Windows Phone 7 : Implications For Digital Forensic Investigators

YUNG ANH LE
B.E. (Manukau Institute Of Technology, NZ)

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

School of Computing and Mathematical Sciences

Auckland, New Zealand
2012

Declaration

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

.....

Signature

Acknowledgements

This thesis was conducted at the Faculty of Design and Creative Technologies in the school of Computing and Mathematical Sciences at Auckland University of Technology, New Zealand. Support was received from many people throughout the duration of the thesis. Firstly I would like to thank my mother Van and my father Tai both of whom provided support and encouragement during the course of the thesis project as well as throughout my entire post graduate study.

I would like to thank my thesis supervisors Mr. Petteri Kaskenpalo and Dr Brian Cusack for their exceptional support and guidance throughout the thesis project. Mr Kaskenpalo provided me with the freedom to explore research directions and choose the routes that I wanted to investigate. Mr Kaskenpalo's encouragement, excellent guidance, creative suggestions, and critical comments that have greatly contributed to this thesis. Mr Kaskenpalo, I would like to thank you very much for your supervision. I enjoyed our discussions and have learned a great deal from you. I also would like to thank Dr. Brian Cusack, who kindly agreed to being my supervisor at very short notice. Dr. Cusack provided me great guidance and mentoring, without which this thesis would not have been possible.

I would like to thank my good friend Simon Lowther who helped me greatly during the thesis project with his help and support, even to the most unreasonable of requests. I would like to thank my friend and fellow MFIT student Jon Pearse for his aid and insights on both matters for digital forensics, and matters non digital forensics. Finally I would like to thank my former fellow MFIT student and MFIT lab supervisor Thomas Laurenson, who's skill and knowledge about forensics helped me when the thesis was going wrong, and who's conversations on life helped me when the thesis was going right.

Abstract

Windows Phone 7 (WP7) is the latest smart phone Operating System (OS) from Microsoft (MS) replacing the previous MS smart phone OS Windows Mobile (WM) 6.5. WP7 was redesigned completely and was not based on a previous version, unlike WM6 which was based on WM5 and so on. Because WP7 was redesigned and not based on WM, WP7 has many differences compared with WM in terms of underlying hardware and software as well as the user interface and how the phone communicates with a PC. Much research has been done on WM forensics and as a result forensics tools and techniques for WM have been established. Due to the changes implemented in WP7, the established WM forensic tools and techniques may be unable to work with WP7.

Literature on WM forensics and WP7 were reviewed and identified the compatibility of the WM forensic tools and techniques with WP7 was not known, and hence leaving a gap between the WM forensics literature and WP7. The research question of "*What forensic data can be extracted from a WP7 phone using current tools and techniques used to extract forensic data from WM phones?*" and a hypothesis was defined. A methodology was defined in order to conduct the research to answer the research question and test the hypothesis.

The research was conducted in five phases. Phase one uses the literature review and the reviews of similar published studies to establish the current WM forensic tools and techniques, and what data can be extracted from a WM phone using the WM forensic tools and techniques. Phase two used the data extracted from the WM phone as a template to generate test data which was loaded onto a WP7 phone. Phase three applied the established WM forensic tools and techniques to the WP7 phone in order to extract the test data from the phone. Phase four compared the results of the data extracted from the WP7 phone with the data extracted from the WM phone. Phase five evaluated the compatibility of the WM forensic tools and techniques based on the results from Phase four.

The research findings showed that of the WM forensic tools and techniques tested, only one tool was able to successfully acquire any data from the WP7 phone. However the data acquired from the WP7 phone is much less than what could be acquired from a WM phone using the same tool. The remaining WM forensic tools and techniques tested were either unable to acquire data from

the WP7 phone or yielded inconclusive results. Based on the research findings, the majority of the WM forensic tools and techniques are not able to extract any data from WP7, and the WM forensic tool which can extract data from WP7 is able to extract much less data than from WM.

Table of Contents

Chapter One: Introduction

Chapter Two: Literature Review

Chapter Three: Methodology

Chapter Four: Research Findings

Chapter Five: Discussion

Chapter Six: Conclusion

Appendices

List Of Tables

List of Figures

List of Abbreviations

ACPO	Association of Chief Police Officers
ASCII	American Standard Code for Information Interchange
DFT	Dark Forces Team
exFAT	Extended File Allocation Table
FAT	File Allocation Table
GPS	Global Position System
HAL	Hardware Abstraction Layer
IE	Internet Explorer
IM	Instant Messaging
IMAP	Internet Message Access Protocol
JTAG	Joint Test Action Group
MMC	Multi Media Card
MMS	Multimedia Message Service
MS	Microsoft
MSDN	Microsoft Developer Network
NAND	Not AND
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
PCB	Printed Circuit Board
PDA	Personal Digital Assistant
POP	Post Office Protocol
RAM	Random Access Memory
ROM	Read Only Memory
SD	Secure Digital
SMS	Short Message Service
TexFAT	Transaction-safe Extended File Allocation Table
TFAT	Transaction-safe File Allocation Table
TX	TouchXperience
UFED	Universal Forensic Extraction Device
UI	User Interface
USB	Universal Serial Bus
UX	User Experience
WCE	Windows CE
WM	Windows Mobile
WMDC	Windows Mobile Device Center
WMFPM	Windows Mobile Forensic Process Model
WP7	Windows Phone 7
WPDM	Windows Phone Device Manager

Chapter One
Introduction

1.0 INTRODUCTION

Windows Phone 7 (WP7) is the latest mobile Operating System (OS) from Microsoft (MS) replacing the previous MS mobile OS Windows Mobile (WM) 6. WP7 was redesigned completely and introduced many changes compared to WM. While much research been done on WM forensics using established forensic tools and techniques, how well the established WM forensic tools and techniques work on WP7 is not known. How the changes made to WP7 will affect current WM forensic tools and techniques used during a forensic investigation is unknown and difficult to predict. The focus of the research will be on how the WP7 affect current forensic tools and techniques used on WM.

The original MS mobile OS was introduced in 1996 and has been marketed under various brands such as Windows CE, Pocket PC, and WM. The length of time WM (and previous versions) have been available has allowed many forensic tools to be developed to work with WM phones, and many studies has been published on the subject on WM forensics. While WP7 replaced WM6 the same way that WM6 replaced WM5, WP7 can almost be considered a different OS. MS redesigned WP7 completely so WP7 is not based on WM (or previous versions). WP7 will not run on any current WM phones, and will not run any WM programs or applications. The redesign of WP7 introduced many changes to WP7, and some of the changes may mean forensic tools and techniques designed to work with WM will no longer work with WP7.

Some of the changes made to WP7 may cause forensic tools and techniques currently used on WM phones not to work when used on WP7 phones. Which of the changes made to WP7 will affect current forensic tools and techniques and to what extent is unknown. There is not yet any literature on WP7 forensics which creates a problem area with WP7 and digital forensics. Section 1.1 will discuss the problem area in more detail and Section 1.2 will discuss the motivation for the research. Chapter 1 concludes with an outline of how the research is structured will be given in Section 1.3.

1.1 PROBLEM AREA

The redesign of WP7 has meant that WP7 had many changes compared to the previous versions of the MS mobile OS such as WM. Almost every aspect of WP7 has changed compared to WM, and the changes will be discussed in more detail in Section 2.3. At the time of the research no literature on WP7 forensics was found, therefore how well current forensic tools and techniques work on WP7 was unknown, and how the changes to WP7 may impact a digital forensic investigation was also unknown.

During a WM forensic investigation, forensic tools and techniques are used to extract data from the WM phone in a forensically sound manner (discussed in Chapter 2). First data is acquired from the phone, and then the data acquired is analysed to find data of interest to the forensic investigation. Data can be acquired from the WM phone either by connecting the phone to a PC via a USB connection, or by directly accessing the phone's memory. WP7 connects to a PC via a USB connection like WM, however the underlying mechanism which provides communication between the phone and the PC has changed. The change in the how the phone communicates with the PC may cause forensic tools to not work with WP7. Direct access to the WP7 phone's memory is possible, since the memory of a WP7 phone and the memory of a WM phone may be similar, but the way data is stored on the WP7 phone's memory is different to how data is stored on a WM phone's memory. Even though current WM forensic tools and techniques may be able to acquire data from the WP7 phone's memory, the change in how the data is stored on the WP7 phone's memory may mean the acquired data may not be able to be analysed by the WM forensic tools and techniques.

Some WM forensic tools can also extract data from WM phones by loading a program onto the WM phone via the USB connection between the WM phone and the PC. The program then dumps the contents of the phone's memory to the PC. Using the WM forensic tools to load a program onto a WP7 phone may not be possible for two reasons. First the communication between WP7 and the PC is different to WM and the PC, so the forensic tool may be unable to load the program onto the WP7 phone. Second WP7 is unable to run any WM programs, so even if the program is loaded onto the WP7 phone, the program may not execute correctly if at all. Currently there is a gap in the literature between the

mobile forensics and WP7. The changes introduced with WP7 compared to WM could affect the ability of WM forensic tools and techniques to acquire and analyse data from a WP7 phone due to the reasons described above.

1.2 MOTIVATION

The MS mobile OS has been available since 1999 in various forms under various brandings with the latest being WP7. The length of time which WM has been available has meant that much research has been done on many aspects of WM including WM forensics. Each new version of WM is based largely on the previous of WM i.e. WM6 was based on WM5, all the way back to the original Windows CE. Because WM was based largely on the previous version, many of the technical and forensic knowledge gained from WM are applicable to many versions of WM. However because WP7 was not based on WM and includes many changes and the current forensic tools and techniques used on WM may not be applicable to WP7. Likewise the research and literature on WM forensics may not be applicable to WP7, leaving a gap in WP7 forensics.

Phones running WP7 is predicted to have 19.5% of market share of the smart phone market by 2015 according to Gartner (a market research firm) (Gartner, 2011b). If the predictions by Gartner turns out to be correct then WP7 will be the second most popular OS for smart phone and even if the predictions by Gartner turn out to be incorrect, WP7 is still likely to be one of the most popular OSs for smart phones.

The motivation of the research is based on the gap in WP7 and WM forensics caused by the redesign of WP7. Currently the effects of WP7 on forensic tools and techniques is unknown. Given the potential of WP7 to be one of the most popular OS for smart phones research into these aspects will be useful for a digital forensic investigator as well as forensic tool developers.

1.3 STRUCTURE OF THESIS

The research will be structured into six chapters. Chapter 1 is an introduction to the research and identifies the problem area requiring research, the motivation for the research, and concludes with an outline of how the research is structured.

Chapter 2 reviews the literature to identify the problem areas between digital forensics and WP7. First literature on digital forensics will be reviewed in Section 2.1, followed by reviews of literature on WM and WP7 to illustrate how WP7 has changed compared to WM in Section 2.2 and Section 2.3 respectively. Then literature on WM forensics will be reviewed to establish the current forensic tools and techniques in Section 2.4. A summary of the issues and problem areas identified by the literature review will be discussed in Section 2.5. Because WP7 was recently released at the start of the research, changes and updates to WP7 and other aspects related to WP7 may occur during the research. Some of the changes may not be incorporated into the research due to resource and time constraints. Section 2.6 will track some of the developments in WP7 which may not be incorporated into the research, but may be of use for further research.

Chapter 3 defines the methodology including the research question and hypothesis to be used to conduct the research. Published similar studies will be reviewed in Section 3.1 to establish the current forensic tools and techniques used on WM, and what data can be extracted from WM using the tools and techniques. The research question and hypothesis will be defined in Section 3.2, which will be further defined into sub questions and sub hypotheses. The research design which outlines how the research will be conducted will be defined in Chapter 3.3. Chapter 3.4 defines how data for the research will be collected, processed, analysed, and presented. The scope or limitations to the research will be defined in Section 3.5.

Chapter 4 reports the findings from the experiments conducted during the research. The specifications of the equipment used during the research is given in Section 4.1. Section 4.2 establishes what data can be extracted from a WM phone using current WM forensic tools and techniques based on the literature review. Section 4.3 uses the information from Section 4.2 to generate test data for the WP7 phone to be tested in the research. Sections 4.4 - 4.11 reports the procedure used to conduct each experiment, the results from each experiment, and some analysis of the results will also be given.

Chapter 5 discusses the findings reported in Chapter 4 in relation to the research question and hypothesis, as well as the implications of the findings to WP7 forensics. Section 5.1 discusses the findings to answer the research question and test the research hypothesis. Section 5.2 discusses the findings to put the

findings into the larger context of WP7 forensics. Section 5.3 discusses new developments of WP7 during the research which were unable to be incorporated into the research. Section 5.4 discusses the alternative tools for WP7 which were developed by sources other than forensic tool developers. Section 5.5 discusses implications of the research for a digital forensic investigator.

Chapter 6 concludes the research with a summary of the findings in Section 6.1, followed by the limitations of the research in Section 6.2, and finally a discussion of possible future research in Section 6.3.

Chapter Two
Literature Review

2.0 INTRODUCTION

The focus of the research is on the Windows Phone 7 (WP7) smart phone Operating System (OS) from Microsoft (MS) and the implications of WP7 on a digital forensic investigation. WP7 was released by MS at the end of 2010 replacing the previous smart phone OS WM6.5 (Microsoft, 2010a). WP7 is forecasted by the research firm Gartner (Gartner, 2011a) to grow from 4.2% of the mobile OS market share in 2010 to 19.5% by 2015 (Gartner, 2011b), making WP7 the second most popular mobile OS behind Android by Google (Android, n.d.).

The digital forensic investigation process for mobile devices such as smart phones are well established and have been standardised by standards organisations such as The National Institute of Standards and Technology (NIST). Digital forensic investigations of predecessors to WP7 such as WM are also well established, and many mobile forensic tools available to digital forensic investigators support WM phones. WP7 introduced many changes to the MS mobile OS WM, and at the time of writing, no literature on WP7 forensics was found.

Literature in several areas of forensics and WM were reviewed to establish the current methods of conducting a forensic investigation involving WM phones. Literature on WP7 was reviewed to establish the changes made to WP7 compared to WM and how the changes may affect a forensic investigation.

Literature on the models and standards for conducting both a general digital forensic investigation (any digital device) and a mobile digital forensic investigation (any mobile device) is reviewed in Section 2.1. Literature on WM phones, and previous studies involving WM forensics were reviewed in Section 2.2. WP7 literature was reviewed in Section 2.3 to establish the changes made to WP7 and compared to WM. Literature on the various tools and techniques used for a forensic investigation involving a WM phone are reviewed in Section 2.4. A summary of problem areas is given in Section 2.5. Because WP7 was a relatively new product and the fast changing nature of the mobile OS landscape, Section 2.6 lists some current developments with WP7 as the research was progressing.

2.1 DIGITAL FORENSIC INVESTIGATION PROCEDURE

The procedure for a digital forensic investigation can vary greatly depending on the resources available, the importance of the investigation, the policies of the company, and the individual situation and circumstances surrounding the investigation. However the process of the investigation can usually be broken down into four parts, as described in the Guide to Integrating Forensic Techniques into Incident Response published by NIST (Kent, Chevalier, Grance, & Dang, 2006) namely Collection, Examination, Analysis, and Reporting. Each stage transforms what is stored digitally on the media into evidence during an investigation as shown in Figure 2.1.

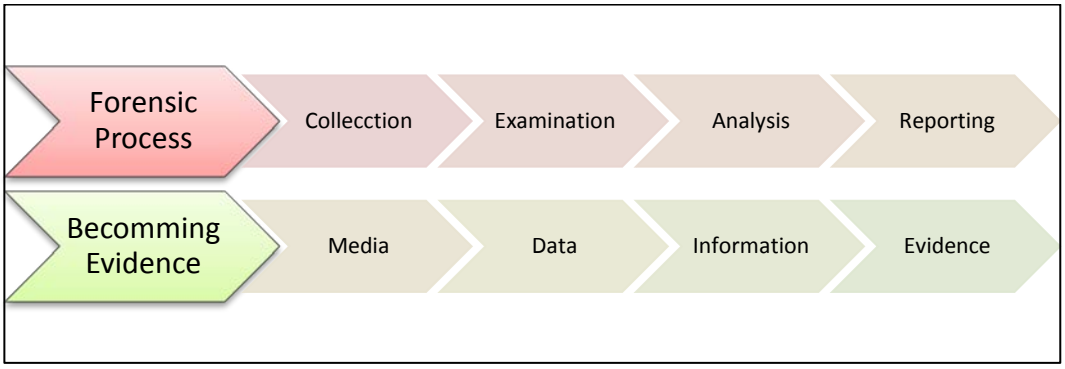


Figure 2.1: The Forensic Process (adapted from Kent et al. (2006))

The forensic process described show how media is transformed into evidence though the four stages. The Collection stage is where data is acquired from a physical item where the data is stored (the media), such as a phone, memory chip, or hard drive. The Examination stage is where the data acquired from the media is examined and the acquired data is transformed into something understandable for the investigator. The Analysis stage is where information from the examination stage is analysed to find information relevant or of interest to the investigation. The Reporting stage is where the entire process of transforming the media into information is documented. Following the process correctly and documenting the process correctly allows the information to become evidence. Evidence does not necessarily mean that the process is only used when the investigation will likely lead to actions in the court (although many do). The process may be applicable for a wide variety of forensic investigations.

A more practical guide to a digital forensic investigation is the Good Practice Guide for Computer-Based Electronic Evidence published by The Association of Chief Police Officers (ACPO) (Association of Chief Police Officers, n.d.), and is used by law enforcement agencies in the United Kingdom. The ACPO guide has four principles which aid the investigator in maintaining the integrity of the data which could be used as evidence. The four principles are outlined in Table 2.1.

Principle	Description
Principle 1	No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
Principle 2	In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3	An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4	The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Table 2.1: ACPO Principles for Good Practice for Computer-Based Electronic Evidence

Principle one is to leave as small as possible digital footprint when conducting a forensic investigation. The investigator should minimise any physical damage to any device or media, as well as minimising any alteration of any data stored on any device or media. Principle two is to only allow competent investigators to do the investigation. The investigator should have the relevant experience or qualifications to perform the investigation. Principle three is to ensure the forensic process of acquiring the evidence is verifiable and repeatable. The forensic process used to acquire the evidence should be documented so should the evidence be acquired again, the results will be the same. The usual mechanism of checking if evidence acquired is the same is through the use of a digital signature or fingerprint of the evidence. Digital fingerprints of files are generally achieved using hashing algorithms. Hashing is discussed in the NIST guide, where the standard hashing algorithms used are MD5 and SHA-1 (Kent et al., 2006). Hashing algorithms perform mathematical calculations on files to give them a unique hash value. With the MD5 hash algorithm, the chances of two different files having the same hash value is one in 3.4×10^{38}, in other words one in every

340 billion billion billion billion (AccessData, 2006). Principle four is where the person in charge of the investigation has to ensure that not only the principles are adhered to, but also the relevant laws and regulations are adhered to.

The NIST and ACPO guidelines focus on different aspects of the investigation, but ultimately achieve the same goals in maintaining the forensic soundness of data collected during an investigation. The NIST and ACPO guidelines are designed to be used for general digital devices in a forensic investigation, and not specific to mobile devices. A comprehensive model for carrying out a forensic investigation on a mobile device is the Guidelines on Cell Phone Forensics published by NIST (Jansen & Ayers, 2007). These guidelines cover all aspects of an investigation to maintain forensic soundness of the evidence and was written as a guide to investigating cell phones in general, and covers smart phones and personal digital assistants (PDA). An even more specific forensic model was proposed by Ramabhadran (2008) named the Windows Mobile Forensic Process Model (WMFPM). The WMFPM was developed specifically for WM forensic investigations.

While there are guidelines for a mobile investigation and guidelines for a WM investigation, the implementation of the guidelines vary depending on the organisation, the purpose of the investigation, and the special circumstances of each investigation. The WMFPM, like the NIST and ACPO guidelines are designed to aid forensic investigators and organizations to set up appropriate policies and procedures to conduct an investigation.

2.2 A BRIEF HISTORY OF WINDOWS PHONE

WP7 is the latest smart phone OS from MS (Microsoft, n.d.-e) which was announced on February 15th at The World Mobile Congress 2010 (Microsoft, 2010b). WP7 replaced WM6, which replaced WM 5 and so on. Figure 2.2 shows the history of WP7 and earlier OSs back to the original Windows Compact Edition (CE) 1.0 released in 1996.

Figure 2.2: Windows CE Timeline (adapted from "A Brief History of Windows CE" (Tilly, 2007))

Windows CE (WCE) was released in 1996 (Randolph & Fairbairn, 2010) as an OS designed to run on embedded devices such as GPS navigation systems, point of sales machines, as well as phones. Phones running WCE were branded simply as running "Windows CE".

In 2000 phones running WCE were rebranded into two different types - Windows PocketPC and Windows SmartPhone. The main difference was the definition, Pocket PCs were phones which required two hands to operate, such as phones with a stylus. The user holds the phone in one hand and the stylus in the other to operate the phone. Smart phones were phones the user could operate with one hand, i.e. phones without a stylus (Markiewicz, 2005). The earlier devices running WCE and Pocket PC may have all the other functionalities of a smart phone but without the phone, such as a PDA.

In 2003 both Pocket PC and Smart Phone were replaced by WM (Microsoft, 2003). The first WM OS was named "Windows Mobile 2003", which was later replaced by WM5, then WM6, until the latest version WM 6.5 in 2010 (Notebooks.com, 2010). WM was losing market share in the smart phone OS market, going from 10.2% in the first quarter of 2009 down to 6.8% in the first quarter of 2011, whereas Apple and Android phones were gaining market share

during the same period (Gartner, 2010). In 2010 WM was rebranded to "Windows Phone".

