4:22:37 AM UTC (Device)	00:00:00	0279516108	Phone3	Device		
Dialed	31-05-2013 4:24:36 AM UTC (Device)	00:00:04	02108425854	Phone1	Device		
Dialed	31-05-2013 4:25:30 AM UTC (Device)	00:00:06	02108425854	Phone1	Device		
Dialed	31-05-2013 1:16:52 PM UTC (Device)	00:00:04	0279516107	Phone2	Device		
Dialed	31-05-2013 1:17:26 PM UTC (Device)	00:00:03	0279516107	Phone2	Device		
Dialed	31-05-2013 1:19:22 PM UTC (Device)	00:00:05	0279516108	Phone3	Device		
Dialed	31-05-2013 1:20:26 PM UTC (Device)	00:00:03	0279516108	Phone3	Device		
Received	31-05-2013 1:22:55 PM UTC (Device)	00:00:03			Device	02108425854	Phone1
Received	31-05-2013 1:23:33 PM UTC (Device)	00:00:02			Device	0279516108	Phone3



Calendar

Subject	Location	Start	End	Timezone	Storage
Due date	School	27-06-2013 2:00:00 PM UTC	27-06-2013 3:00:00 PM UTC	Pacific/Auckland	Device
Competition	Gym	28-08-2013 2:00:00 PM UTC	28-08-2013 3:00:00 PM UTC	Pacific/Auckland	Device

SMS Messages

From	To	Message	Time	Status	Storage	Index	Folder	Service Center
	0212087313	Bye	31-05-2013 2:20:41 PM UTC (Device)	Sent	Device	9	Sentbox	
+64212087313		Test txt3	31-05-2013 1:29:03 PM UTC	Read	Device	7	Inbox	+64221420018
+64212087313		Test txt1	31-05-2013 1:25:58 PM UTC	Read	Device	5	Inbox	+64221420018
233		You topped up \$20 Your bal: \$20.00 \$10Text now includes All You Need Text. To add text 'BUY 10txt' to 233. FairUse Applies	31-05-2013 2:56:23 AM UTC	Read	Device	4	Inbox	+64221420018
233		Thanks for your top up. We've added your free \$10Text. This pack auto renews monthly. To cancel it text STOP 10TXT to 233 in the next month. TCs apply	31-05-2013 2:56:17 AM UTC	Read	Device	3	Inbox	+64221420018
2degrees		Welcome to 2degrees Prepay Plus. Thks for joining. Your num is 0220744606. See 2dm.co.nz to top up and for rates and terms. Questions? Call us free 24/7 on 200 \$10Text now includes All You Need Text. To add text 'BUY 10txt' to 233. FairUse Applies	31-05-2013 2:24:31 AM UTC	Read	Device	2	Inbox	+64221420018
2degrees		Whoops! You need to activate your account before you can get online through 2degrees. Please call 200 from your 2degrees mobile now.	31-05-2013 2:19:54 AM UTC	Read	Device	1	Inbox	+64220227672

MMS Messages

From	To	Subject	Time	Priority	Folder	Status	Entry ID
	0279516108		31-05-2013 2:02:32 PM UTC (Device)	Normal	Sentbox	Read	5
MMS							
File Name	smil						
Hash (MD5)	2c95cf7d02be0a3ccc1f9fde03497b60						
Hash (SHA1)	9814a97a79423a15711d81c02d4db7e8647bfac9						
File Name	IMG_20130601_020110_0						
Hash (MD5)	b908c4dba8b962e941d0d1fc071eeb00						
Hash (SHA1)	a8b3fb156aa74f0347b1d399d2ce1b3e0f2e0d7f						
MMS	Pics						
File Name	text_0						
Hash (MD5)	6501cd97649d2f55daaccfc3bc3dddb						
Hash (SHA1)	537ce2df1f2e36fb34cbd03b5690056676ddad11						
+64279516107	+64220744606	Pics	31-05-2013 1:54:01 PM UTC	Normal	Inbox	Read	4
MMS							