For the purposes of the research WP7 refers to Windows Phone 7 and WM refers to all versions of Windows Mobile OS prior to WP7, including Windows Mobile, Windows PocketPC, Windows SmartPhone, and WCE. All these devices will be referred to as a phone rather than a device, even though not all these devices have phone functionality.

The evolution of the WP7 OS may give the impression that each successive version of the mobile OS was built on top of the previous version incrementally, which is largely true for older versions of the OS. For example WM 6 was based on WM 5 which was based on WM 2003 and so on all the way back to the original WCE (Herrera, 2007). WM being based on the previous version allows different versions of WM to have backwards compatibility, which is to say WM6 can run many applications designed to run on WM5, and WM5 can run many applications designed to run on WM6.

2.2.1 Backwards Compatibility

Because the WM OS was based on the previous version, there is much commonality between them. Generally speaking a newer version of WM can run applications designed for an older version of WM. Newer versions of WM being able to run software designed for older versions is known as backwards compatibility. Backwards compatibility means many applications designed for WM was designed to work on many different versions of WM. Even though there may be inherent backwards compatibility due to the design of WM, there were applications which only ran (or only ran well) on specific versions of WM, or phones with specific hardware. The WM platform (OS and hardware) may have a variations between manufacturers and generations of phones. The many varying types of WM phones means the WM OS is fragmented.

2.2.2 Windows Mobile Platform Fragmentation

Having a variation of phones all branded as WM phones is known as fragmentation, and the more the hardware and/or software vary, the more fragmented a platform is said to be. For a developer, WM fragmentation means an application may only work on some phones, and not others, since the developer is

unsure as to exactly what the phone will be in terms of hardware and software. Both Steve Ballmer, MS CEO (Warren, 2010) and Steve Job, Apple CEO (Miller, 2010) have criticised the Android mobile OS from Google as being too fragmented. Applications designed for Android phones may not work on all Android phones, whereas applications designed to run on WP7 or iPhone will work on every WP7 phone and every iPhone.

Phones which ran WM can vary greatly in hardware. The hardware requirements for WM (different versions of WM has different hardware requirements) were minimal and left a lot of scope for manufacturers to implement different hardware into their WM phones. Take a range of phones designed to run WM, the phones may all be different, some WM phones may have a touch screen, whereas another does not. Some may have a camera, some may not. One application may run well on one WM phone, yet run very poorly on another due to different processor, memory, graphics, and other hardware. Phones with the same hardware can vary greatly in software also. For example two smart phones may be running the same version of WM (say 6.5), yet look and feel completely different to the user since different manufacturers can customize the OS so much.

Generally a cheap WM will have inferior hardware compared to a more expensive WM phone, and an older WM phone will have inferior hardware to a later model WM phone. These differences mean that even though a phone was branded as running WM, the hardware and performance could vary greatly. So even though applications (apps) are designed to run on WM, some WM phones will not run the app, and others with varying degrees of performance. These difference in hardware and software implementation of different WM phones creates the fragmentation between the different WM phones.

2.2.3 Windows Mobile User Experience

ISO 9241-210 (ISO, 2010) defines User Experience (UX) as

> "A person's perceptions and responses that result from the use or anticipated use of a product, system or service".

The user is said to have a rich UX with a product if the use of the product is enjoyable to the user. Because of the fragmentation of WM phones, some WM

phones may give the user a very rich or good UX, whereas other may not. The UX was inconsistent and varied greatly depending on which WM phone was used.

2.3 WINDOWS PHONE 7

To prevent further fragmentation of WM phones and the resulting inconsistent UX, WP7 was completely redesigned by MS to such an extent that WP7 can almost be considered an entirely different OS to WM. WP7 had strict hardware requirements as well as strict software guidelines for applications, giving all WP7 phones a consistent rich UX and less fragmentation.

With the new hardware and software requirements, WP7 was not backwards compatible with any previous versions of WM, meaning older software designed to run on WM will not run on WP7. WP7 will also not run on any older devices designed to run WM. The hardware required to run WP7 is much higher than that of WM. The internal workings on the OS has also been changed, WP7 now requires a 8GB (minimum) SD card, which is not removable by the user. Most modern WM phones supports a user removable storage media, but in the case of WP7 (much like Apple's iPhone), no user removable storage media is supported. One of the reasons for WP7 not supporting a user removable storage media is because WP7 uses the Read Only Memory (ROM) and the SD card together and treat the two as a single unit - “It creates a single file system that spans the internal storage and the SD card” (Microsoft, 2011b). So if the SD card is removed, the information is useless since only parts of the information is on the SD card, and parts are still in the WP7's ROM. WP7 will not operate without the SD card. If the card was replaced, the whole system is reconfigured when the phone is turned back on. On WM phones user data stored on the removable storage media such as an SD card can be forensically acquired and analysed independently of the phone. On a WP7 phone the internal SD card cannot be forensically acquired or analysed independently of the phone.

2.3.1 Synchronisation

Synchronisation is the process of syncing the data or files on the WM/WP7 device with a computer, such as a Windows PC (desktop/laptop). The types of data which is synchronised or sync could be emails, contacts, music, and other personal data. The process of establishing a connection between a WM phone to a

computer is known as pairing or syncing. Each time a new WM phone is connected to the PC, the phone and the PC has to be synced before any data exchange can occur. The software in which WM uses to sync with a Windows PC is ActiveSync or Windows Mobile Device Centre (WMDC) depending on what version of Windows (Herrera, 2008; Microsoft, n.d.-b), and the software in which WP7 uses to sync with a Windows PC is Zune (Microsoft, n.d.-d).

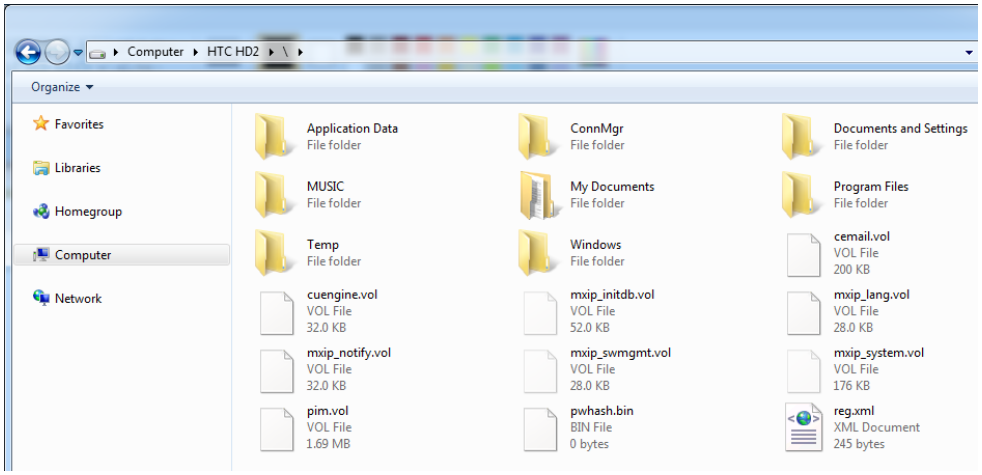


Figure 2.3: Windows Mobile Files

WM allows syncing of emails, contacts, and other user files such as pictures and music with the PC. WM also allows access to the files on the phone. The WM phone is shown on the PC as a device which can be viewed using Windows Explorer (although some files are read only) as shown in Figure 2.3. The system files on a WM phone is similar to that of Windows on a PC (Casey, Bann, & Doyle, 2010). WP7 allows syncing of user media files such as music and pictures only, and does not show on the PC as a device, and the files on the WP7 phone cannot be viewed by the PC. The system files on a WP7 is unknown as no literature was found on the subject.

2.3.2 Hardware

WP7 has much tighter hardware requirements compared to WM (Polimenov, 2010a, 2010b; Thurrott, 2010). The requirements were intended to reduce fragmentation and offer a consistent and rich user experience. Table 2.2 is summary of the hardware requirements for WP7 and how the requirements differs from WM devices. With WP7 MS has specified much tighter hardware

requirements and have limited the amount of customization which can be done in software. The result of the tighter requirements means when dealing with a WP7 device, not only does the system look and feel the same between devices from different manufactures, the hardware will also be very similar. Note these requirements are minimum requirements, so some WP7 phones may have better hardware or have add-ons not mentioned such as a hardware keyboard.

Type	**Windows Phone 7**	**Windows Mobile**
Screen	480x800 (WVGA) or 320 x 480 (HVGA) Capacitive touch screen with 4 touch points. *Only 480 x 800 phones are currently available	Varying resolution May or may not be touch screen Models with touch screen may have single or multi touch point May nor may not have a stylus
Graphics	DirectX 9 hardware acceleration	Varying hardware and technologies
Buttons	Back, Start, Search, Power/Sleep, Volume Up, Volume Down, Camera	Varying buttons depending on manufacturer and model
Camera	5 Megapixel + with flash	May or may not have camera. Models with camera may have varying pixel count
Sensors	Accelerometer, Compass, Light sensor, Proximity Sensor	Most models did not have any of these sensors
CPU	ARMv7 1GHz or higher	Varying CPU with varying speeds
RAM	256MB	Varying sizes
ROM	256MB + 8GB (minimum)	Varying sizes
GPS	Assisted GPS (AGPS)	May or may not have GPS sensor
Radio	FM radio turner	May or may not have FM radio
Bluetooth	2.1 + EDR	May or may not have Bluetooth

Table 2.2: Windows Phone 7 Hardware Requirements

Table 2.3 is a summary of the hardware requirements for WP7, and whether the requirements impacts a digital forensic investigation. Most of the hardware changes are unlikely to affect a forensic investigation except for the Random Access Memory (RAM), ROM, and the synchronisation mechanism which will be discussed later in the respective sections.

2.3.2.1 Screen

The screen requirements of a capacitive touch screen of a certain resolution prevents fragmentation since all WP7 phone will have a known screen type. The screen requirements also delivers a certain level of user experience to the user. The screen requirements does not impact on a digital forensic investigation.

2.3.2.2 Graphics

The graphics requirements allows for a certain level of performance on a WP7 phone, which allows a certain level of user experience. The technology in the graphics engine of WP7 does not impact on a digital forensic investigation.

Hardware Requirement	Impacts Forensic Investigation
Screen	
Graphics	
Buttons	
Camera	
Sensors	
CPU	
RAM	X
ROM	X
GPS	
FM Radio	
Wi-Fi	
Bluetooth	
Synchronisation (USB)	X

Table 2.3: Windows Phone 7 Hardware Impact On Forensics

2.3.2.3 Buttons

The buttons requirement on WP7 is to prevent fragmentation and deliver user experience, as every WP7 will have the same buttons which do the same things. One of the last and most advanced WM phones released was the HD2 by HTC (HTC, n.d.) The HD2 met all the hardware requirements of WP7, except for the buttons requirement. The HD2 had extra send and end buttons popular on WM phones. Because the HD2 did not totally conform to the buttons requirement MS announced that WP7 will not be made available to the HD2 (Flynn, 2010), even though the HD2 was capable of running WP7. A fact made evident by hackers succeeding in getting the HD2 to run WP7 (Warren, 2011). The number of buttons does not affect the digital forensic investigation process.

2.3.2.4 Camera

The camera requirements ensures all WP7 phones have a camera of a certain quality. The camera requirement prevents fragmentation and ensures the same UX on any WP7 phone. The camera requirements does not impact the digital forensic investigation process. The pictures taken with the camera and where they are stored can impact the digital forensic process.

2.3.2.5 Sensors

The many sensors required in a WP7 allows for a richer UX, and prevents fragmentation. The sensors indicate if the device is moving, which way the device is moving, and the orientation. Application developers for WP7 phone can utilise the sensors to create a richer UX. The sensors does not impact the digital forensic investigation process.

2.3.2.6 CPU

The CPU requirement is high in order to deliver a rich UX for the end user, and prevents fragmentation The actual architecture and speed of the CPU does not impact the digital forensic investigation process.

2.3.2.7 RAM

The RAM requirement ensure WP7 can deliver a rich UX to the end user and prevents fragmentation. There may be valuable data residing in the RAM which may be of interest to a digital forensic investigation. How the architecture of the RAM, and how data is stored in the RAM, and how best to acquire that data may impact the digital forensic investigation process if the RAM architecture has changed.

2.3.2.8 ROM

The ROM requirement ensures WP7 can deliver a rich UX to the end user and prevents fragmentation. With WM phones, all data (system files and user files) are stored in the ROM. With WP7, the data is stored on the ROM and the internal SD card (Microsoft, 2011b). WP7 does not have a user removable memory i.e. the internal SD card is not removable by the user and can't be changed with another SD card. The SD card is also locked to the phone, and cannot be removed and used in another phone. Inserting a new SD card into the WP7 will lock the new SD card and the WP7 OS will be reset to default factory settings. The internal SD card which is used together with the ROM which creates a single file system. How the files are spread between the ROM and the internal SD card is unknown. The ROM is where data is stored, and the changes to the ROM may mean that forensic tools are unable to acquire data from the ROM.

2.3.2.9 GPS

The GPS requirement ensures WP7 can deliver a rich UX to the end user and prevents fragmentation. The actual GPS chip (the brand or type) does not impact a digital forensic investigation, but the fact that a GPS will be available on every WP7 phone means that there may be location data stored on the phone. The GPS data is stored on the phone and not on the GPS chip, so GPS chip does not impact the digital forensic investigation, however GPS data does.

2.3.2.10 FM Radio

The FM radio requirement ensures WP7 can deliver a rich UX to the end user and prevents fragmentation. The FM radio does not store data and does not impact the digital forensic investigation process.

2.3.2.11 Wi-Fi

The Wi-Fi (or wireless local area network) on a WP7 phone should be no different to having Wi-Fi on a WM phone. Which is to say, the implementation of Wi-Fi (such as 802.11 a/b/g/n) hasn't changed from WM.

2.3.2.12 Bluetooth

The Bluetooth on a WP7 phone should be no different to having Bluetooth on a WM phone. Which is to say, the implementation of Bluetooth hasn't changed from WM.

2.3.3 Software

The WP7 also has guidelines for the look and feel of an application as well as the User Interface (UI) of an application. The style outlined in the guideline is codenamed Metro (Polimenov, 2010c). These guidelines are also to prevent fragmentation and to deliver a consistent and rich user experience, since the look and feel of any WP7 phone will be the same.

As discussed earlier WP7 is not backwards compatible with earlier versions of WM software, which means WP7 cannot run on phones designed for WM, and WP7 is not able to run software designed for WM. With the changes in WP7 platform as well as the applications (apps), there is a possibility that the tools designed to extract data WM phones will not be able to extract the same data

from WP7 phones. Table 2.4 is a summary of the data extracted from WM phones by Casey et al (2010), and how every data type has changed in WP7.

Windows Phone 7 Software Platform	Changed from Windows Mobile	Impacts Forensic Investigation
Connection to Computer	X	X
System Files		
File System	X	X
System Files	X	X
Registry	X	X
Deleted Files	X	X
User Files		
Contacts	X	X
Call Logs	X	X
Messages/ Emails	X	X
Calendar / Appointments	X	X
User Documents / Pictures	X	X
Internet Browsing History	X	X
Bookmarks	X	X

Table 2.4: Windows Phone 7 Software Changes

2.3.3.1 File System

The file system used by WM is a variant of FAT known as Transaction safe FAT or TFAT (MSDN, 2010b). The entire file system is stored in the ROM. The file system used by WP7 is a Transaction safe variant of exFAT or TexFAT (MSDN, 2010a). Digital forensic tools designed to work with WM devices may not be able to extract of interpret the data correct due to these changes.

The compression used by WM is known as XPR, and the compression used by WP7 is known as XPH. XPH is both faster than XPR and provides better compression than XPR (XDA Developers, 2011e). How much of the WP7 file system is compressed is unknown. How forensic tools may analyse and interpret data which has been compressed using XPH is also unknown.

2.3.3.2 Registry

On WM, the registry is stored in hive files or hives - user.hv, default.hv or system.hv (depending on version of WM) (Casey et al., 2010). The registry of WM is similar to that of Windows for a PC. The registry of WP7 is unknown as no literature was found on the subject.

2.3.3.3 Deleted Files

Deleted files have been recovered from WM with varying success, usually by taking a physical image of the phone (Klaver, 2010; Rehault, 2010). Due the changes in the file system and the other factors described earlier, the techniques used to recover deleted files from WM may not work with WP7.

2.3.3.4 User Files

The majority of the data of interest in a mobile forensic investigation is in the user data such as contacts, messages, emails, and web browsing. Digital forensic tools designed for WM can extract user files from WM devices. Besides the changes in appearance and functionality of the user files, the implementation of the way the files are stored on WP7 phone may have changed.

2.3.3.5 Contacts

Contacts on a WM device are stored in a database file named pim.vol (Casey et al., 2010). Contacts in WM may contain phone numbers and/or emails. These are usually entered into the phone manually or synchronised with Outlook.

Contacts in WP7 can be similar to those in WM in that they can be manually entered, but WP7 also synchronises contacts with Instant Messaging (IM) (such as Yahoo Messenger (Yahoo, 2011)), social networks (such as Facebook (Facebook, 2011)), and Windows LIVE (Microsoft, 2011a). Contacts on WP7 is access though the People Hub (Stroh, 2010), one of the hubs outlined in the MS guidelines to the User Interface for WP7 (MSDN, 2011). The appearance and accessibility of the contacts has changed in WP7 compared to WM, but the actual implantation of how the contacts are stored on WP7, and thus how to extract the data is unknown.

WP7 no longer allows synchronisation with Outlook. In order to get Outlook contacts onto the phone, a Outlook Hotmail Connector has to be installed (Microsoft, n.d.-c). The Outlook Hotmail Connector synchronises Outlook contacts with a Hotmail account (which is linked to a Windows LIVE account) and the contacts will then be synchronised from Hotmail to the phone.

2.3.3.6 Call Logs

On WM, call logs are stored in the clog.db database, which is part of the pim.vol database (Casey et al., 2010). The Call log in WP7 is similar to call log in WM in

appearance and functionality. Implementation of how the call logs are stored in WP7 is unknown.

2.3.3.7 Messages / Emails

WM uses cemail.vol and pim.vol databases to store text messages and mail items (MSDN, 2009). There is also a messaging folder which stores the files in .mpb format, and .att for attachments (Casey et al., 2010).

Messages in WP7 include both Short Message Service (MMS) which are text only messages and Multimedia Message Service (MMS) which can contain text, pictures, and videos. The way the messages are presented has changed due to the MS UI guidelines, and the hardware and system changes described earlier may mean the way the emails and messages are stored may also have changed. The details on how the emails are stored are not known.

WP7 can send and receive emails from a number of sources including webmail, Microsoft Exchange, and POP mail. Table 2.5 lists the types of email accounts supported by WP7.

Email Type	Description
Windows Live	Hotmail, Xbox Live, and Live Messenger
Outlook	Microsoft Exchange type server, usually used in a corporate environment
Yahoo! Mail	Yahoo's email service
Google	Google's email service
Other/Advanced	POP or IMAP, commonly used by ISPs for emails.

Table 2.5: Email support in Windows Phone 7

Emails in WP7 works slightly differently from how other data is managed by WP7. For example, with Contacts, WP7 will show all contacts in the one place (the People Hub) even though the contacts may have come from different source. Likewise with the Calendar, WP7 will use one calendar app showing many appointments from many sources. With emails however, each email account which is set up has to run on a separate email app. So if the user has set up four email accounts, there will be four email apps, one for each email account (Thurrott, 2010).

2.3.3.8 Calendar / Appointments

WM uses pim.vol to store calendar and appointments and both can be synced with Outlook (Casey et al., 2010). The calendar and appointments in WP7 differs from WM in terms and appearance as well as functionality. Appointments in WP7 can be either entered manually, or the imported from a variety of calendars including Windows Live and Google, and presents all the appointments in the one single calendar application.

2.3.3.9 User Documents / Pictures

In WM, the user's personal files such as documents and pictures are stored in the My Documents folder, which will be familiar to those who use a Windows PC. WM files can be read directly by the PC and copied or synced to the PC.

WP7 user files cannot be viewed or copied to the PC in the same way WM can, but can be synced to the PC using Zune. WP7 also allows many user files to be stored on the cloud (SkyDrive) and the PC can be synced to the cloud (Thurrott, 2010).

2.3.3.10 Internet Browsing History

With WM files such has browsing history, cache and cookies can be found in the Windows\Profiles\guest folder (Casey et al., 2010).

WP7 has a newer version of Internet Explorer (IE) (the default web browser for both WM and WP7) (Thurrott, 2010), and as a result, the internet browsing history may be stored differently on WP7 compared to WM. Where and how the internet browsing history is stored is not known.

2.3.3.11 Bookmarks

Bookmarks (or favourites) are stored based on the version of the web browser. By default WM stores bookmarks in the Windows\Favorites folder (Casey et al., 2010). Because WP7 has a newer version of IE, where the files such as bookmarks are stored is unknown.

2.4 WINDOWS MOBILE FORENSICS

A typical mobile forensic investigation is conducted using forensic tools (software) designed to examine and analyse mobile phones. Some of the tools have been

listed in NIST Guidelines on Cell Phone Forensics (Jansen & Ayers, 2007) mentioned in Section 2.1. The tools typically provide a logical acquisition of the mobile phone, meaning only files visible to the tool are acquired. More advanced methods allow a physical acquisition of the mobile phone, meaning everything is acquired. Physical acquisitions can yield more information than logical acquisitions, but has a higher risk of damaging the phone, and usually require specialised equipment and in-depth knowledge about the internals of the phone. Logical and physical acquisitions will be discussed in Section 2.4.2.

2.4.1 Windows Mobile Hardware

Most modern smart phones have two types of internal memory - ROM and RAM, and may also have external or removable memory (Casey et al., 2010).

2.4.1.1 ROM

Read Only Memory (ROM) is where the files are stored and includes the OS, and user files. These days the ROM is usually flash memory (usually NAND) and sometimes referred to as flash or flash memory by many articles. ROM in older devices was read only and working data (data while the device was running) was stored elsewhere, so all the working data on the device was lost when the device was turned off. Modern devices can read and write to the ROM, so working data is not lost if the device is turned off.

2.4.1.2 RAM

Random Access Memory (RAM) has the same functionality as RAM in a computer, data in the RAM is used as temporary storage, and is lost if the device is turned off or reset.

2.4.1.3 External / Removable Memory

In most modern WM phones the removable memory comes in a form of a memory card such as an SD card. The memory card can be changed and removed and can usually be read directly by other devices such as a PC. The data stored on the card is not lost if the card is removed or the device is turned off.

2.4.2 Windows Mobile Forensic Acquisition

Data from WM phones like data from most digital devices can be acquire either logically or physically. Logical acquisition is acquiring data which is only visible to the forensic tool whereas a physical acquisition is a bit-by-bit copy of the entire storage. The storage area may contain deleted data and unallocated or blank areas. As shown in Figure 2.4 a logical acquisition only acquires the visible data from the storage area, whereas a physical acquisition will acquire the entire storage area, including the deleted data and unallocated or blank area.

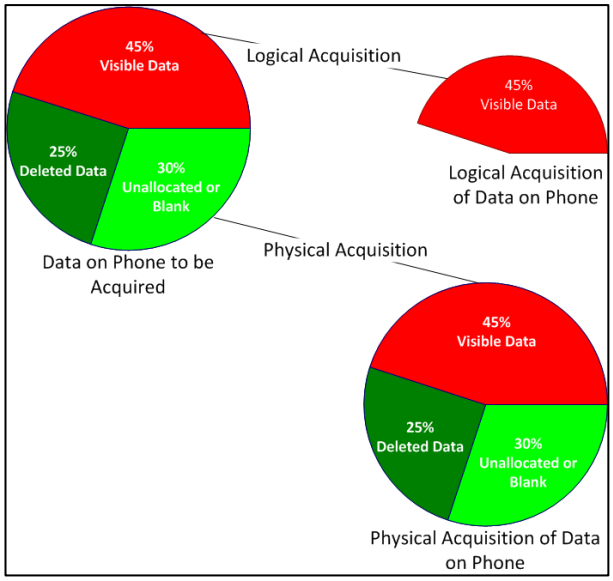


Figure 2.4: Physical vs. Logical Acquisition

Physical acquisitions are usually preferred over logical acquisitions (Ayers, Jansen, Cilleros, & Daniellou, 2005). The majority of forensic tools can only perform logical acquisitions from WM phones. Some forensic tools can perform both logical and physical acquisitions from WM phones (Casey et al., 2010)

2.4.2.1 Logical Acquisition

Logical acquisition of WM phones are usually performed using forensic tools such as the ones listed in Table 2.6. Most forensic logical acquisition tools cannot access the WM phone's memory directly but rather through a Hardware Abstraction Layer (HAL) (Klaver, 2010). The HAL for WM is either Active Sync or WMDC, depending on what version of Windows is running on the connected

PC (see Section 2.3.1), and most WM forensic tools require Active Sync/WMDC to be installed on the PC in order to acquire any data from the WM phone.

As discussed in Section 2.3.1 once the WM phone is synced with the PC via Active Sync/WMDC, both the data on the WM phone and the removable storage card (if the WM has one) is visible to the PC showing both system files and user files. The visible files can be acquired by the forensic tools but non-visible files such as deleted or unallocated files will not be acquired.

WP7 connects to the PC using a USB connection in the same way as WM, but instead of using Active Sync/WMDC to sync with the PC, WP7 uses Zune. Once the WP7 phone is synced with the PC using Zune, the data on the WP7 phone is not visible to the PC directly, and can only be view through Zune. Zune automatically synchronises user media files such as pictures, movies, and music files with the PC, and any copying, deleting, or moving of the media files on the WP7 phone has to be done using Zune. Most WM forensic tools require Active Sync/WMDC to acquire data from the WM phone. The effects of WP7 using Zune on the WM forensic tools are unknown, hence what data can be extracted from a WP7 phone using the WM forensic tools is unknown.

2.4.2.2 Physical Acquisition

A physical acquisition methods such as using the test standards from the Joint Test Action Group (JTAG) (IEEE Standards Association, n.d.) or chip extraction (Klaver, 2010) (both discussed in Section 3.1) requires direct access to the device where data is stored, such as the WM phone's memory which is a chip. The JTAG method requires the WM phone to be opened and requires access to the memory chip using JTAG test points on the phone's mainboard (Kim, Hong, & Ryu, 2008). The chip extraction method requires the memory chip to be removed from the phone's mainboard completely and acquired using specialised chip readers. Physician acquisition methods like JTAG and chip extraction may acquire data not obtainable using logical acquisition methods, but has a higher risk of damaging the device (Klaver, 2010). Specialist equipment is also required to access or extract the memory without damaging any data or hardware.

With WM phones, a physical acquisition using forensic tools is possible without opening the phone. Forensic tools such as XRY (Micro Systemation, 2011) and UFED (Cellebrite, 2011) are able to perform physical acquisitions on

WM phones once the WM phone is synced to the PC using Active Sync/WMDC. The forensic tool copies an agent (an application) onto the WM phone, and the agent dumps the data on the WM phone's memory to the forensic tool (Klaver, 2010). Because WP7 cannot run any WM applications, should the forensic tools be able to copy the agent onto the WP7 phone, the agent may not be able to run.

Another method of acquiring a physical dump from a WM phone through Active Sync/WMDC is using the bootloader method (Rehault, 2010). The bootloader is the part of the phone which gets loaded when the phone is turned on or reset (Klaver, 2010). Some WM phone manufacturers have customised bootloaders installed so the device can be updated, tested, or for maintenance reasons. Most bootloaders have limited capabilities because there is a high risk of hacking and a high risk of damaging the device. Rehault (2010) used the bootloader on an HTC TyTn II smart phone running WM6, and a program from HTC designed to communicate with the bootloader, and was able to capture the entire image of the ROM. The bootloader method used by Rehault will only work with HTC devices, since the bootloader from different manufacturers are different, and the program written to communicate with the bootloader was specific to the HTC bootloader. Klaver (2010) refers to physical acquisition using tools utilizing Active Sync/WMDC as a pseudo physical acquisition. Pseudo physical acquisition methods rely on the Active Sync/WMDC connection to communicate between the PC and the WM phone to acquire the data. The effects of WP7 using Zune on the pseudo physical acquisition methods are unknown, hence what data can be extracted from a WP7 phone using the pseudo physical acquisition methods are unknown.

For the purposes of the research both pseudo physical acquisition methods and physical acquisition methods will be referred to as physical acquisition methods.

2.4.3 Mobile Forensic Tools And Techniques

The usual method of conducting a mobile forensic investigation is by using mobile forensic tools. The tools are designed to aid the investigator throughout the forensic investigation process. Most tools will allow the investigator to acquire data with hashing to ensure integrity of the data, can analyse the acquired data, and can generate report or logs to ensure the process is repeatable and verifiable.

Some tools will perform all these tasks, while others may only do some of these tasks, so a combination of tools may have to be used. The investigator does not have to use tools for a digital investigation, for example the tools available to the investigator may not be compatible of acquiring or analysing data from a device. In these cases the investigator may have to perform each stage of the investigation manually. Most mobile forensic tools can perform many types of analysis on data acquired from phones, such as contacts, appointments, and emails. Most mobile forensic tools also support many different phones and many different platforms.

WP7 no longer uses ActiveSync/WMDC to synchronise with the PC, but using Zune. Since most mobile forensic tools require ActiveSync/WMDC to extract data from the WM phone, there is a possibility that the tools designed for WM will not work on WP7. Testing of these tools to acquire data from a WP7 phone will be performed to see how these tools cope with WP7.

The research used a selection of mobile forensic tools to test the compatibility of the tools with WP7. The tools selected were discussed in the Guidelines on Cell Phone Forensics from NIST (Jansen & Ayers, 2007), Cell Phone Forensic Tools: An Overview and Analysis from NIST (Ayers et al., 2005), or have been used in previous published studies on WM forensics (see Section 3.1). The tools selected were based on availability at the time of the research. Table 2.6 shows a summary of the tools.

Forensic Tool	Manufacturer	Version	WP7 Compatible	Notes
Device Seizure	Paraben	4.6.4374.35749	No	Trial
Encase	Guidance Software	7.01.01	No	Academic Training
MOBILedit! Forensic	Compelson Labs	6.0.0.1397	No	Trial
XRY Complete	Micro Systemation	6.0.1	Yes (Logical files only)	Full Version
Oxygen PM	Oxygen Software	2012 3.7.0.1	No	Trial
Secure View	Susteen Inc	3.4.0T	No	Trial
FTK	AccessData	1.81.6b10.04.02	No	Trial
Foremost	Open Source	1.5.7	No	Open Source
Scalpel	Open Source	1.60	No	Open Source
Phone Image Carver	GetData	1.2.8.52	No	Trial

Table 2.6: Summary of Mobile Forensic Tools

The tools TULP2G (Netherlands Forensic Institute, 2007) and ITSUTILS (Hengeveld, 2010b) were available for testing, but were not be tested as part of the research. TULP2G has not been updated since March 2007. The TULP2G website says

> "Current TULP2G plug-ins don't contain state of the art technology for the examination of mobile phones. Most plug-ins were made years ago to demonstrate framework principles. Nowadays a lot of better (commercial and open source) tools exist to assist you in the examination of mobile phones." (Netherlands Forensic Institute, 2007).

ITSUTILS will not be tested because the author noted on the website

> "i am waiting until i get my hands on a wm7 phone, on which i don't expect itsutils to work without major modifications" (Hengeveld, 2010b).

2.5 SUMMARY OF ISSUES AND PROBLEM AREAS

The literature reviewed on WM forensics established the current tools and techniques used on a WM phone during a forensic investigation, and what data can be extracted from the WM phone. The literature reviewed on WP7 identified the many changes made to WP7 compared with WM. How the changes to WP7 will affect the WM forensic tools and techniques and what data can be extracted from a WP7 phone using the WM forensic tools and techniques are unknown.

One of the changes likely to impact a digital forensic investigation is the way in which WP7 synchronises with the PC. WM forensic tools performing both logical and physical acquisitions rely on the ActiveSync/WMDC connection between the WM phone and the PC to acquire data. Because WP7 uses Zune rather than ActiveSync/WMDC, the WM forensic tools and techniques may be unable to communicate with the WP7 phone, and may be unable to acquire data from the WP7 phone. Should some of the WM forensic tools be able to communicate with the WP7 using the Zune connection, the WM forensic tools may still not be able to perform physical acquisition from the WP7 phone. WM forensic tools copy an agent onto the WM phone, and the agent dumps the data from the WM phone's memory to the WM forensic tool. Because WP7 cannot run

any WM applications, even if the agent was successfully copied onto the WP7 phone, the agent may not run and hence may not be able to dump data to the WM forensic tool.

Other changes which may impact a digital forensic investigation are the changes to the WP7 file system. WP7 uses the phone's memory and the internal SD card together to create a single storage area. Physical acquisition methods such as JTAG and chip extraction may be able to acquire a physical dump of the WP7 phone's memory, but because the data on the internal SD card is not acquired, the physical dump acquired may be missing important data. Exactly how the files are spread between the phone's memory and the internal SD card is not known, but the internal SD card on WP7 is encrypted, and cannot be acquired using standard forensic methods of acquiring memory cards.

The file system used by WP7 and the compression used by WP7 are both different to the file system and compression used on WM. WP7 uses the TexFAT file system and the XPH compression, whereas WM uses the TFAT file system and the XPR compression. The impact of the new file system and compression used on WP7 on WM forensic tools and techniques are unknown. Should a complete physical dump of the WP7 phone be acquired, the WM forensic tools and techniques may not recognise the file system and/or unable to decompress the file, both of which are required to analyse the dump file.

WP7 phones can be an exceptional source of evidence, even more so than WM phones due the larger storage and better capabilities such GPS location and integration with online services such as Facebook and Hotmail. WP7 is predicted to be the second most popular types of smart phones in the world by 2015, more popular than the iPhone from Apple. With so much potential evidence stored on WP7 phones and the possible popularity of WP7 phones, the is a need to extract data from WP7 phones. At the time of writing, no published studies were found on testing for compatibility of current WM forensic tools and techniques on WP7 phones.

2.6 LATEST DEVELOPMENT IN WINDOWS PHONE 7

Due to the fast changing nature of the smart phone market, and because WP7 is still a new product, the platform will likely to go through many changes and

updates throughout the research. Section 2.6 discusses some of the latest developments with WP7, including both official updates from MS and hardware vendors, as well as unofficial updates which users of WP7 have put together.

In January 2011 Julien Schapman released the first public best version of Registry Editor for WP7 (Schapman, 2011a), and Windows Phone Device Manager (WPDM) and TouchXperience (TS) (Schapman, 2011b; XDA Developers, 2011a). Registry Editor is an application which runs on the WP7 phone and allows searching, creating, editing, and deleting of registry keys and values. Registry Editor was only tested on HTC phones, and not known if the application will work with any other brands of phones. No details were given of how to install the application on the WP7 phone. WPDM and TX is a client/server type of setup where WPDM runs on the PC and TX runs on the WP7 phone. WPDM is able to view files on the WP7 in a similar way to Windows Explorer can view files on the computer. WPDM allows the user to view, copy, and modify files on the WP7 phone, backup and restore the WP7 phone.

In March 2011 MS started rolling out the update for WP7 codenamed 'NoDo' to WP7 devices. The update name was Windows Phone Update – March 2011. The update included some fixes and improvements, as well as adding the Copy and Paste function which was missing from WP7 (Microsoft, n.d.-g).

In April 2011 The Dark Forces Team (DFT) managed get a WP7 phone, the HTC HD7 to run Android (Peters, 2011). DFT were responsible for many famous hacks on other phones including getting WP7 and Android working on HTC HD2 which was designed to run WM (XDA Developers, 2011c). Although not directly relate to the research, getting another OS to run on a WP7 phone demonstrates that the hardware layer of the HD7 is similar enough to other HTC devices that the software could be modified to run Android. The actual Android ROM for the HD7 was still being tested and has not been released by DFT yet, and there is no indication on when it will be released.

In May 2011 a developer on the XDA-Developers forum created an application to allow backup and restore of WP7 phones using Zune (XDA Developers, 2011d). The application works by exploiting the built in WP7 tool to update the phone called updatewp.exe. Updatewp.exe is designed to update WP7, but also allows backup and restore of phone. The application runs updatewp.exe to either backup or restore the WP7 phone, then terminates updatewp.exe before

any updating of the phone is done. Also in May 2011 another XDA-Developers user used WPDM to successfully extract SMS messages from a WP7 phone (XDA Developers, 2011b). The process involves using WPDM to copy the file store.vol from the WP7 phone to the PC. Once on the PC a custom perl script was use to decode the store.vol file for SMS messages.

Also in May 2011 MS announced a new update to WP7 codenamed Mango (Microsoft, n.d.-g). The Mango update was released in September which updated WP7 to WP7.5, and added some 500 feature improvements. Due to time constraints, the research was conducted on WP7, and not the newly updated WP7.5.

2.7 CONCLUSION

In Chapter 2 some digital forensic models and guidelines from NIST and ACPO were reviewed to establish the accepted methods and procedures for conducting a digital forensic investigation to produce forensically sound evidence. A brief history of WM phones and how the redesign of WM phone became WP7 were reviewed to establish the major changes made to WP7. Some recent published studies on WM phone forensics were reviewed to establish where potential evidence may be stored on a WM phone, and the different tools and techniques used to extract potential evidence from a WM phone from both a logical and physical acquisition.

With the major changes made to WP7, and the fact there is no compatibility between WP7 and any previous WM OS, the current tools and techniques used for a WM phone during a forensic investigation may not be suitable for use for a WP7 phone. Many of the mechanisms needed in order to perform a forensic investigation on a WM phone has either changed or is not available in WP7. So far no published literature on testing or survey of tools for WP7 have been found.

Chapter 3 will define the research methodology which will be used to conduct the experiments including the review of similar published studies, the research question and hypothesis, the research design, and the limitations of the research.

Chapter Three
Methodology

3.0 INTRODUCTION

Chapter 2 reviewed the literature relating to mobile digital forensic investigation, Windows Mobile (WM) phones, Windows Phone 7 (WP7) phones, and WM phone forensics. The literature established the current forensic tools and techniques used on a WM phone during a forensic investigation. Literature on WP7 was reviewed which illustrated the major changes made to WP7 compared to WM, including some components which may be critical for a forensic investigation. Chapter 3 will outline a research methodology for the research and will formulate the research question, the sub questions, the associated hypotheses, and define the specifications for the experiments.

What data can be forensically extracted from a WP7 using current tools and techniques used on WM phones will be tested through a series of experiments. Test data (based on data from previous studies) will be loaded onto a WP7 phone and experiments using forensic tools and techniques used on previous studies will be conducted to extract the test data. The data extracted from the WP7 phone will be compared to the data extracted from a WM phone from previous studies.

The research methodology will be based on the applying scientific method in digital investigations (Casey, 2011). The experiments will be largely based on previous studies which are reviewed in Section 3.1. The research questions and hypotheses are discussed in Section 3.2. The research design which includes the test equipment specification, test data specification, experimental procedures are discussed in Section 3.2. The limitations of the research are discussed in Section 3.5, followed by the conclusion in Section 3.6.

3.1 REVIEW OF SIMILAR PUBLISHED STUDIES

Section 3.1 reviews selected similar published studies in order to establish the current forensic tools and techniques used to extract data from WM phones. The reviews will focus on what forensic tools were used, what forensic techniques were used, how the forensic tools and techniques were applied to WM, and what data can be extracted from the WM phone. The forensic tools and techniques and

extracted data will be used to form the methodology and experiments of the research.

3.1.1 Introduction To Windows Mobile Forensics

Introduction to Windows Mobile Forensics by Casey et al. (2010) provides a general overview to WM forensics and where potential evidence may be stored. Potential evidence on WM may be stored on the phone as a file, in an embedded database, in the registry, or may have been deleted.

The experiments in the article were conducted on three different phones, an HTC S620 running WM6, a Motorola Q running WM5, and a Samsung i607 running WM5. The tools XACT (a commercial tool) and ITSUTILS (an open source tool) were used to acquire an image of the Motorola Q. XACT can load an agent (application) on the WM phone which dumps data from the WM phone's memory to the PC, whereas ITSUTILS can read storage areas on the phone's memory. Both XACT and ITSUTILS require ActiveSync to be installed on the PC in order to perform the acquisitions.

After acquiring data from the WM phone, the embedded databases were analysed starting with cemail.vol. cemail.vol contains messages (email, SMS, MMS) stored across multiple embedded databases within cemail.vol. Casey et al. (2010) explained each of the embedded databases within cemail.vol and the relationships between the databases. Custom forensic tools were developed by the authors to interpret some information in the cemail.vol file. XACT was used to show data in cemail.vol acquired from the Samsung i607 phone, in both the raw format (hex or ASCII) and as messages. The raw and processed views of cemail.vol on XACT showed that the actual text within the messages were stored as plain text (ASCII), so forensic examiners could use a hexviewer to look for text to find deleted messages.

In order to verify the data in cemail.vol, Casey et al. (2010) copied the cemail.vol acquired from the WM phone to a WM emulator replacing the generic cemail.vol of the emulator. The cemail.vol file on the WM emulator was locked so can't be replaced easily, so a workaround had to be used. Once the cemail.vol file has been replaced, the messages can be viewed on the emulator in the same way messages can be viewed on a WM phone.

Casey et al. (2010) then used the Microsoft (MS) Remote Registry Editor (a tool from Microsoft to allow developers to edit and manage the registry on a WM phone) to view the registry of the Samsung i607. The registry of WM is similar in format to the registry of the Windows Operating System (OS) for PCs. Although no specific data was extracted or examined from the registry, examples of useful keys in the registry where potential evidence may be stored were given.

Casey et al. (2010) continued to examine messages, in particular emails and MMS messages. While messages and information such as sender, date and similar are stored in cemail.vol, artefacts are created by WM when an email or MMS message is opened or sent. The artefacts include data such as images and other attachments sent with the message. The artefacts may remain even after the original message is deleted. XACT was used to examine the artefacts and how to match artefacts with the original message in cemail.vol was demonstrated.

Finally Casey et al. (2010) offered a case study where eavesdropping apps such as MobileSpy (Mobile Spy, 2011) and FlexiSpy (FlexiSPY, 2011) may be installed on the WM phone. The apps log the activities of the phone such as voice calls and messages and allows a user to view the logs remotely via the internet. Normally the apps do not show as running on the WM phone so the user is unaware and unable to detect the presence of the apps. The authors explained that investigators may be able to find traces of the apps by looking in the registry.

3.1.2 Windows Mobile Advanced Forensics: An Alternative To Existing Tools

Windows Mobile Advanced Forensics: An Alternative To Existing Tools by Rehault (2010) demonstrated an uncommon method to perform a physical acquisition (known as a dump) of the WM phone using the bootloader. As discussed in Chapter 2, the bootloader contains the first pieces of code which is executed when the phone is turned on. The bootloader performs initial checks, usually on the hardware before loading the OS. The bootloader can also used to perform updates on the phone. With WM phones made by HTC (HTC, 2011a), the bootloader also may also contain commands designed for diagnostics and maintenance. The author was able exploit the commands contained in the bootloader to take a physical dump of the phone's memory and analysed the dump file to extract data from the WM phone.