File Name	applicationsmil_1.smil						
Hash (MD5)	d403cd9082bf3a5d60e0b9ecea8e9293						
Hash (SHA1)	8f541a4055f57fb447e2a2b7d21396fb8c5b4f36						
File Name	imagejpeg_2.jpg						
Hash (MD5)	76465bfcfa262f82e2cfed6031bb1551						
Hash (SHA1)	bccaf78c2cace2b328100735ca58b54c934eb3de						
+642108425854	+64220744606		31-05-2013 1:48:01 PM UTC	Normal	Inbox	Read	2
MMS							
File Name	smil.xml						
Hash (MD5)	82abe439d689e760221a8c4a1d0ec3ea						
Hash (SHA1)	48b67e533b2cfb4cb233c1b13d1818bb4065fa33						
File Name	IMG_20120603_040345.jpg						
Hash (MD5)	08fa31933c3c398f9c251a49599a2e35						
Hash (SHA1)	f1b711a5044963728beb365fa3ade8388126e812						
MMS	Pics						
File Name	text_0.txt						
Hash (MD5)	6501cd97649d2f55daaccfc3bc3dddb						
Hash (SHA1)	537ce2df1f2e36fb34cbd03b5690056676ddad11						


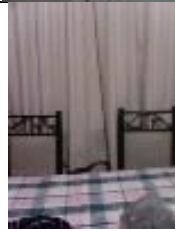
Web History

Web Address	Access Count	Display Name	Time
http://www.aut.ac.nz/	1	http://www.aut.ac.nz/	31-05-2013 4:02:03 PM UTC (Device)
http://www.msab.com/index?gclid=CPCbuKPcwLcCFc4hpQodOy4Auw	1	http://www.msab.com/index?gclid=CPCbuKPcwLcCFc4hpQodOy4Auw	31-05-2013 4:04:19 PM UTC (Device)

Web Search

Text	Time
www	31-05-2013 4:23:45 PM UTC (Device)

Pictures

Picture	Name	Type	Size	Path	Storage	Created
	IMG_20130601_020045_0.jpg	Jpeg	238.82 KB	/mnt/sdcard/DCIM/Camera/IMG_20130601_020045_0.jpg	Removable Media	31-05-2013 3:00:44 PM UTC
	IMG_20130601_020110_0.jpg	Jpeg	272.68 KB	/mnt/sdcard/DCIM/Camera/IMG_20130601_020110_0.jpg	Removable Media	31-05-2013 3:01:10 PM UTC

*Other pictures that were extracted include default pictures, MMS and webview which were all stored on the device and removable media.

Audio

Name	Type	Size	Path	Storage	Created
2013-06-01-05-351754120863.amr	Amr	37.85 KB	/mnt/sdcard/voice/2013-06-01-05-351754120863.amr	Removable Media	01-06-2013 6:35:34 AM UTC
2013-06-01-05-363775523.amr	Amr	35.66 KB	/mnt/sdcard/voice/2013-06-01-05-363775523.amr	Removable Media	01-06-2013 6:36:42 AM UTC

*Other audios that were extracted include default audios i.e. ringtones which were all stored on the device and removable media.

Files/Unrecognized

File <Binary“data“not“included“in“export>

Name OINotePad.odex

Size 113.02“KB

Path /system/app/OINotePad.odex

Storage Device

Created 01-08-2008“12:00:00“PM“UTC

Hash“(MD5) 2a5aa37c923cc15edc78eb95661f47ed

Hash“(SHA1) 2594b09ac789cdd856982bffb6cd5dc7e7df6c62

XRY System Extraction Log using DP1U

Index	Module	Status	Time	Message
1	MAIN	Success	10:23:53 AM	Initiating Process at 02-Jun-13 10:23 AM
2	MAIN	Success	10:23:53 AM	XRY Version 6.5
3	MAIN	Success	10:23:53 AM	OS: Windows 7 x86, Service Pack 1
4	MAIN	Success	10:23:53 AM	License key: 2-1388919
5	MAIN	Success	10:23:53 AM	Process options: Logical (Full read)
6	MAIN	Success	10:23:53 AM	Selected views: [All]