Rehault (2010) originally used a program called mtty.exe which was a terminal application developed by HTC to communicate with the bootloader. Once the phone was put into bootloader mode, a serial connection was made with the PC using the USB port. However, due to errors using mtty.exe, the author wrote a custom program called ComTTY which was designed and used to perform the physical acquisition of the phone.

Once the physical dump was acquired, Rehault (2010) reconstructed the file system by creating a custom python script called dissect.py. Four partitions were present in the dump, and all the user data was stored in the last partition which was a TFAT partition. Rehault (2010) noted that once the TFAT partition was reconstructed, forensic tools such as Encase, FTK, and other file carvers can read the TFAT partition.

A tool from MS called d_readvol.exe (Microsoft, 2006) was used to extract registry keys from the dump. The relevant registry keys in both the system registry and the user registry where potential evidence may be stored were outlined.

Using knowledge about how WM stores messages from previous studies (one of which was reviewed in Section 3.1.1), Rehault (2010) wrote a python scripted called MsgCarving.py to reconstruct the messages contained in cemail.vol. Compression was dealt with using a custom tool called comp.dll.

The bootloader method was used on a newer phone, the HTC HD2 running WM6.5 and was successful in acquiring a physical dump from the phone. However the bootloader method "cannot be applied to other branded/model of smartphones". The author also noted "the methods and tools described in the article might be relevant for every Windows CE (WM) operating system, this may change with the next version of Windows CE" (Rehault, 2010).

3.1.3 Windows Mobile Advanced Forensics

Typically, a WM forensic investigation is conducted using forensic tools which acquires data from the WM phone logically. Windows Mobile Advanced Forensics (Klaver, 2010) discusses more advanced methods of dealing with WM forensics beyond logical acquisition using tools.

Klaver (2010) discusses the typical WM hardware components such as RAM and ROM, and typical software components such as the bootloader, file

system, and databases. Different methods of physical acquisitions (chip extraction, JTAG, and bootloader) (discussed in Section 3.1.4) were also discussed. Tools such as XACT and ITSUTILS which are able to acquire a physical image of the WM phone without using the typical physical acquisitions methods such as JTAG or chip extraction are referred to as pseudo physical acquisitions by Klaver (2010).

ITSUTILS was used to acquire a physical dump of the WM phone. An agent is copied onto the WM phone allowing ITSUTILS to communicate with the WM phone via the ActiveSync connection to acquire the physical image.

The physical dump file could be thought of as a container, inside which are more containers, inside which may be more containers as illustrated in Figure 3.1. The physical dump contains partitions, which can be thought of as drives. Establishing the file system used in the phone's memory allows the partitions to be reconstructed. Some partitions may also be compressed, and so the compression used has to be known in order to reconstruct the compressed partitions. Once the partitions are reconstructed, each partition can be examined to see what file system is used. Once the file system for each partition is established, then the files inside each partition can be reconstructed. Some of these files are databases, and some potential evidence are contained in the databases, and so the databases have to be decoded to find the potential evidence.

Klaver (2010) manually reconstructed the physical dump file by writing custom tools in a similar manner to Rehault (2010) discussed in Section 3.1.2. The custom tool were created and used by Klaver (2010) to decode cemail.vol in order to extract messages, and to find deleted messages.

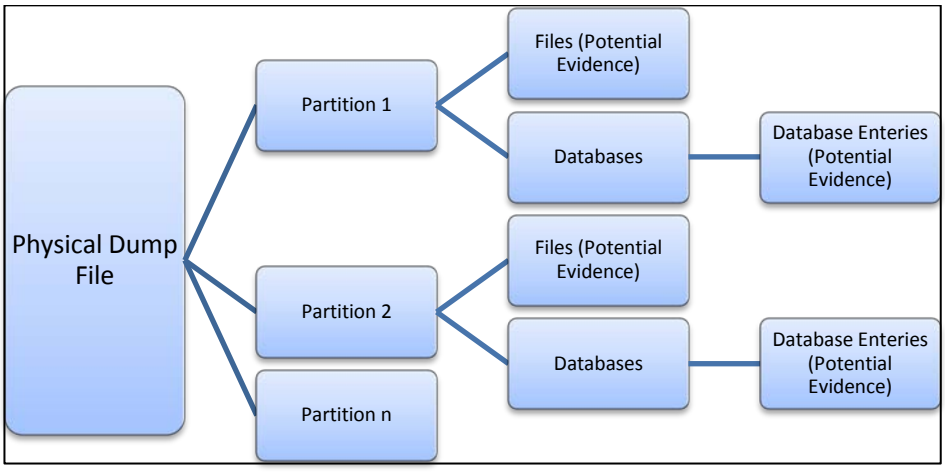


Figure 3.1: Dump file analysis

3.1.4 Forensic Data Acquisition From Cell Phones Using JTAG Interface

The article Forensic Data Acquisition From Cell Phones Using JTAG Interface by Kim, Hong, & Ryu (2008) gives an overview of the different acquisition methods which can used on a mobile phone: logical (what the authors called software), JTAG, and physical chip extraction. Kim et al. (2008) explains that most tools for mobile phone forensics perform logical acquisition, and while using tools is an easy and convenient method of acquiring data, the data acquired may not be as forensically sound as other methods. The chip extraction is the "ideal forensic data acquisition method" Kim et al. (2008), but there are difficulties in removing the memory chip the phone, then reapplying the chip to another device which can communicate with the chip. Due to the difficulties of removing the chip from the board, and having the correct equipment to communicate with the chip, Kim et al. (2008) suggested "Therefore, it is desirable to apply this method when JTAG and software approach are not available". The JTAG method provides a more complete forensic image (dump) compared to the logical method, and without the risks involved with removing the memory chip compared to the chip extraction method as shown in Figure 3.2.

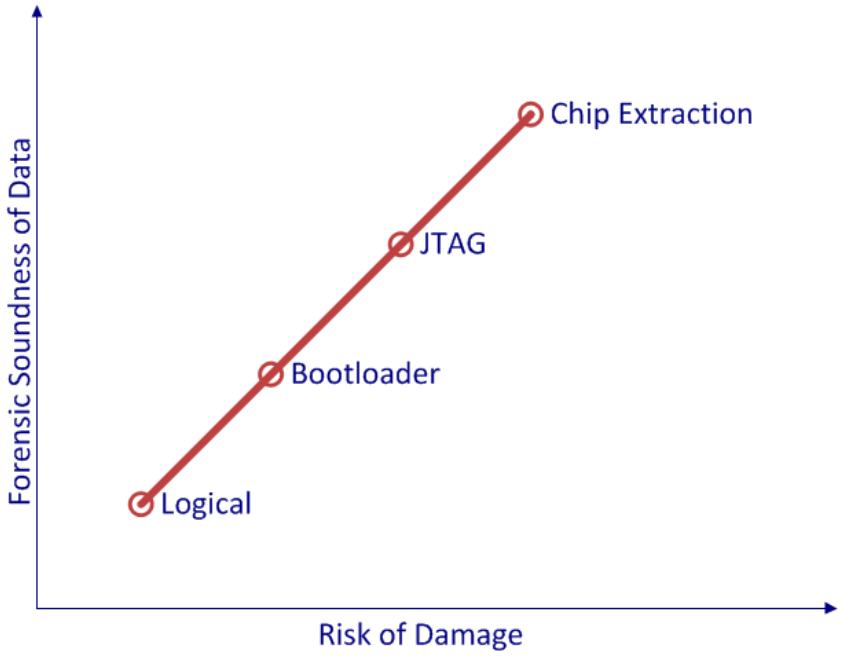


Figure 3.2: Risk of Data Acquisition Methods

The Joint Test Action Group or JTAG is a standard for testing and debugging circuit boards. JTAG test points are different between different phones, a procedure to find the JTAG test points was outlined. Kim et al. (2008) used a

phone (target phone), a JTAG debugger, and forensic software (which forensic software was not mentioned) to acquire a JTAG acquisition. First the JTAG points on the Printed Circuit Board (PCB) of the target phone had to be found. Exactly how to find each test point on a given phone was not described in the article. Next the JTAG debugger was set up with suitable settings for the specific chipset used on the target phone. Once the JTAG debugger was set up with the correct settings, the reference voltage coming out of the target phone was put into the JTAG debugger to check if the debugger was receiving the signal. When JTAG points were found, JTAG debugger set up correctly, and signals between the target phone and debugger were working correctly, a physical dump of the target phone's memory can be acquired.

The physical dump from the target was not analysed or reconstructed as the article's focus was on the JTAG acquisition. Kim et al. (2008) explained the difficulty of reconstructing the physical dump "since each phone manufacturer has its own file structure and each phone model of the same maker has different data structure". Kim et al. (2008) concluded "The next obvious step is to focus on data interpretation of the acquired raw digital data. This remains a possibility for future work".

3.1.5 A Comparison Of Forensic Evidence Recovery Techniques For A Windows Mobile Smart Phone

The recent article A Comparison Of Forensic Evidence Recovery Techniques For A Windows Mobile Smart Phone by Grispos, Storer, & Glisson (2011) compares the methods of acquisitions and the tools used on WM phones. Test data was loaded onto a WM phone, and a series of tools (both for logical and physical acquisitions) were used to extract the test data from the WM phone.

Test data such as pictures, messages, and documents was loaded onto a WM phone, then used a tool from Cellebrite called Universal Forensic Extraction Device Physical Pro (UFED) (Cellebrite, 2011) was used to firstly acquire a physical acquisition, then a logical acquisition of the WM phone. After acquiring the logical acquisition UFED was used to analyse the logical acquisition (logical result set). The WM phone was also manually examined using the User Interface (UI) of the phone as a normal user would (manual result set). The physical dump was then analysed using a series of tools listed in Table 3.1 (physical result set).

The logical result set, the manual result set, and the physical result set where then compared.

Grispos et al. (2011) stated "different acquisition tools and methods recover different subsets of data from memory", and according to Moore (2006) (as cited by Grispos et al. (2011)) " there is no standard format of accumulating information in a mobile phone or standard file system".

Tool	Version	Web Page
Physical Analyzer	1.1.3.8	http://www.cellebrite.com/forensicproducts/ufed-physical-pro.html
WinHex Forensic Edition	15.4 SR-5	http://www.x-ways.net/winhex/index-m.html
Forensic Toolkit	3.0.1.2052	http://accessdata.com/products/forensic-investigation/ftk
Encase	6.13.0.43	http://guidancesoftware.com/
Foremost	1.5.7	http://foremost.sourceforge.net/
Scalpel	1.60	http://www.digitalforensicssolutions.com/Scalpel/
Simple File Carver	1.6	http://www.simplecarver.com/
Phone Image Carver	1.2.8.52	http://www.phoneimagecarver.com/

Table 3.1: Tools Used by Grispos et al (2011)

3.2 RESEARCH QUESTION AND HYPOTHESIS

Section 3.2 will derive the research question and hypothesis for the research. A review of previous similar studies will be discussed to establish the current landscape of WM forensics. Issues and problem areas relating to WM forensics (namely WP7 forensics) will be evaluated, and the research question and hypothesis will be formed based on the problem areas identified.

3.2.1 Review of Similar Studies

The studies reviewed in Section 3.1 are a selection of literature about the current forensic tools and techniques used in WM forensics, and were used in order to formulate the research question and the hypothesis. The studies reviewed shows there are many ways of acquiring data from WM, and many tools and methods to analyse the data. Even with the different forensic tools and techniques for WM acquisition and analysis, there is no single method which captures all the data on the WM phone.

The previous studies done on WM phones can be broadly divided into two categories - logical acquisition and analysis, and physical acquisition and analysis. Generally Physical acquisition and analysis can extract more information than logical acquisition and analysis, but there is a higher risk of damaging the phone. Logical acquisitions and analysis are usually done by a single tool, usually a software packages designed to aid the investigator through the forensic process. These tools are usually able to acquire the data, analyse the data, and have powerful reporting capabilities. Physical acquisitions and analysis can also be done using a single tool such as XRY in the same manner that a logical acquisitions and analysis is done. Physical acquisitions can also be done using other methods such as JTAG or chip extraction, and analysis of the physical dump can be done using different tools or manually analysed.

The article by Casey et al. (2010) reviewed in Section 3.1.1 provides information about the WM OS and file locations, identifying where potential data can be found. WM has a similar structure to the Windows desktop OS with location of files being in similar locations, and the registry being similar in structure. However WM also contains embedded databases which may contain potential evidence. Casey et al. (2010) performed acquisitions using XACT (both logical and physical) and ITSUTIL (physical only). Analysis of both the logical and physical acquisitions were done using XACT, as well as customs tools written by the authors wrote in order to decode the physical dump and embedded databases which XACT was not able to fully analyse.

Rehault (2010) reviewed in Section 3.1.2 used the bootloader method to acquire a physical dump of a WM phone. The Bootloader used in the article allows the phone to communicate with a PC using serial communications (via the USB), and a custom tool written by the author was used to acquire the physical dump. Analysis of the dump was done using customs tools written by the author in a similar way to Casey et al (2010). Using the custom tools Rehault (2010) was able to reconstruct the dump file and extract potential evidence from the dump.

The bootloader method is little used in WM forensics since bootloaders on WM phones vary from manufacturer to manufacturer. The bootloader method also requires the bootloader of the phone to be able to read the contents of the memory on the phone and output the contents through the serial connection, which not all bootloaders will do. The WM phone used in the article was a TyTn II made by

HTC running WM 6. Rehault (2010) did the experiment on a later model phone, the HD2 also by HTC running WM 6.5. With some modifications, the author was able to acquire a physical dump from the HD2. "However, this method cannot be applied to other brand/model of smartphones" (Rehault, 2010). HTC announced that the bootloader for many HTC phones will be unlocked because

> "HTC was overwhelmed by the enthusiasm of our fans for the possibilities of developing software for HTC devices. HTC has a strong commitment to our developers and, in line with the launch of HTCdev.com and the OpenSense SDK, we felt it was important to fully enable developer success and unlock the bootloaders on our devices" (HTC, 2011b).

Unlocking the bootloader will allow developers to customise the bootloader allowing functions such as a physical acquisition. Once again, the unlocked bootloader is only applicable to HTC phones, and only some 2011 model HTC phones will support the unlocking of the bootloader. The WP7 used for the research (HD7) was not listed as a supported device for unlocking of the bootloader at the time of research.

The article by Klaver (2010) reviewed in Section 3.1.3 provides an overview the WM hardware, the different acquisition techniques, and how to rebuild a dump file. The article discusses JTAG and chip extraction as methods of physical acquisition of WM phones. Klaver (2010) also used XACT and ITSUTILS like Casey et al (2010), for logical analysis and used custom tools to do physical analysis like. While Casey et al (2010). focused on logical acquisitions and analysis, and Rehault (2010) focused on physical acquisition and analysis, Klaver's (2010) article focused on both.

Kim et al. (2008) reviewed in Section 3.1.4 gives an overview of the different methods of data acquisition from mobile phones and the risk and benefits of each. Logical acquisitions are not as forensically sound as physical acquisitions. Of the physical acquisition methods, the bootloader is the least forensically sound and works with a very limited number of phones. The chip extraction method is the most forensically sound but is also the most difficult and requires specialist hardware. The article focused on the JTAG method of data acquisition which is applicable to most modern phones and although not as forensically sound as chip extraction has much less risk of damaging the phone. The article applied to

modern phones in general, and not specific to WM phones. The article describes process of finding JTAG test points in order to acquire a physical dump of the phone as the test points varies from phone to phone. The article does not describe how to analyse and rebuild the dump as the process will vary from phone to phone.

Grispos et al. (2011) reviewed in Section 3.1.5 evaluated the effectiveness of different tools and techniques of extracting potential evidence on a WM phone. Test data was put on the WM phone and both a logical and physical acquisition was made of the phone using UFED. UFED was also used to analyse the logical acquisition while eight other tools were used to analyse the physical acquisition. The results of logical and physical analysis were compared. No single tool or technique was able to extract all the test data. Grispos et al. (2011) focused on using tools to analyse the physical dump, and did not manually analyse the physical dump .Grispos et al. (2011) concluded as part of the future work

> "Since this work was conducted and submitted for review, version 7 of the Windows Mobile operating system has been released. New research is now required to investigate the effectiveness of mobile forensics tools on this new platform. The design of the test set presented here provides a basis for future comparisons and evaluation"

The studies by Casey et al. (2010), Rehault (2010), and Klaver (2010) suggests that analysis of a logical acquisition can be done using commercially available tools, whereas analysis of physical acquisition usually require custom tools to manual rebuild the dump file. The study by Grispos et al. (2011) used eight different tools to analyse the dump file rather than manually analysing the dump file. The study by Kim et al. (2008) describes the different methods of data acquisition from mobile phones and focused on the JTAG method. Kim et al. (2008) describes the process to find the appropriate JTAG test points in order to perform a physical acquisition from a mobile phone. The JTAG method of physical acquisition is applicable to most modern mobile phones.

3.2.2 Review of Issues and Problem Areas

Section 3.2.2 reviews the issues and problems identified in Chapter 2 and together with the reviews of similar studies discussed in Section 3.1 will help select the research question and hypothesis for the research.

3.2.2.1 Synchronisation

WM uses either ActiveSync or WMDC (depending on which version of Windows) to synchronise data between the phone and the PC, usually via USB (hereto referred to as sync mechanism). Most forensic tools use the sync mechanism to perform acquisitions from the phone. Tools like XRY perform both a logical and physical acquisition using the sync mechanism. The bootloader method and ITSUTILS both use the sync mechanism to perform physical acquisitions.

WP7 does not use ActiveSync or WMDC (discussed in Chapter 2) to synchronise data with the PC. WP7 uses Zune as the sync mechanism, and the data presented to the PC is different to that of WM. When WM is synced with the PC, the PC is able to see the WM system and user files, contacts, calendar, and many other files. When WP7 is synced with the PC, the PC is unable to see any files on WP7. With Zune, the PC is able to see the user's media files such as music and videos.

The change in the sync mechanism from WM to WP7 may cause tools which rely on ActiveSync/WMDC to be unable to communicate with WP7 and therefore unable to perform logical and physical acquisitions.

3.2.2.2 File System Changes

The file system of WM has been well documented in previous studies, and the location of where potential evidence may be stored and how to extract the potential evidence has also been well documented. Most forensic tools are able to analyse the data acquired from WM, and an investigators are able to manually analyse data acquired from WM because the file system, location of data, and the structure of the embedded databases are known.

The file system changes implemented in WP7 means WP7 uses a different file system to WM, the compression used in WP7 is different to WM, and the way the files are stored on WP7 is also different to WM. The file system used by WP7 is TexFAT rather than TFAT used by WM. The compression used in WP7 is XPH rather than XPR used in WM. WP7 also spreads the files between the phone's memory and the internal SD card whereas WM stores all the files on the phone's memory alone. The location of data and the structure of the embedded databases in WP7 are also unknown. The file system changes to WP7 could affect the ability of forensic tools to analyse data from WP7 as the forensic tools may not be able to

interpret TexFAT or XPH. The file system changes could also make manually reconstructing a WP7 dump file difficult as customs tools used to reconstruct WM dump files were written to interpret TexFAT and XPR. The spreading of the files between the phone's memory and the internal SD card by WP7 could mean that manual reconstruction of a WP7 dump file may not be possible as part of the data required may be stored on the internal SD card which is encrypted.

3.2.3 Research Question

As reviewed in Section 3.2.1 there are established tools and techniques for acquiring and analysis WM phones. However as reviewed in Section 3.2.2, there has been changes made to WP7 which may prevent the established tools and techniques to acquire or analyse data from WP7. Hence, the main research question for the research is:

> (Q0) What forensic data can be extracted from a WP7 phone using current tools and techniques used to extract forensic data from WM phones?

The above research question can be broken down into the following sub questions:

> (Q1) Are current forensic tools and techniques used for logical acquisitions of WM capable of logical acquisitions of WP7 phones?
>
> (Q2) What forensic data can be extracted from a WP7 phone using logical analysis tools and techniques currently used for WM phones.
>
> (Q3) Are current tools and techniques used for a physical acquisitions of WM phones capable of physical acquisitions of WP7 phones?
>
> (Q4) What forensic data can be extracted from a WP7 phone using physical analysis tools and techniques currently used for WM phones.

3.2.4 Hypothesis

WP7 has many changes since the previous version of WM. The most significant changes for a forensics investigator are the sync mechanism changes discussed in Section 3.2.2.1 and the file system changes discusses in Section 3.2.2.2. Based on these changes the hypothesis for the research is:

(H0): The current tools and techniques used to extract forensic data from WM phones are not capable of extracting forensic data from WP7 phones.

The above hypothesis can be broken down into the following sub hypotheses:

(H1): The current forensic tools and techniques used for logical acquisitions of WM are not capable of logical acquisitions of WP7 phones.

(H2): The current forensic tools and techniques used for analysis of logical acquisitions of WM phones are not capable of analysis of logical acquisitions of WP7 phones.

(H3): The current tools and techniques used for a physical acquisitions of WM phones are not capable of physical acquisitions of WP7 phones.

(H4): The current tools and techniques used for analysis of physical acquisitions of WM phones are not capable of analysis of physical acquisitions of WP7 phones.

3.3 RESEARCH DESIGN

Section 3.3 discusses the research which will be undertaken in order to answer the research questions and test the hypotheses. The scientific method will utilised in the research to test the hypotheses. The forensic process and changes to WP7 will be incorporated into the research. The research methodology was largely based on the methodology used by Grispos et al. (2011) where test data was loaded onto a phone, and a series of forensic tools were techniques were used to extract the data. Rather than comparing the data extracted by each tool with the results extracted

by other tools, the research will comparing the data extracted from a WP7 phone with the data extracted by the same tool on a WM phone.

3.3.1 The Scientific Method

To test if the current forensic tools and techniques used on WM phones will work on WP7 phones, experiments will be conducted on a WP7 phone using some of the forensic tools and techniques used in the previous studies to test what data can be extracted from the WP7 phone. The experiments will be conducted using the scientific method in digital investigations (Casey, 2011). The scientific method can have many different variations and implementations. For the research, the following method will be used: - A hypothesis is formed based on the gathered information and resources, experiments are performed, data is collected, and the data is analysed to see if the hypothesis was right or not. The process can be an iterative process depending on the results as shown in Figure 3.3.

The hypothesis, and the derived sub hypotheses have been discussed in Section 3.2. The procedures/experiments on WP7 will be formed and discussed Chapter 4 of the research. The results from the experiments will be compared to the results from experiments done in previous studies on WM to test the hypothesis.

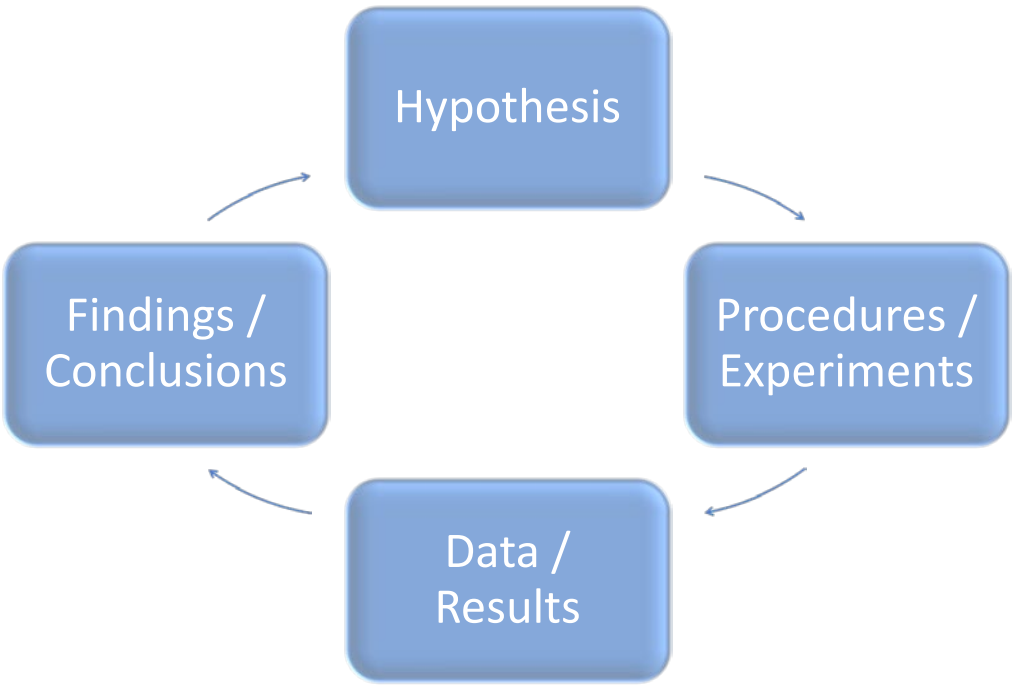


Figure 3.3: The Scientific Method

3.3.2 The Forensic Process

As discussed in the Chapter 2 the forensic process is a model to aid organisations implement their forensic procedures to suit their requirements. The forensic process is designed to ensure data extracted is forensically sound, meaning the method of data extraction is reliable, verifiable, and repeatable. The forensic process has four stages- Collection, Examination, Analysis, and Reporting. Some of the procedures used during the forensic process for WM phones is applicable to WP7 phones, while some may not be as shown in Figure 3.4.

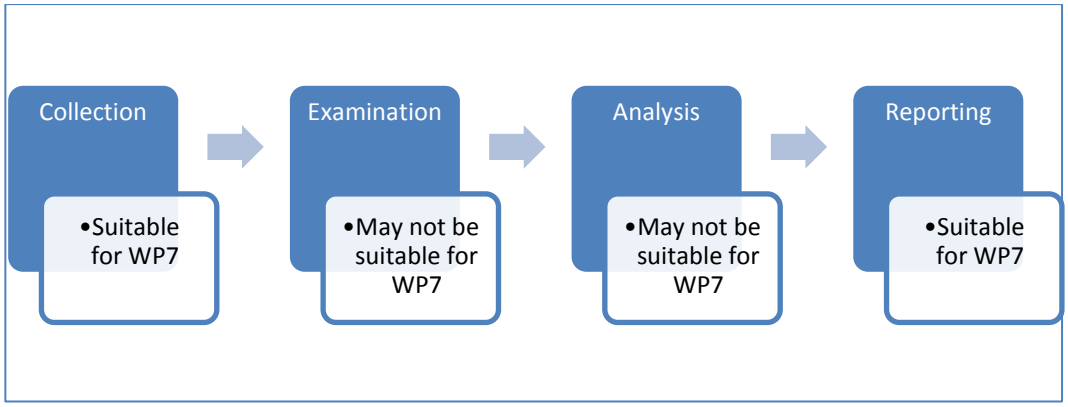


Figure 3.4: The Forensic Process for Windows Phone 7

The Collection stage is where the item (a WM or WP7 phone) is physically collected and secured. A WM phone and a WP7 phone are similar in physical size and connections (USB, Wi-Fi, Bluetooth). Procedures currently used to collect and secure a WM phone to ensure forensically sound recovered data is applicable to a WP7 phone.

The Examination stage is where data is acquired from the item (a WM or WP7 phone). Because of the changes to the WP7 sync mechanism, file system, and lack of backwards compatibility with WM (discussed in Section 3.2.2), the procedures currently used to acquire data from a WM phone may be suitable for acquiring data from a WP7.

The Analysis stage is where the data acquire from the phone is analysed to find relevant information which may be used as evidence for an investigation. Because of the changes to WP7 file system (discussed in Section 3.2.2.2) the procedure currently used to analyse data from a WM phone may not be suitable for analysing data from a WP7 phone.

The Reporting stage is where the entire process is documented to ensure the forensic investigation is verifiable and repeatable. Even though the reporting is shown in the process model diagram as a separate stage at the end, the reporting covers the all stages of the forensic process. The procedures currently used to document the forensic process of a WM phone investigation is applicable to a WP7 phone.

Based on the changes made to WP7, the procedures used in the collection and reporting stages of the forensic process on a WM is applicable to WP7. The procedures used in the examination and analysis stages of the forensic process on a WM may not be applicable to WP7. Hence the research will be focused on the examination and analysis stages of the forensic process.

3.3.3 New Features of WP7

While WP7 added many new features and have changed many features of WM, the majority of the changes has not affected the types of data normally extracted in a forensic investigation, such as call log and contacts. Two new features, which were available in some later high end models of WM phones come standard with all WP7 phones - Internet Explorer (IE), and Global Position System (GSP) capabilities.

Every WP7 phone comes with IE as the default web browser (although the user is able to install other browsers). WP7 has a powerful processor, powerful graphics capabilities, and is tightly integrated with MS's LIVE (cloud) services. The information stored in IE may be as valuable as that stored in IE on a PC.

Every WP7 phone has a built in GPS which can be used for navigation, as well as location services. The GPS allows for a few extra features to be integrated into the phone. Two of these features may contain information relevant to a forensic investigation. The first is Geo-tagging, where the location of the phone (the GPS co ordinates) are added to the photo taken. The exact location of where the photo is taken can be identified using the GSP co-ordinates. The second is satellite navigation (sat nav). Many forensic tools can extract data from sat nav devices such as Tom Tom, which may contain addresses and locations where the user has been.

3.3.4 Research Phases

The research consists of five phases as shown in Figure 3.5. Phase One uses the previous studies discussed in Section 3.1 to establish the current WM forensic tools, the current WM forensic techniques, and what data can be extracted from WM (WM data).

Phase Two uses the WM data established in Phase One as a template to generate test data for the WP7 phone. The test data will also be generated based on new features of WP7 discussed in Section 3.3.3. Phase Three applies the WM forensic tools and techniques to the WP7 phone to extract the test data from the WP7 phone. Phase Four compares the data extracted from the WP7 phone using the WM forensic tools and techniques with the data extracted from a WM phone using the same WM forensic tools and techniques. Phase Five will analyse the results of Phase Four to evaluate the compatibility of WM forensic tools and techniques on WP7 phones.

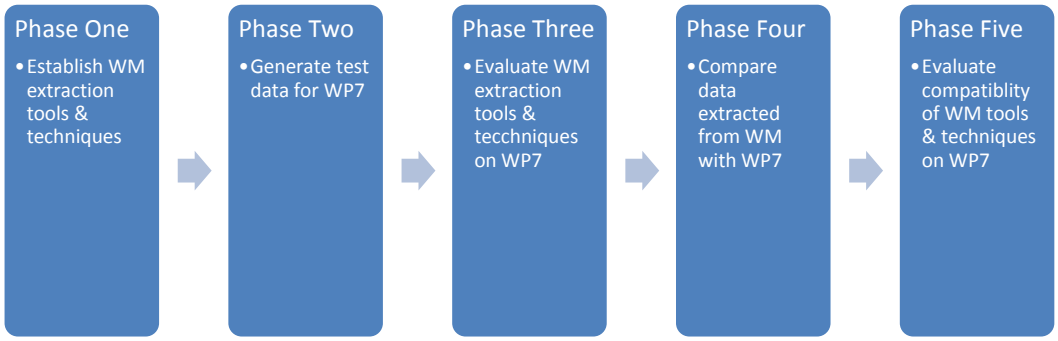


Figure 3.5: Research Phases

3.3.5 Data Map

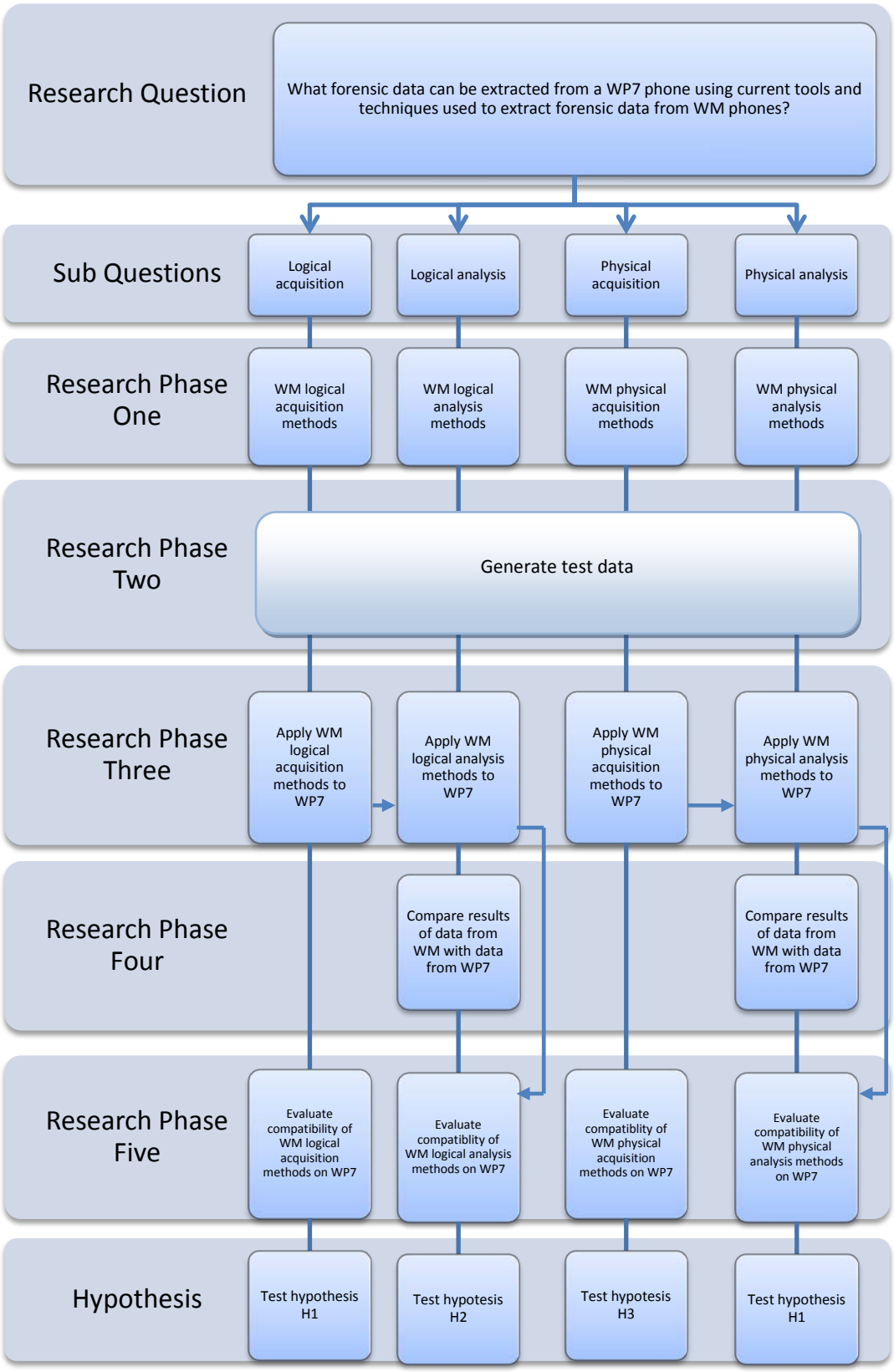


Figure 3.6: Data Map

3.4 DATA REQUIREMENTS

Four types of data were needed for the research. The first was the forensic tools and techniques used on WM (WM forensic tools and techniques). The second was the types of data extracted from WM (WM data) using WM forensic tools and techniques. The third was test data for WP7 (WP7 test data). Finally the fourth was the data extracted from WP7 using WM forensic tools and techniques (WP7 extracted data).

The WM forensic tools and techniques, and WM data were gathered from reviews of similar studies in Section 3.1 which was done in Phase One of the research. WP7 test data was generated in Phase Two based on WM data and also incorporated changes to WP7 (see Section 3.3.3). WM forensic tools and techniques were used to extract WP7 test data in Phase Three of the research. The WP7 extracted data was compared to WM data in Phase Four of the research.

3.4.1 Data Collection

Data was gathered from literature review, review of similar previous studies, as well as from experiments conducted during the research. Figure 3.7 shows an overview of the data collection process. Data on WM forensic tools and techniques were collected from literature review and reviews of previous similar studies. Based on recommendations from standards originations such as NIST and the forensic tools and techniques used in WM forensics, a list of WM forensic tools and techniques were formed. The list of WM forensic tools and techniques were compiled in Phase One of the research, and were applied to WP7 in Phase Three.

WM data types was also gathered from literature review and reviews of previous similar studies. Each tool had certain capabilities as to what data can be extracted from a WM phone. Based on the capabilities of each tool and what data was extracted from previous similar studies, a list of WM data was compiled in Phase One of the research. The WM data was used to create the WP7 test data in Phase Two, and will also be used to as a benchmark to compare with WP7 extracted data in Phase Four.

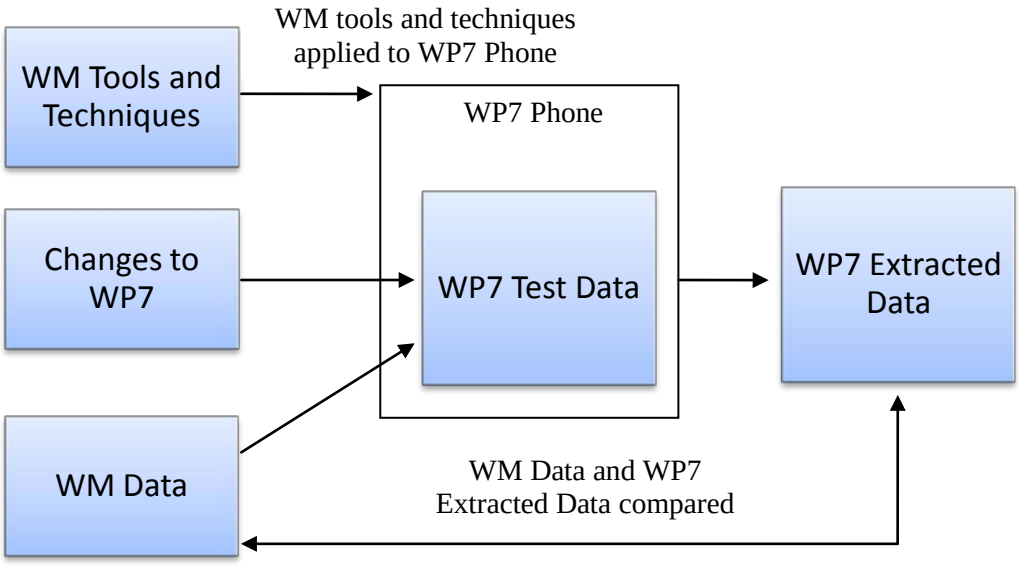


Figure 3.7: Data Collection Overview

WP7 test data was created based on WM data as well as changes to WP7. The WP7 test data was generated and loaded onto the WP7 phone in Phase Two of the research. The WM forensic tools and techniques established in Phase One were applied to the WP7 phone containing the WP7 test data in Phase Three. The data extracted using WM forensic tools and techniques on the WP7 phone was compared to the WM data in Phase Four.

3.4.2 Data Processing

The WM forensic tools and techniques and WM data does not require processing. Both were based on literature review and reviews of previous similar studies. WM forensic tools and techniques will be a list of tools and a list of techniques currently used in WM forensics. Likewise WM data will also be a list containing the types of data currently extracted from a WM phone.

WP7 test data will also be a list of types of data based on the WM data as well as new features of WP7. WP7 test data will be generated and loaded onto a WP7 phone. Each type of data will be manually entered into the phone and will be checked manually to verify the data entered is correct.

Once WP7 test data has been successfully loaded onto a WP7 phone, WM forensic tools and techniques will be used on the WP7 phone in a series of experiments see how much of the WP7 test data can be extracted. The WP7 extracted data (results of these experiments i.e. what data was able to be extracted

and what data wasn't) will be in the same format as WM tools and techniques and WM data which will be discussed in Section 3.4.4.

With data based on literature review and previous studies (i.e. WM tools and techniques, and WM data) the data and the process of getting the data are documented. With WP7 test data the process of generating the data, loading the data onto the phone, and verifying the data has been loaded successfully will be documented. Likewise with WP7 extracted data, each tool or technique used, how the tool or technique was used, and what data was extracted, and how the data was extracted will also be documented. Documenting the process as well as the results will ensure integrity of the data extracted, and will mean the process is verifiable and repeatable, should any findings be challenged.

3.4.3 Data Analysis

The main data analysis done in the research will be comparing the WM data (data extracted from WM phones using WM forensic tools and techniques) and WP7 extracted data (data extracted from WP7 phones using WM forensic tools and techniques). Using the same tools and techniques to acquire the same types of data will allow a direct comparison, showing how compatible WM tools and techniques are on WP7 phones.

WP7 test data has to be analysed (compared) with WM data to ensure that the two match. For example, if tool A is able to extract data X, Y, and Z from a WM phone, then tool A will be part of WM tools and techniques data, and X, Y, and Z will be part of WM data. WP7 test data needs to contain X1, Y1, and Z1, where X1 is the WP7 equivalent of X, Y1 equivalent to Y and so on. Because should tool A be able X1, Y1, and Z1, then analysis becomes very easy. However should X1 and X are not the same due to some errors or failure to properly analyse the data, then analysis becomes difficult and could produce errors.

3.4.4 Data Presentation

Because there are many WM tools and techniques, many types of data in WM data, which means many types of data in WP7 data, keeping track of what tools extracts what data on which phone can get out of hand very quickly. In order to keep track of the many types of data involved in the research, all the data will be presented in a table or matrix form. An example of a table is shown in Table 3.2

where the tools are listed and the data each tool is able to extracted is shown. If Table 3.2 were WM tools and techniques and WM data, then WP7 extracted would be in the same format with the same data types with the same tools and techniques.

Tool	**Data A**	**Data B**	**Data C**	**...**	**Data n**
Tool 1	X	X	X		
Tool 2		X			
Tool 3		X	X		
...					
Tool n					

Table 3.2: Data Presentation

3.5 LIMITATIONS OF RESEARCH

The focus of the research is to test what data can be extracted from a WP7 phone using current WM forensic tools and techniques used to extract data from WM phones. Logical acquisition and analysis are usually performed using forensic tools, and physical acquisition and analysis can be performed using tools or other methods which may require specialist equipment. A limitation of the research is the availability of the forensic tools and equipment. Due to resource limitations not all forensic tools discussed in Chapter 2 and Chapter 3 will be tested during the research. Likewise not all the forensic techniques discussed in Chapter 2 and Chapter 3 will be tested during the research. The forensic tools available for testing during the research are listed in Chapter 4.

The bootloader will not be tested as no suitable bootloader for WP7 was found during the research. The chip extraction method requires specialist equipment both to remove the chip from the phone's mainboard, but also to read data from the chip. The equipment required for chip extraction was not available for research so chip extraction will not be tested. Equipment capable of a physical acquisition using JTAG was available for the research so the JTAG method of acquisition will be tested.