7	MAIN	Success	10:23:53 AM	Processing device [Huawei U8160 (Untested)] connected to Micro Systemation Generic ADB Port (COM10) [COM10]...
170	ANDROID	Forbidden	10:26:14 AM	Failed to extract file /system/etc/bluetooth/auto_pairing.conf
171	ANDROID	Forbidden	10:26:14 AM	Failed to extract file /system/etc/bluetooth/audio.conf
172	ANDROID	Forbidden	10:26:14 AM	Failed to extract file /system/etc/bluetooth/main.conf
173	ANDROID	Forbidden	10:26:14 AM	Failed to extract file /system/etc/bluetooth/input.conf
183	ANDROID	Forbidden	10:26:16 AM	Failed to extract file /system/etc/dbus.conf
184	ANDROID	Success	10:26:16 AM	/sbin
185	ANDROID	Forbidden	10:26:16 AM	/init.target.rc
186	ANDROID	Forbidden	10:26:16 AM	/init.rc
187	ANDROID	Forbidden	10:26:16 AM	/init.qcom.sh
188	ANDROID	Forbidden	10:26:16 AM	/init.qcom.rc
189	ANDROID	Forbidden	10:26:16 AM	/init.goldfish.rc
190	ANDROID	Forbidden	10:26:16 AM	/init
191	ANDROID	Success	10:26:16 AM	/data
274	MAIN	Success	10:27:11 AM	THUMBNAILED (6.5) completed successfully
275	MAIN	Success	10:27:11 AM	Starting process of PATHSIZEDECODER (6.5)
276	PATHSIZEDECODER	Success	10:27:11 AM	Processing image:
277	MAIN	Success	10:27:12 AM	PATHSIZEDECODER (6.5) completed successfully

*There were errors during the extraction process.

XRY System Extraction Log using DP4

Index	Module	Status	Time	Message
1	MAIN	Success	9:34:47 AM	Initiating Process at 02-Jun-13 9:34 AM
2	MAIN	Success	9:34:47 AM	XRY Version 6.5
3	MAIN	Success	9:34:47 AM	OS: Windows 7 x86, Service Pack 1
4	MAIN	Success	9:34:47 AM	License key: 2-1388919
5	MAIN	Success	9:34:47 AM	Process options: Logical (Full read)
6	MAIN	Success	9:34:47 AM	Selected views: [All]

7	MAIN	Success	9:34:47 AM	Processing device [Huawei C8600] connected to Micro Systemation Generic ADB Port (COM10) [COM10]...
8	MAIN	Success	9:34:47 AM	Hardware id: USB\VID_0a1c&PID_7000&Rev_0229&MI_00
9	MAIN	Success	9:34:47 AM	Using manual selection device model override
10	MAIN	Success	9:34:47 AM	Media Resp = [Cable]
11	MAIN	Success	9:34:47 AM	Starting process of ANDROID (6.5)
12	ANDROID	Success	9:34:47 AM	Connecting
13	MAIN	Failed opening port	9:34:47 AM	ANDROID (6.5) completed with error
14	MAIN	Success	9:34:47 AM	2 items read to Device / General Information folder

*There was an error during the extraction process. Extraction of Phone 4 cannot be completed with DP4

Appendix 4: XRY Device Extraction Information Summary

	Phone 1		Phone 2	Phone 3	Phone 4
Device Profile	DP1	DP1U	DP2	DP3	DP1U
IMEI	357147040188755	357147040188755	861721010178209	358098 04 378738 3	867104010332924
IMSI	530016607871854	530016607871854	530052178263620	530052178263619	530240102717485
Network Code	53001	53001	53005	53005	53024
NSP	VFNZ	VFNZ	TNZ	TNZ	2degrees
Manufacture	Huawei	Huawei	ZTE Corporation	SAMSUNG	2degrees
Model	Vodafone 858	Vodafone 858	R1	GT-E3210B	C8660
Revision	2.2.1	2.2.1	24/06/2010	08/02/2009	2.3.6
ICCID	-	-	-	-	8964240001027174850