If the hypotheses are proven correct, and the current WM forensic tools and techniques used for forensic examinations of WM phones are unable to extract data from WP7 phones, the next step would be to manually examine the data. In previous studies by Klaver (2010) and Rehault (2010), both authors developed their own tools in order to reconstruct the files from a physical dump as

well as recovering information stored in embedded databases. Reconstructing the file system is a time consuming process, and can vary greatly from device to device (Breeuwsma, Jongh, Klaver, Knijff, & Roeloffs, 2007). While the file system and databases are well documented with WM phones, the file system used in WP7 is not as well documented. WP7 uses a different file system, different compression, and WP7 also spreads the files between the phone's memory and the internal SD card, all of which adds another layer to reconstruct. Due to time constraints of the research, the physical dump files acquired will not be manually reconstructed.

During the course of the research the WP7 platform and the WM forensic tools and techniques was constantly changing (see Section 2.6). New models of WP7 phones were released, WP7 got updates including the Mango update which was rebranded WP7 as WP7.5, alternative tools for WP7 were released, and many of the forensic tools were also updated. Some of the new versions of the forensic tools were incorporated into the research, but the newer WP7 phones, the WP7.5 update, and the alternative tools were not incorporated into the research.

The scope of the research will be to test selected available WM forensic tools (discussed in Chapter 4) and the JTAG method on a WP7 phone to extract data from the WP7 phone.

3.6 CONCLUSION

In Chapter 3 similar previous studies on WM forensics were reviewed in Section 3.1 which established the current WM tools and techniques to extract data from a WM phone. The research questions and hypotheses were formed in Section 3.2 based on the reviews of similar previous studies and the problem areas in WP7 forensics. The research design discussed in Section 3.3 outlines the how the research will be conducted in the different phases of research. Finally in Section 3.4 the data requirements were discussed, outlining how data would be collected, process, analysed and presented in the research to ensure the results are valid and correct.

The review of the previous studies established the current WM forensic tools and techniques as well as the data which could be acquire from a WM phone using these tools and techniques. Test data will be generated based on previous

studies as well as new features of WP7 and will be loaded onto a WP7 phone. The established WM forensic tools and techniques will be applied to the WP7 phone with the test data. The results (what data was extracted) from the WP7 phone will be compared to results from data extracted from WM from previous studies. The comparisons of data extracted from WM and data extracted from WP7 will be used to test hypotheses and to answer the research question.

Chapter Four will discuss in detail gathering of the data using the methodology outlined in Chapter 3. Details of the data including the experiments conducted will be discussed as well as processing, analysis, and presentation of the data will also be discussed.

Chapter Four
Research Findings

4.0 INTRODUCTION

Chapter 3 defined the methodology, the research question (and sub questions) and the hypothesis (and sub hypothesis) to be used in the research. The methodology defined in Chapter 3 was used in Chapter 4 to conduct the experiments. The findings from the experiments are reported and analysed in Chapter 4, and the research hypothesis and research question will be tested and answered in Chapter 5.

To test the hypothesis, a series of experiments will be conducted to extract data from a Windows Phone 7 (WP7) phone in the same was as data were extracted from a Windows Mobile (WM) phone in similar published studies. The forensic tools and techniques currently used on WM phones (WM tools and techniques) were established in Chapter 3. The data which could be extracted from a WM phone (WM data) using the WM tools and techniques was also established in Chapter 3. The WM data will be used as a template to generate test data which will be loaded onto a WP7 phone. The WM tools and techniques will be applied to the WP7 phone to attempt to extract the test data.

Section 4.1 lists the equipment used during the research. Section 4.2 lists the forensic tools and techniques used on WM phones and the types of data which can be extracted from WM phones using the forensic tools and techniques. Section 4.3 details how the test data was generated and loaded onto the WP7 phone.

Forensic tools and techniques used on WM phones can be divided into four categories, logical acquisition, logical analysis, physical acquisition, and physical analysis. Section 4.4 reports and analyses the results from applying logical acquisition tools and techniques to the WP7 phone. Section 4.6 reports and analyses the results from applying logical analysis tools and techniques to the WP7 phone. Section 4.8 reports and analyses the results from applying physical acquisition tools and techniques to the WP7 phone. Finally Section 4.10 reports and analyses the results from applying physical analysis tools and techniques to the WP7 phone.

4.1 EQUIPMENT

The equipment used during the research includes a WP7 phone, three different Personal Computers (PC), a JTAG Riff Box, and forensic tools. The equipment used during the research are summarised in Table 4.1 below. Full specifications of the WP7 phone, the PCs, and the JTAG Riff Box are listed in Appendix A. Details of the forensic tools used will be given in the respective sections.

The WP7 phone used during the research was reset before test data was loaded onto the phone. The process of resetting and loading data onto the phone is discussed in Section 4.3. PC1 was used for the majority of the experiments, PC2 was used to run experiments which required Encase 7, and PC3 was used to run experiments which required Backtrack 5. The Riff Box was used to acquire a physical dump of the WP7 phone using the JTAG method.

Equipment	Model	Serial	Link	Notes
WP7 Phone	HTC HD7	HT0APRY00901	Table A1	OS Version: 7.0.7392.0
PC1	Windows 7 Professional 32 Bit SP1	N/A	Table A2	MFIT lab standalone PC (PC22)
PC2	Windows 7 Enterprise 64 Bit	71866	Table A3	MFIT Lab PC4
PC3	Windows 7 Enterprise 64 Bit	71858	Table A4	MFIT Lab PC3
JTAG Riff Box	Riff Box 1.30	FF.679E:0DDB-01F1:1A45	Table A5	

Table 4.1: Summary Of Equipment

4.2 DATA FROM LITERATURE REVIEW

Section 4.2 uses the literature reviewed in Chapter 2 and the reviews of similar published studies in Chapter 3 to establish the current WM forensic tools used, the current WM forensic techniques used, and the data which can be extracted from a WM phone using the forensic tools and techniques. Table 4.2 lists the main studies used to establish the WM forensic tools, techniques, and data extracted. The WM forensic tools are discussed in Section 4.2.1, the WM forensic techniques are discussed in Section 4.2.2, and the WM data which could be extracted are discussed in Section 4.2.3. The WM data will be used to generate

test data for the WP7 phone and the WM tools and techniques will be applied the WP7 phone to test what data can be extracted.

Article	Authors	Discussed	Abbreviation
Cell Phone Forensic Tools: An Overview and Analysis	(Ayers et al., 2005)	Section 2.4.3	NIST
Introduction to Windows Mobile Forensics	(Casey et al., 2010)	Section 3.1.1	IWMF
Windows Mobile Advanced Forensics: An Alternative to Existing Tools	(Rehault, 2010)	Section 3.1.2	WMAFAlt
Windows Mobile Advanced Forensics	(Klaver, 2010)	Section 3.1.3	WMAF
Forensic Data Acquisition from Cell Phones using JTAG Interface	(Kim et al., 2008)	Section 3.1.4	FDAJTAG
A Comparison of Forensic Evidence Recovery Techniques for a Windows Mobile Smart Phone	(Grispos et al., 2011)	Section 3.1.5	CWM

Table 4.2: Summary of Literature and Studies Reviewed

4.2.1 Windows Mobile Forensic Tools

The current forensic tools used on WM phones were complied based on the literature reviewed in Chapter 2 and the similar studies reviewed in Chapter 3. A summary of the WM forensic tools is shown in Table 4.4 which lists the tools, the source, and the capabilities of the tool. Note that many of the tools had changed since the previous similar studies were originally published, and the later versions of the tools used for the research are listed in the respective sections

WM Forensic Technique	Source	Acquisition	Analysis
Using Forensic Tools	Table 4.4	Logical and Physical	Logical and Physical
Bootloader	WMAFAlt	Physical	N/A
JTAG	FDAJTAG	Physical	N/A
Chip Extraction	WMAF, FDAJTAG	Physical	N/A
Manual Analysis	WMAF, WMAFAlt	N/A	Physical

Table 4.3: Windows Mobile Forensic Techniques

WM Forensic Tool	Source	Logical Acquisition / Analysis	Physical Acquisition	Physical Analysis
PDA / Cell Seizure	NIST	X	X	X
GSM .XRY / XACT	NIST, IWMF, WMAF	X	X	X
Oxygen PM	NIST	X		
MOBILedit! Forensic	NIST	X		
TULP2G	NIST	X		
CellDEK	NIST	X	Not stated	Not stated
PhoneBase	NIST	X		
Secure View	NIST	X		
ITSUTILS	IWMF, WMAF		X	X
Mobile Spy	IWMF			
Universal Forensic Extraction Device	CWM	X	X	X
Physical Analyzer	CWM			X
WinHex Forensic Edition	CWM			X
Forensic Toolkit	CWM			X
Encase	CWM	X		X
Foremost	CWM			X
Scalpel	CWM			X
Simple File Carver	CWM			X
Phone Image Carver	CWM			X

Table 4.4: Windows Mobile Forensic Tools

4.2.2 Windows Mobile Forensic Techniques

The current forensic techniques used on WM phones were complied based on the literature reviewed in Chapter 2 and the similar studies reviewed in Chapter 3. A summary of the WM forensic tools is shown in Table 4.3. Due to resource constrains and availability of equipment, not all WM forensic techniques were tested. The WM forensic techniques which will be tested are listed in the respective sections.

4.2.3 WM Data

The current data extracted from WM phones using current WM tools and techniques were complied based on the literature reviewed in Chapter 2 and the similar studies reviewed in Chapter 3. A summary of the data extracted from WM phones is shown in Table 4.5.

WM Data	Source
Call Log	IWMF, CWM
Messages (SMS/MMS)	IWMF, WMAFAlt, WMAF, CWM
Emails	IWMF, WMAFAlt, WMAF, CWM
Contacts	CWM
Calendar	CWM
Browsing History	CWM
User Files	IWMF, CWM
Registry	IWMF, WMAFAlt
Deleted Data	WMAFAlt, MAF

Table 4.5: Windows Mobile Extracted Data

4.3 WINDOWS PHONE 7 TEST DATA

Section 4.3 details the creation of the test data which was loaded onto the WP7. The WP7 test data was based on the WM data listed in Table 4.5 as well as having GPS/Geo-Tagging data in the photos (discussed in Section 3.3.3). Table 4.6 shows a summary of the WP7 test data. The test data was created manually on the WP7 phone and includes deleted data. The process of how each type of data was created will be explained in the following sections.

Note as there is no built in app for WP7 to view or edit the registry, no registry entries were added or modified as part of the test data.

4.3.1 Resetting The WP7 Phone

The WP7 phone was reset to factory settings as recommended by Thurrott (2010). Once the phone is reset and the phone starts for the first time, some initial settings are required. The phone was set to used 'Recommended' phone settings, the time zone was set to 'Auckland, Wellington (UTC+12)', and details of the Windows LIVE account (created earlier) was entered (internet connection required). The phone was allowed to finish the factory reset. The time on the phone was verified with a PC to ensure the time settings were correct.

Type Of Data	Normal Data	Deleted Data
Call Log	1 x incoming 1 x missed 1 x outgoing	1 x incoming 1 x missed 1 x outgoing
Messages (SMS/MMS)	1 x SMS received 1 x SMS sent 1 x MMS sent	1 x SMS received 1 x SMS sent 1 x MMS sent
Emails	1 x sent 1 x received	1 x email
Contacts	1 x contact imported from Windows Live	1 x manually entered with phone number and email
Calendar	1 x entered into Windows Live	1 x manually entered
Browsing History	www.google.com Search for 'HTC HD7' and go to the first page returned (www.htc.com) www.microsoft.com www.aut.ac.nz	No deleted items
GPS / Geo-Tagging	Data from photos	Data from deleted photo
User Files	2 x photos taken using the built in camera. 2 x videos taken using the built in camera. 1 x OneNote notes containing text, a picture, and a voice recording. 1 x Word documents will be created. 1 x Excel spreadsheets will be created.	1 x photo 1 x video 1 x OneNote note 1 x Word document 1 x Excel spreadsheet

Table 4.6: Windows Phone 7 Test Data

4.3.2 Call Log

WP7's 'Call history' stores the last 300 calls which are divided into three types: incoming, outgoing, and missed calls (Stroh, 2010). The WP7 phone was visually inspected to check the call log was empty. Then two calls were made to the WP7 phone from the same phone (Phone A), one call was answered, the other call was not answered. The result was an incoming call and a missed call from Phone A in the 'call history'. Then the WP7 phone called the number in the 'call history' (Phone A). The call resulted in an 'outgoing' call in the call history to Phone A. The process was repeated again using different phone (Phone B). The result was six different calls of three different types from two different phone numbers. The entries from one phone (Phone B) was deleted from the call log, leaving only three calls from one number. The call log was visually inspected to verify the results.

NOTE: Call logs in WP7 are not accessible to applications, even those running on the phone, as many developers have mentioned on many online forums, including Microsoft's (MS) forum (Microsoft, 2010c). Due to the accessing problems there may be issues when attempting to extract the call log.

4.3.3 Text Messages (SMS) and Multimedia Messages (MMS)

SMS (text only messages) and MMS (messages containing text as well as an image or video) are treated as one and the same by WP7 in that both SMS and MMS messages are stored in the same place, presented the same way, and sent and received the same way. If the user sends only text, the message is sent as an SMS, and if the user sends a picture (with or without text), then the message is sent as an MMS. Currently WP7 can received both picture and video MMS, but can only send pictures (Stroh, 2010).

Visually WP7 shows messages as 'conversations', which means the messages are grouped by contacts (sender/receiver of the messages) rather than all the messages together. So if there are 10 messages from the same person, then the messages would show as one conversation, and if there are 10 messages from 10 different people, then the messages would show as 10 conversations.

The WP7 phone already had one SMS message after a factory reset. The message appears every time the phone is reset. The message is from 'Windows Phone', is a read only message, and can't be replied to. The message was checked visually, and was left on the phone undeleted. An SMS message containing 'A' was sent from Phone A to the WP7 phone. The WP7 phone then replied with an SMS message containing 'Re A' as shown in Figure 4.1. The process was repeated with Phone B with the message 'B' and the reply of 'Re B'. The result was SMS messages on the WP7 phone split into two conversations - Phone A and Phone B.

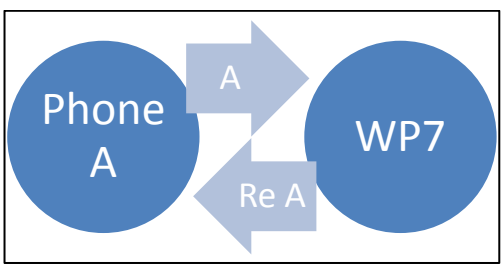


Figure 4.1: Test Data - SMS Message

An MMS message with an image was then sent from the WP7 phone to Phone A. Due to a network error, the MMS message never reached the intended recipient, and so no MMS reply was received. However the MMS message was saved on the WP7 phone. The same process was repeated for Phone B. The result was two conversations (Phone A and Phone B) and inside each conversation were be two SMS messages and one MMS messages. The messages from Phone B were then deleted, leaving only messages from Phone A.

4.3.4 Emails

WP7 can send and receive emails from a number of sources including webmail, Microsoft Exchange, and POP mail. Table 4.7 lists the types of email accounts supported by WP7.

Email Type	Description	Notes
Windows Live	Includes Hotmail, Xbox Live, and Live Messenger	
Outlook	Microsoft Exchange type server	Usually used in a corporate environment.
Yahoo! Mail	Yahoo's email service	
Google	Google's email service	
Other/Advanced	POP or IMAP	Commonly used by internet service providers for emails

Table 4.7: Emails in WP7

Emails in WP7 works slightly differently from how other data is managed by WP7. For example, with Contacts, WP7 will show all contacts in the one place (the People Hub) even though the contacts may have come from different source. Likewise with the Calendar, WP7 will use one calendar app showing many appointments from many sources. With emails however, each email account which is set up has to run on a separate email app. So if the user has set up four email accounts, there will be four email apps, one for each email account (Thurrott, 2010).

For testing purposes, only one account will be used, and since every WP7 phone has to have a Windows Live account in order to fully function, the Windows Live account will be used for testing. The WP7 phone initially had no email accounts after a factory reset. The WP7 phone was checked visually to ensure there were no email accounts. A new Windows Live account was created

on the WP7 phone directly (an internet connection was required). Once a Windows LIVE account was active, there were two emails already on the account from Windows LIVE. Once the account was created an email was sent from the WP7 phone. Once the recipient has received the email, the recipient then sent a reply to the WP7 phone. The recipient also sent new email. Once the second email was received, the email will be read and deleted. The result was one email sent and one email received, and one email deleted, all from the same recipient. The email in the deleted folder was then deleted, leaving only one sent email and one received email.

4.3.5 Contacts

WP7 presents all the contacts in a single application known as the 'People' Hub. Contacts can be added from a variety of sources such as phone contacts, call log, emails, social networking (such as Facebook) and Instant Messaging (IM) (such as Windows Live Messenger) (Stroh, 2010). The contacts may not only be a phone number and/or an email, but also the various online services associated with that person as well, such as an image from Facebook.

WP7 will populate the contact list when a new account is added, for example, if a Windows Live account is added, and the Windows Live account has 20 contacts, those 20 contacts will be imported to the WP7 phone. Then if another account, say Google was added, and that Google account has 12 contacts, those contacts will be imported to the WP7 phone. WP7 will try to 'sync' the contacts, meaning that if there are two 'John Doe's' then only one 'John Doe' is shown, but has the details from both the Windows Live and Google account.

For testing purposes, two contacts were created. One by manually entering the information into the WP7 phone with both a phone number and an email address. The second added from the call log having a phone number only. Note that all the contacts added to the WP7 phone will be synchronised automatically with the associated LIVE account. The manually entered contact was then deleted, leaving only the contact from the LIVE account.

4.3.6 Calendar

Appointments in WP7 can be either entered manually, or the imported from a variety of calendars including Windows Live and Google, and presents all the appointments in the one single calendar application.

The WP7 phone initially had no appointments in the calendar after a factory reset. The calendar was checked visually on the WP7 phone to ensure calendar was clear. Once accounts with appointments are added (such as Windows Live), the WP7 phone will import any appointments in the calendar from Windows Live account. The Windows Live account used did not have any appointments in the calendar. Again a visual inspection was done on the WP7 to ensure there were no appointments in the Windows Live account. The Windows Live website was also checked to verify there were no appointments. Two appointments were added, one manually into the WP7 phone, one into Windows Live. Both appeared on the WP7 device. The manually entered appointment was deleted, leaving only the appointed from the LIVE account.

4.3.7 Web Browsing

Web browsing on WP7 is done by default using the Internet Explorer (IE) application. The WP7 phone initially had no browsing history or cache after a factory reset, and each page (site) which is visited will be saved in the browsing history.

When IE is opened for the first time, the default homepage will be opened (the homepage will vary between phones). Then the following pages were visited in the following order:

www.google.com

Searched for 'HTC HD7' and went to the first page returned (www.htc.com)

www.microsoft.com

www.aut.ac.nz

No more web pages were visited in order to keep the browsing history intact for testing. There is no option to remove single entries from the browsing history, but rather the entire history can be deleted, so no browsing data was deleted.

4.3.8 GPS / Navigation

The GPS capabilities built into all WP7 phones are used by different programs for different purposes such as locating the phone when lost, maps and navigation, and geo-tagging when taking a photo.

Locating the phone when lost is useful, but has no data of interest in a forensic investigation. Maps and navigation may contain useful data for a forensic investigation. However currently there is a very limited number of dedicated navigation programs for WP. Most mobile forensic tools are able to extract data from these navigation programs, but since none exists for WP7, navigation data will not be investigated in the research. The geo-tagging of photos and videos can be useful for a forensic investigation. The geo-tagging or GPS data is stored on the photo or video files, and so will be discussed in the User Files section.

4.3.9 User Files

User files on the WP7 can be in a variety of different forms, and so will be broken into the following categories - pictures, videos, and documents.

4.3.9.1 Pictures

Pictures on WP7 is accessed through the 'Pictures Hub' (Stroh, 2010). Pictures on WP7 phone can be either taken using the built in camera, or can be synchronised with pictures from the PC using Zune (Thurrott, 2010).

After a factory reset, WP7 already had nine pictures on the device. These are sample pictures stored in a folder called '7'. Other than the images in the '7' folder, there are no other pictures on the WP7 phone. The folder was checked visually to verify. When the Camera is used for the first time WP7 asks if location settings should be used to indicate where the photo was taken (geo-tagging). The feature was enabled. Three photos were taken using the built in camera with the default settings. Pictures taken using the inbuilt camera are stored in a folder called 'Camera Roll'. After the three photos were taken, the phone was visually checked to verify the 'Camera Roll' folder had been created in the 'Pictures Hub' and 'Camera Roll' folder contained the three pictures taken. One of the pictures taken was then deleted, leaving two pictures.

4.3.9.2 Videos

Videos on WP7 can be accessed through the 'Pictures Hub' like pictures, or can be accessed through the 'Music + Videos Hub'. Videos on WP7 can be either taken using the built in camera, or can be synchronised with videos from the PC using Zune.

After a factory reset, WP7 had no videos on the phone. A visual check was done on the WP7 phone to verify there were no videos on the phone. A video will then be taken on the WP7 phone using the built in camera. Then two more videos were taken again using the same method giving a total of three videos. All videos were taken using the default settings. Videos taken using the inbuilt camera are stored in the 'Camera Roll' folder if viewing using the 'Pictures Hub', or in 'Videos' section of the 'Music + Videos Hub'. One of the videos taken was then deleted, leaving two videos.

4.3.9.3 Documents

Documents refers to files which the user has created. These may include Office documents such as Word or Excel (Stroh, 2010), notes or memos, and other files which the user has created. The main source of user documents other than videos or pictures would be an Office document such as Word or Excel which comes standard with WP7 (Thurrott, 2010). The Office which comes standard with WP7 is known as Office Mobile, which has four applications, OneNote, Word, Excel, and PowerPoint. There is also a feature called SharePoint which allows users to share and collaborate on documents. The SharePoint feature will not be looked at as part of the research. All the Office documents is accessed through the 'Office Hub' (Thurrott, 2010).

OneNote is a an application for taking notes which may include text, pictures, and voice. Two notes were created using OneNote, one containing text only, and the other containing text, a picture, and a voice recording. Details of the two OneNote notes are listed in Table 4.8. Note2 was then deleted, leaving only Note1.

Title	Text	Picture	Voice
'Note1'	'Text1'	None	None
'Note2'	'Text2'	Picture taken using the camera	Recording made using the WP7 device.

Table 4.8: OneNote Notes

The picture taken when creating a note does not show in the 'Pictures Hub' i.e. the picture cannot be accessed without opening the note.

Two Word documents were created, the first document called 'Testdoc1' containing the text 'Word test document 1', and the second document called 'Testdoc2' containing the text 'Word test document 2'. 'Testdoc2' was then deleted, leaving only 'Testdoc1'. After saving a document Word will ask for the name of the user, and the user was left as the default user.

Two Excel spreadsheets were created, the first spreadsheet called 'Testexcel1' containing the text 'Excel test spreadsheet 1' and the second spreadsheet called 'Testexcel2' containing the text 'Excel test spreadsheet 2'. 'Testexcel2' was then deleted, leaving only 'Testexcel1'.

Mobile Office for WP7 allows opening and edition of PowerPoint slideshows, but does not allow creating slideshows. The idea of mobile PowerPoint is to review and tweak presentations while on the road before giving a presentation. The presentation is usually done on a PC and copied to the WP7 phone using either SharePoint or SkyDrive (Thurrott, 2010). SharePoint is a business product which costs money, whereas SkyDrive is a free cloud storage service from MS. Files on SkyDrive is accessed through the web browser then saved to the WP7 device. Connecting to cloud services may introduce data into the browser's cache and history, so no PowerPoint files will be copied to the WP7 phone.

4.4 LOGICAL ACQUISITION

Based on the tools listed in Table 4.4, the tools listed in Table 4.9 are ones available for testing for the research. Note many of the tools has been updated since the original studies were first published.

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 4.9: Tools Available for Testing

4.4.1 Device Seizure

Device Seizure (Paraben, 2011) was installed on PC1. The WP7 phone was connected to PC1. Device Seizure was executed. Data Acquisition was chosen, then WM Logical was chosen. Device Seizure was not able to recognise or connect to the WP7 phone. The logical acquisition process was retried both with and without Zune software installed on PC1. Both cases failed to recognise the WP7 phone.

4.4.2 XRY

XRY 6.0.1 was installed on PC1. XRY requires Zune not to be installed on the PC in order to acquire data from WP7. The WP7 phone was connected to PC1. Acquisition of the WP7 was executed by manually selecting the model of WP7. Logical acquisition was selected and executed successfully as shown in Figure 4.2.

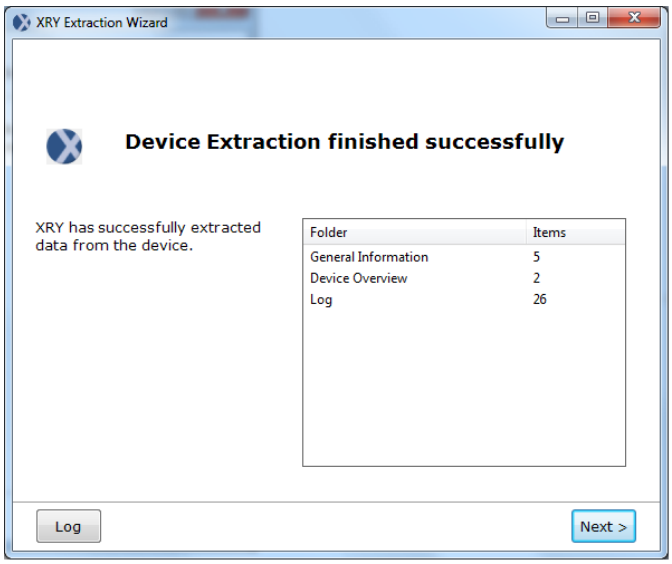


Figure 4.2: XRY Logical Acquisition

4.4.3 Oxygen Forensic Suite

Oxygen Forensic Suite (Oxygen Software, 2011) was installed on PC1. The WP7 phone was connected to PC1. Oxygen Forensic Suite was executed. Data acquisition was executed. Oxygen Forensic Suite failed to recognise or connect to the WP7 phone as shown in Figure 4.3. The logical acquisition process was retried both with and without Zune software installed on PC1. Both cases failed to recognise the WP7 phone.

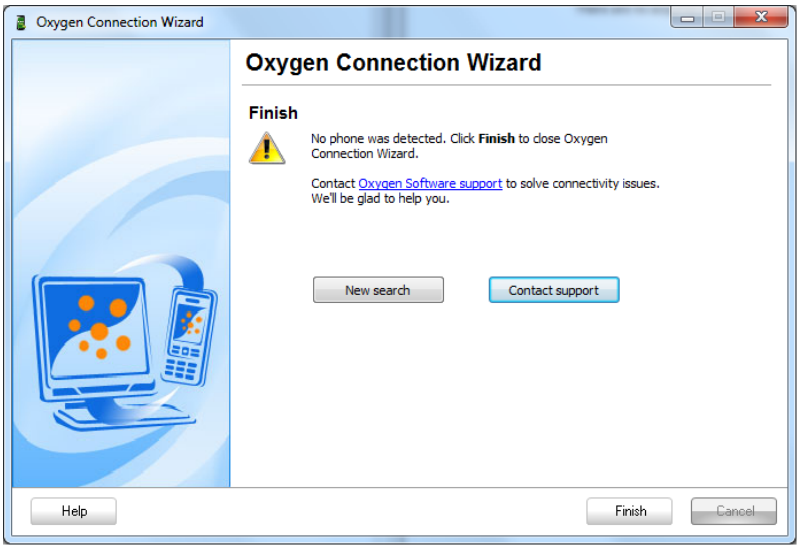


Figure 4.3: Oxygen Forensic Suite Logical Acquisition

4.4.4 MOBILedit! Forensic

MOBILedit! Forensic (Compelson Labs, 2011) was installed on PC1. The WP7 phone was connected to PC1. MOBILedit! Forensic was executed. Data acquisition was executed. MOBILedit! Forensic failed to recognise or connect to the WP7 phone as shown in Figure 4.4. The logical acquisition process was retried both with and without Zune software installed on PC1. Both cases failed to recognise the WP7 phone.

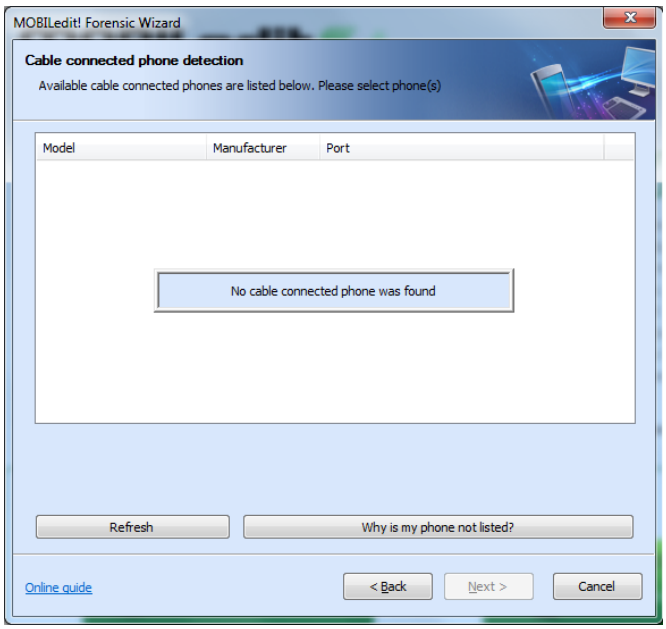


Figure 4.4: MOBILedit! Forensic Logical Acquisition

4.4.5 Secure View

Secure View (Susteen Inc, 2011) was installed on PC1. The WP7 phone was connected to PC1. Secure View was executed. Data acquisition was executed. Secure View requires selection of the specific model of the phone. The WP7 used was not listed. 'Windows Mobile' was selected. Secure View was not able to recognise or connect to the WP7 phone as shown in Figure 4.5. The logical acquisition process was retried both with and without Zune software installed on PC1. Both cases failed to recognise the WP7 phone.

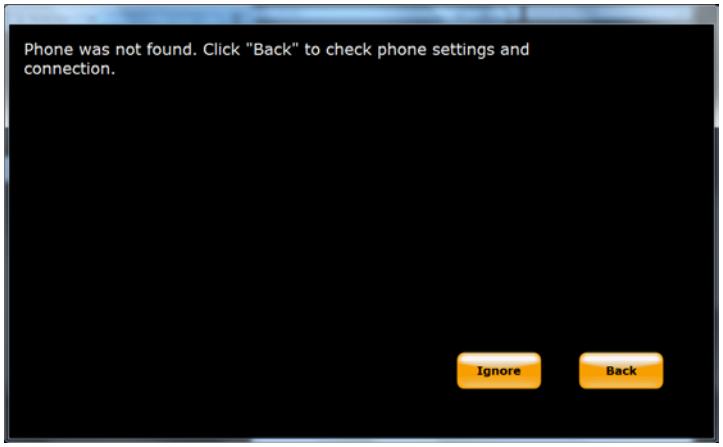


Figure 4.5: Secure View Logical Acquisition

4.4.6 Encase

The WP7 was connected to PC2. Encase was executed with admin rights on PC2. A new Encase case was created and 'Acquire Smartphone' was executed and WM 6.X was selected. Encase failed to recognise or connect to the WP7 phone as shown in Figure 4.6. The logical acquisition process was retried both with and without Zune software installed on PC1. Both cases failed to recognise the WP7 phone.

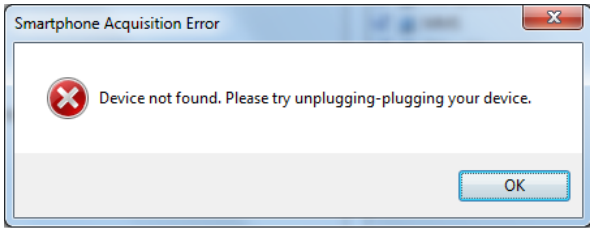


Figure 4.6: Encase Logical Acquisition

4.5 LOGICAL ACQUISITION RESULTS

Based on the literature review (Chapter 2) and previous similar studies reviewed in Chapter 3, all the tools used for the logical acquisition experiments were able to perform logical acquisitions of WM phones. Based on the literature review, only XRY had published any support for WP7 phones . The results of the logical acquisition experiments showed that XRY was able to connect to the WP7 phone and was able to perform a logical acquisition of the WP7 phone. Whereas Device Seizure, Oxygen Forensic Suite, MOBILedit! Forensic, Secure View, and Encase were unable to connect to the WP7 phone, and so was unable to perform a logical acquisition. The results of logical acquisitions experiments were consistent with the literature for tools.

A possible reason why most WM forensic tools are unable to connect to the WP7 phone is because the syncing mechanism between the phone and the PC has changed in WP7 (Section 3.2.2.1). WM connected to the PC using either ActiveSync or WMDC. Once connected to the PC, the files on the WM phone can be browsed using a file browser (such as Explorer). Viewing, editing, and copying files on the WM phone can also be done on the PC. Most WM forensic tools either install ActiveSync or WMDC as part of the installation of the tool, or requires the tool to be installed in order for the tool to work.

WP7 however doesn't connect to the PC using ActiveSync/WMDC, but using Zune. Once the WP7 phone has made connection with the PC, Zune synchronises media files such as music and pictures between the WP7 phone and the PC. Files on the WP7 phone cannot be viewed on the PC using a file browser, files on the WP7 phone can only be viewed using Zune, and only media files can be viewed. All other files on the WP7 phone are not shown in either Zune or the file browser. Note that XRY, which supports WP7 requires Zune not to be installed on the PC.

Most of the WM forensic tools were unable to recognise the WP7 phone, rather than recognising the phone and unable to interpret the data, which suggests that the way in which the phone connects to the PC (using Zune) was the issue. Because the logical acquisition experiments did not directly test if the change from ActiveSync/WMDC to Zune was the reason that most WM tools were

unable to acquire data from the WP7 phone, further research is required to verify the cause of why the WM tools were unable to acquire data from the WP7 phone.

4.6 LOGICAL ANALYSIS

Of the WM forensic tools tested for logical acquisition, only XRY was able to successfully acquire data from the WP7 phone. Since analysis is only possible if data has been acquired, only XRY was able to analyse the data from the WP7 phone. A summary of the data recovered by XRY is shown in Table 4.10. XRY was able to recover only pictures and videos. Details of the files extracted by XRY are listed in Appendix B.

Type Of Data	**Recovered by XRY**
Call Log	NIL
Messages (SMS/MMS)	NIL
Emails	NIL
Contacts	NIL
Calendar	NIL
Browsing History	NIL
GPS / Geo-Tagging	FULL
User Files	Partial (see Table 4.11)
Deleted	NIL

Table 4.10: XRY Logical Analysis

The nine pictures (discussed in Section 4.3.9.1) were all recovered, and the two videos (discussed in Section 4.3.9.2) were also recovered as shown in Table 4.11. As discussed in Section 4.3.9.1, WP7 comes with nine sample pictures already loaded on the phone. Two additional pictures were taken using the built in camera. All nine sample pictures and the two taken using the camera were recovered by XRY. The two pictures taken using the camera contained GPS coordinates within the EXIF (EXIF.org, 2011) or meta data which XRY also extracted. No other user documents were extracted.

User File	**Recovered**	**Note**
Pictures	FULL	Pictures taken using the built in camera contained GPS co-ordinates
Videos	FULL	
Documents	NIL	

Table 4.11: User Files Extracted by XRY

4.7 LOGICAL ANALYSIS RESULTS

Based on the literature for the tools, the literature review (Chapter 2) and reviews of similar studies, Table 4.12 shows the data each tool is capable of extracting from a WM phone.

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				

Table 4.12: Logical Analysis Results for Windows Mobile

From the results of the logical analysis experiments, all the tools tested except for XRY were unable to acquire any data from the WP7 phone. XRY was able to acquire only the images and videos from the WP7 phones. Table 4.13 shows a comparison of the data XRY can extract from a WM phone compared to the data extracted from the WP7 phone. Table 4.13 shows that XRY can extract much more data from a WM phone than can be extracted from a WP7 phone.

Data Type	XRY on Windows Mobile	XRY on Windows Phone 7
Call Log	X	
Messages (SMS/MMS)	X	
Emails	X	
Contacts	X	
Calendar		
Browsing History		
User Files	X	X
Registry	X	
Deleted Data	X	

Table 4.13: Data Extracted by XRY

The files extracted by XRY (images, movies, and music) are synchronised automatically when the WP7 is connected to Zune on the PC. That is if the WP7 phone contained media files, Zune copies the files from the WP7 phone to the PC.

So XRY does not extract any more data from the WP7 than what Zune normally copies to the PC by default. However from a forensic standpoint, XRY offers a more forensically sound method of extracting the data, along with other features useful for a forensic investigation such are reporting capabilities.

4.8 PHYSICAL ACQUISITION

Based on the WM forensic tools listed in Table 4.4 and the WM forensic techniques listed in Table 4.3, XRY, Device Seizure, and the JTAG method will be used in the research to perform a physical acquisition of the WP7 phone.

4.8.1 XRY

Using XRY to perform a physical acquisition is done in the same as a logical acquisition (see Section 4.4.2). When acquiring data from XRY by selected the WP7 phone, there is no option perform a physical. XRY was executed again acquiring from a 'generic' Windows Mobile device. A physical acquisition was selected. XRY was unable to detect the WP7 phone as shown in Figure 4.7. Note that XRY requires Zune software not be installed on the PC in order to work with WP7.

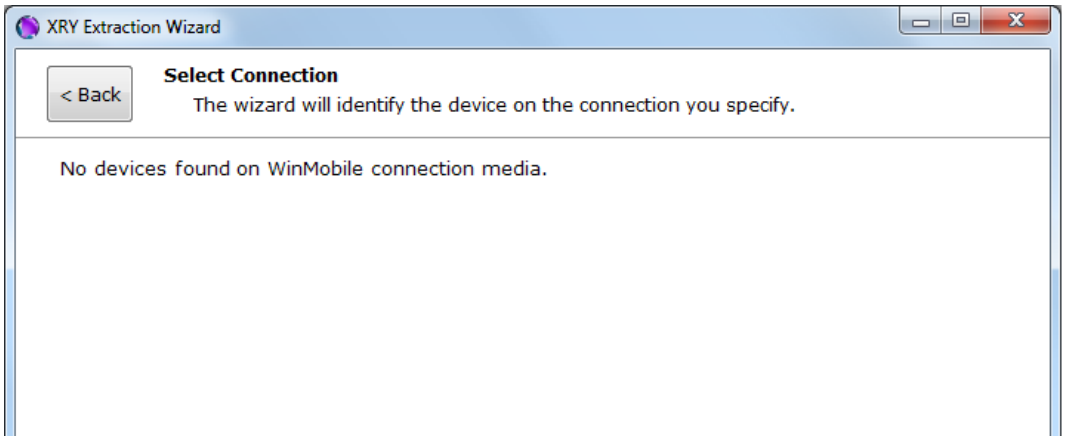


Figure 4.7: XRY Unable to connect to WP7 phone

4.8.2 Device Seizure

Using Device Seizure to perform a physical acquisition is done in the same way as a logical acquisition (see Section 4.4.1). Windows Mobile 5-6 physical acquisition was selected (shown in Figure 4.8). Device Seizure was unable to proceed with physical acquisition of WP7 phone. The physical acquisition process was retried

both with and without Zune software installed on PC1. Both cases failed to recognise the WP7 phone.

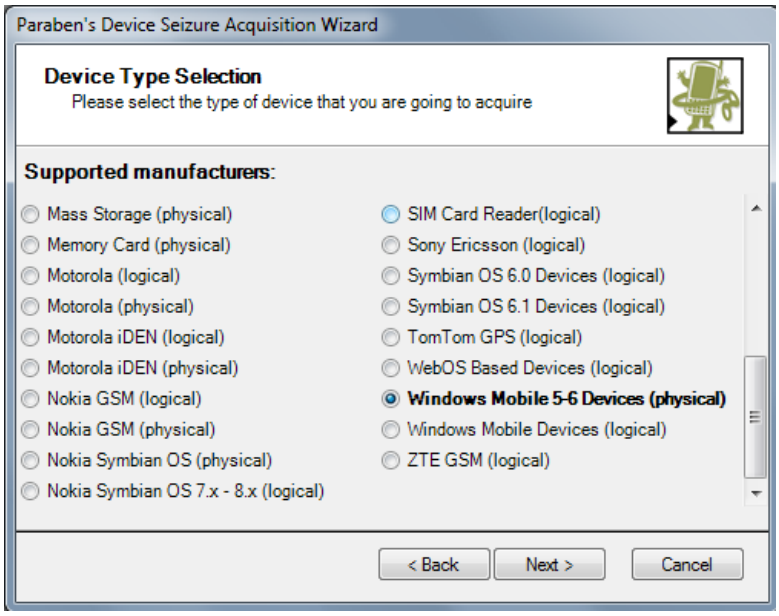


Figure 4.8: Device Seizure Physical Acquisition

4.8.3 JTAG

JTAG physical acquisition was done using the Riff Box. The WP7 phone was disassembled to expose the JTAG pins. Normally wires would be soldered to the JTAG pins as shown in Figure 4.10. For sizing reference, the coin in Figure 4.10 is a New Zealand one dollar coin which helps indicate the size of the JTAG pins. Due to the small and delicate nature of the JTAG pins and the related risk of damaging the pins, a board which connects directly to the pins (a jig) was purchased (Multi-com.pl, 2011). The Riff Box was connected to the JTAG pins of the WP7 using the jig, and the power and USB connections were made according to the configuration shown in Figure 4.9. The actual setup is shown in Figure 4.11. Note the internal SD card built into every WP7 phone was left in the WP7 mainboard.

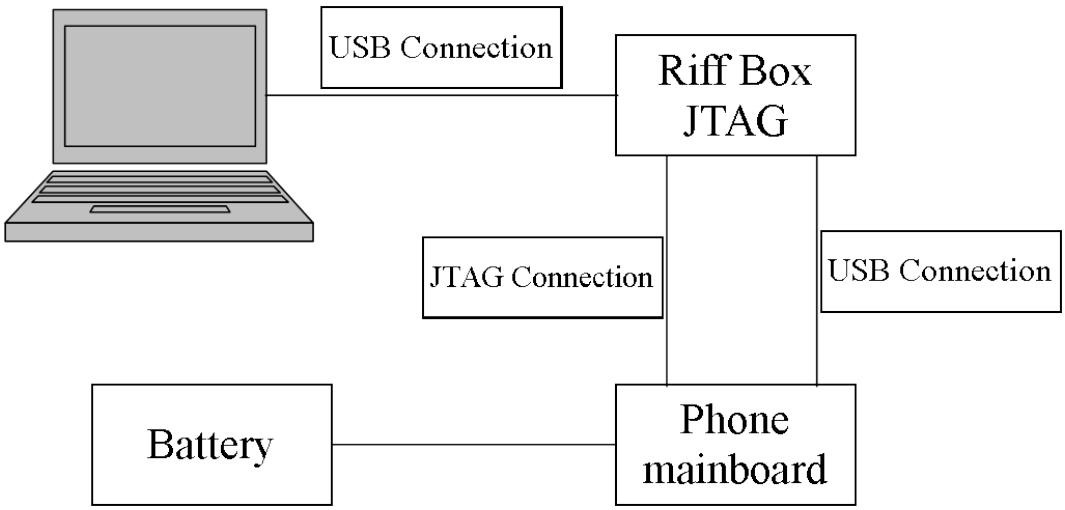


Figure 4.9: Riff Box JTAG Setup Diagram

The Riff Box was connected to PC1 and JTAGManager (Riff Box software) was installed. Both the firmware on the Riff Box, and the JTAGManager application were updated to the latest version using the update feature of JTAGManager. The HTC HD7 module (contains settings and instructions) for JTAGManager was also downloaded and installed.

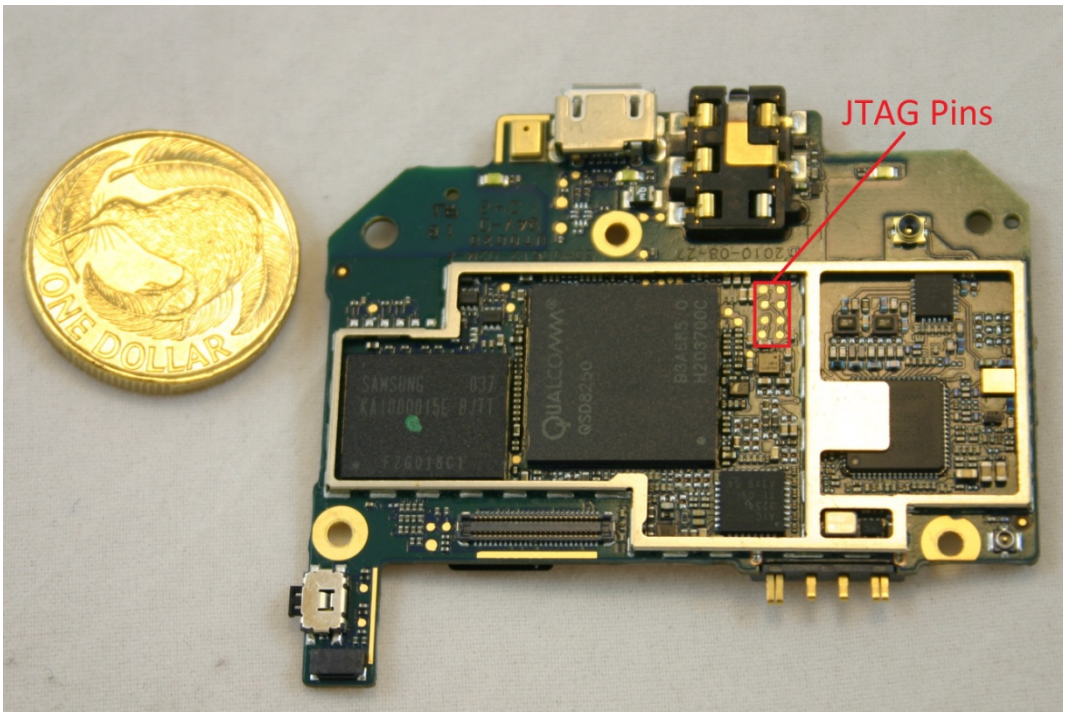


Figure 4.10: JTAG Test Pins on WP7 Phone

Using the HD7 settings, a physical dump was taken of the WP7 phone. The physical acquisition process using the Riff Box was about 30 minutes and resulted in a 512MB binary file (the same size as the ROM).

With forensic tools there are usually mechanisms built in to ensure the integrity of the acquired data, such as MD5 hashing or similar. The documentation for the Riff Box does not mention any hashing or error checking functionality. So how error checking (if any) is performed by the Riff Box is unknown. One way to check for data integrity is to perform multiple acquisitions and compare the hash values of the dumps. The chances of two non identical dumps having the same hash values are very small (Section 2.1). If two dumps have the same hash value, then the dumps are considered the same and that the acquisition process is reliable and repeatable.

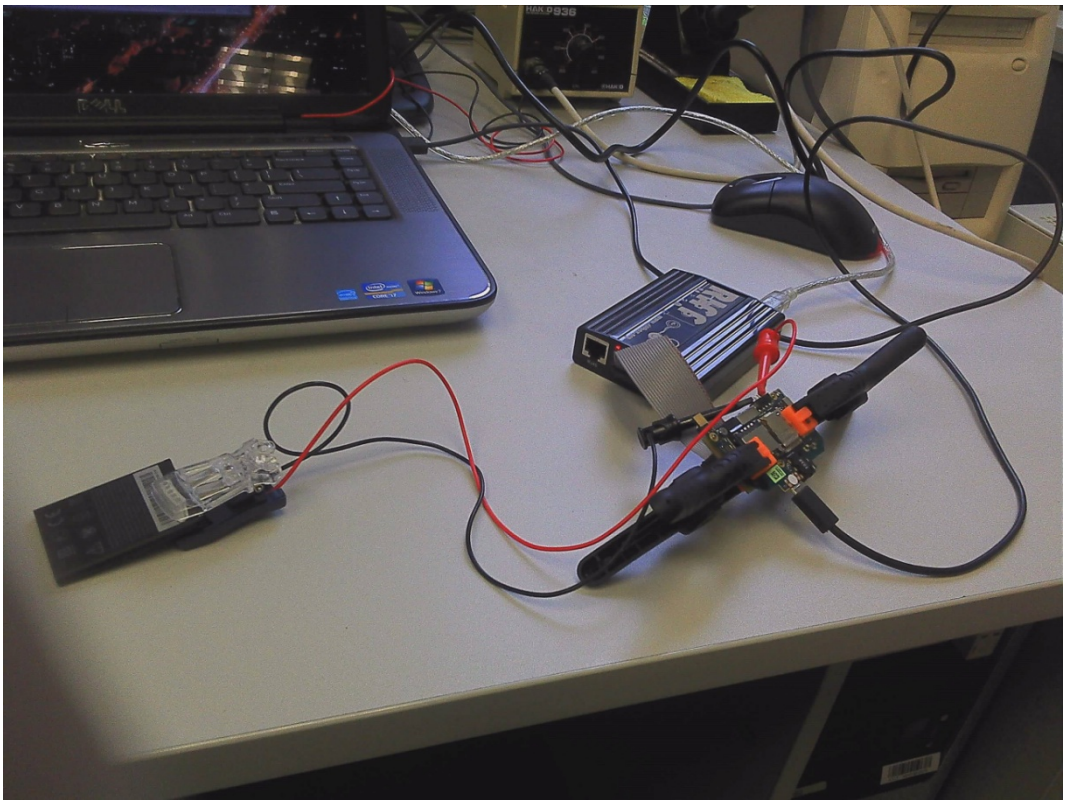


Figure 4.11: JTAG Riff Box Actual Setup

Two further acquisitions were done on the WP7 phone, giving a total of three dumps. When the dumps were compared, all three had different hash values. The different hash values of the dumps may indicate that there are errors in the dumps, but not necessarily. Because the mainboard of the WP7 phone is powered, the

contents of the memory may be modified because of ware levelling or some other mechanisms (Breeuwsma et al., 2007; Klaver, 2010). Because changes may be occurring to the memory while the mainboard is on is unknown, there may be valid reasons why acquisitions from flash memory may not be identical (and therefore a different hash value), but may be valid. Details of the dump files acquired by the Riff Box are listed in Appendix C.

Another way to verify the integrity of the dump file is to analyse and extract the data. In the case of the WP7, the contents of the test data is known. So should the test data be extracted, the extracted data can be compared to the original test data, and if the two are the same, then the dump is valid. However due to the many changes made to WP7 (discussed in Chapter 2) forensic tools normally used to analyse a WM dump may not be able to analyse a WP7 dump. Analysis of the WP7 dump is discussed in Section 4.10.

4.9 PHYSICAL ACQUISITION RESULTS

Based on the literature review (Chapter 2) and previous similar studies reviewed in Chapter 3, XRY, Device Seizure, and the JTAG method are able to perform physical acquisitions of WM phones. Neither the literature for XRY nor Device Seizure mentioned support for physical acquisitions of WP7, and neither XRY nor Device Seizure were able to physically acquire any data from the WP7 during the physical acquisition experiments. According to the literature for the Riff Box, a physical acquisition using the JTAG interface was possible from the WP7 phone (an HTC HD7), and during physical acquisition experiments the Riff Box was able to perform physical acquisitions from the WP7 phone. However as discussed in Section 4.8.3, each dump file acquired from the WP7 phone was slightly different, and the integrity (or forensic soundness) of the dump files would be very difficult to verify.

Another factor affecting the physical acquisition of a WP7 phone is how the internal SD card is used by WP7 (discussed in Section 3.2.2.2). With WM, the phone's memory stores the Operating System (OS) as well as user files (such as images and music). User files can also be stored on an SD card (or other types of removable memory), but the OS is not stored on the SD card. If the SD card was removed, the files on the SD card would no longer be available, but the WM

phone would still operate. However, WP7 uses the SD card in conjunction with the phone's memory, so everything (OS and user files) are stored across both phone's memory and the SD card. The technical details of exactly how data is shared between the phone's memory and the SD card has not been released by MS. However an article on www.theunwired.net (a smart phone news website) states

> "The Windows Phone 7 OS addresses the RAM memory and the internal memory as a kind of JBOD drive (Just a Box Of Disks/Just a Bunch Of Drives) where multiple physical memories (or drives) are combined into a single virtual disk ... As the name implies, disks are merely concatenated together, end to beginning, so they appear to be a single large disk and that's indeed the way Windows Phone 7 handles the memory" (Hess, 2010).

Other sources have stated a similar arrangement of WP7's memory and the SD card, including MS which stated in one of their support documents for WP7

> "When the operating system integrates the SD card with your phone: It reformats the SD card. It creates a single file system that spans the internal storage and the SD card. It locks the card to the phone with an automatically generated key." (Microsoft, 2011b).

If the SD card was removed from the WP7 and replaced with a new SD card, the phone would need to be reset and all the existing data is lost.

The Riff Box uses the JTAG interface which acquires a physical dump of the memory, and not of the SD card. As a result the dump may be a complete dump of the WP7 phone's memory, but not a complete dump of the WP7 OS.

4.10 PHYSICAL ANALYSIS

Based on the tools listed in Table 4.4, the tools used to analyse the physical dump acquired using the Riff Box (Section 4.8.3) are shown in Table 4.14.

Tool	Version	Notes
FTK	1.81.6 b 10.04.02	Trial
Encase	7.01.01	Academic Training
Foremost	1.5.7	Open Source
Scalpel	1.60	Open Source
Phone Image Carver	1.2.8.52	Trial

Table 4.14: Physical Analysis Tools

Although XRY is capable of WM physical analysis, the experiment in Section 4.8.1 shows that XRY is not capable of a physical acquisition of WP7, and so unable to analyse the physical dump, as XRY does not allow analysis of a dump acquired external to XRY.

FTK and Encase have built in functionality to analyse dump files. Foremost, Scalpel, and Phone Image Carvers are file carvers, which means analysing the dump files for specific types of files. FTK also has file carving capabilities. To carve out files, they types of files to be carved (what files to look for) has to be specified. Table 4.15 lists the types of files used for each of the file carving programs.

Type	FTK	Foremost	Scalpel	Phone Image Carver
BMP	X	X	X	X
GIF	X	X	X	X
JPEG	X	X	X	X
PNG	X	X	X	X
EMF	X			X
PDF	X	X	X	X
HTML	X	X	X	X
OLE	X			
AOL/AIM	X			
TIFF		X	X	
AVI		X	X	X
MOV		X	X	X
MPG		X	X	X
WAV		X	X	X
DOC		X	X	X
DOCX				X
PST		X	X	X
MP3		X	X	X
WMV		X	X	X
WMA		X	X	X
DAT (NT registry file)		X	X	
ZIP		X	X	X

Table 4.15: File Carving Settings

4.10.1 Forensic Took Kit (FTK)

The dump file was loaded into FTK on PC3. FKT was unable to recognise the dump file and displayed the files as 22 unknown files, each about 26MB in size. The file carving function was used with all file types selected as shown in Figure 4.12.

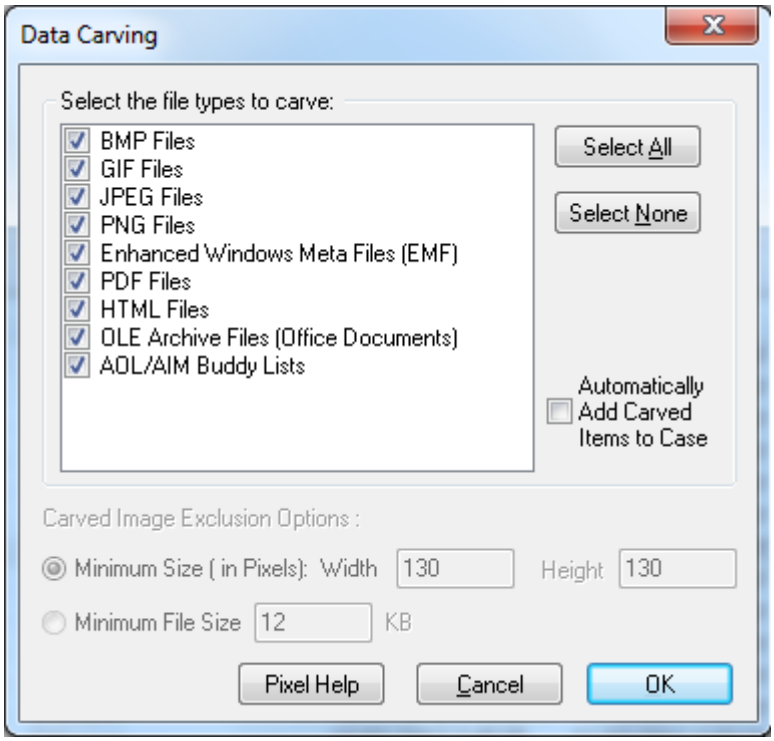


Figure 4.12: FTK File Carving Settings

Type	BMP	GIF	JPEG	PNG	HTML
Number of files	2	5	31	470	2

Table 4.16: Files Carved By FTK

The files carved by FTK are summarised in Table 4.16. Of the two bmp files found, both were fully viewable with no visible corruption. Of the five gif files, two were viewable with no visible corruption, two were viewable but had visible corruption, and one was not viewable at all. Of the 31 jpeg files found, three were viewable with no visible corruption, the remaining files were either had visible corruption or were not viewable. Of the 470 PNG files, 244 were viewable with no visible corruption, the remaining files were either viewable with visible corruption or not viewable. Of the two html files, both had readable text for the first four lines, then the rest of the file was unreadable text.

Of all the image files carved by FTK which were viewable, none appeared to be part of images contained in the test data loaded onto the WP7 phone. Of the two html files carved by FTK, neither appeared to be complete enough to be a full html document.

All three dump files were analysed in FTK with the same results.

4.10.2 Encase

The WP7 dump was loaded into Encase on PC2 as a raw image. An attempt was made to mount the image as a disk as well as a volume, both as FAT32 and exFat. In all cases Encase was unable to analyse the image. Encase showed the dump file as 'unallocated clusters', displaying the raw data, but no analysis or data process was performed. All three dump files were loaded into Encase with the same results.

4.10.3 Foremost

Backtrack 5 R1 32bit was installed on PC3 and Foremost was executed. Foremost was able to carve out the following files

Type	Complete	Incomplete	Evidence	Total
GIG	3		0	5
JPG	3 (duplicate)		0	31
JPG	3 (duplicate)		0	3252
PNG	0		0	507
BMP	0		0	7
TIF	0		0	1
MPG	0		0	12
MPG	0		0	12
MPG	0		0	17
HTM	0		0	2
WMV	0		0	1
WMA	0		0	1
WMA	0		0	1
ZIP	0		0	652

Table 4.17: Files Carved by Foremost

The files carved by Foremost are summarised in Table 4.17. Of all the files carved by Foremost, only three gif images and three jpg images were complete. Note that although a total of six jpg images were carved, there were only three images which were duplicated. Of the six complete images, none match those which were loaded onto the WP7 phone as part of the test data. The remaining files were either incomplete or count not be opened.

4.10.4 Scalpel

Scalpel uses the same configuration file as Foremost, and was configured with the same file types to carve (Table 4.15) using the same dump files. Scalpel is based on Foremost and was originally a Linux application, however there is also a Windows version of Scalpel. The Windows version was installed on PC1 and executed to carve files from the dump file. However Scalpel for Windows had many errors and was unable to carve any files. Backtrack (version 5R1 32bit Gnome), a collection of open source forensic software which runs under Linux was used. Backtrack which includes both Foremost and Scalpel (Backtrack, 2011) was installed on PC3 and executed. Scalpel under Linux also encountered many errors and was unable to carve any file.

4.10.5 Phone Image Carver (PIC)

Phone Image Carver was installed on PC1 and one of the dumps files were loaded. The file types to carve for were selected as shown in Table 4.15 . Phone Image Carver was able to carve out the following

Type	Number of Files	File Size	Date Created
DOCX	1	5KB	
JPG	29	4KB - 450KB	
MOV	463	171KB - 3.5GB	
MPEG	17	10MB	
TIFF	1	19.5MB	30 Apr 2010

Table 4.18: Files carved by Phone Image Carver

The files carved by Phone Image Carver are summarised in Table 4.18. The Word document (DocX) carved by Phone Image Carver was a 5KB with no details of created or modified dates. Of the twenty nine (29) JPG images carved by Phone Image Carver, only two were complete. The remaining images were all either corrupted or not viewable. The two images fully extracted by Phone Image Carver are not part of the test data loaded onto the WP7 phone, so is likely to be images associated with either the WP7 OS, or an application. None of the images had details of created or modified dates. The four hundred and sixty three (463) MOV movie files extracted are sized between 171KB to over 3.5GB. Even with compression the dump file cannot contain so many large files. None of the MOV movie files had details of created or modified dates. The seventeen MPEG movie

files extracted were all 10MB in size with no details of created or modified dates. The single TIFF image carved by Phone Image Carver was a19.5MB file with a created date of 30 Apr 2010. The entire carving process was repeated using three different dump files, all with the same results.

Note that because the version of Phone Image Carver used in the research is a demo version, there is no facility to save or export the carved files. The files can only be viewed using Phone Image Carver.

4.11 PHYSICAL ANALYSIS RESULTS

The data integrity of the physical dump file acquired during the physical acquisition experiments could not be verified (see Section 4.8.3) so three different dump files were acquired from the WP7 phone, and all each tool tested in the physical analysis experiments performed the same analysis operation on all three dump files. If analysis of the dump files yielded different results for each dump file, then the results would suggest that the dumps files were sufficiently different and may be corrupted. The results of the physical analysis experiments shows each tool used yielded the same results from each of the dump files. However unless data was extracted from the dump files which could be compared with the original test data on the WP7 phone, the data integrity of the dump files cannot be determined. The results of the physical analysis experiments shows that none of the tools tested were able to extract any of the original test data on the WP7 phone.

None of the tools tested in the physical analysis experiments were able to extract any of the original test data from the WP7 phone. While some complete files were extracted and many partial files were extracted, none of the files were part of the original test data. There could be multiple factors why the tools were unable to extract data from the physical dump files. The dump file may be corrupted and/or invalid (see Section 4.8.3), and so any data extracted from the dump will not be accurate. The tools may have been unable to recognise the TExFAT file system used by WP7 (Section 3.2.2.2), and so unable to extract data from any TExFAT partitions on the dump file. The compression used on WP7 is different to the compression used on WM. WM used a compression called XPR, whereas WP7 uses a newer version known as XPH (Hengeveld, 2010a; XDA Developers, 2010), which means until the data is decompressed the tools will not

be able to extract any data from the dump file. The data may be spread across the phone's memory and the internal SD card (Microsoft, 2011b), in which case a dump of the phone's memory is only part of the data. Any one of the factors mentioned above, or indeed even all the factors mentioned above may be the reason(s) why the tools were unable to extract any test data from the dump files, and further research is needed to confirm which factor(s) is or are affecting then results (discussed in Chapter 5).

The majority of the factors mentioned above are related to the changes made to WP7 which may affect a mobile forensic investigation (discussed in Section 2.3), namely changes to the file system used by WP7. Which factors and how many factors are preventing the tools to extract data from the WP7 phone requires more research which will be discussed in Chapter 5.

4.12 CONCLUSION

Chapter 4 reported and analysed the findings of applying WM forensic tools and techniques on a WP7 phone containing test data. The WM forensic tools and techniques were applied to the WP7 phone in four stages - logical acquisition, logical analysis, physical acquisition, and physical analysis. The findings from each stage was reported and analysed.

The WM forensic tools and techniques were established based on the literature reviewed in Chapter 2 and the reviews of similar published studies in Chapter 3. Likewise the data extracted from a WM phone using the WM forensic tools and techniques were also based on the literature reviewed in Chapter 2, and the reviews of similar published studies in Chapter 3. The data extracted from WM phones were used as a template to generate test data which was loaded onto the WP7 phone. The WM forensic tools and techniques were divided into four stages, logical acquisition, logical analysis, physical acquisition, and physical analysis. Each stage applied the WM tools and techniques to the WP7 phone to test what data can be extracted from the WP7 phone. The results were then reported and analysed in each of the respective sections.

Chapter 5 will evaluate the results from the experiments in Chapter 4, the suitability of current WM forensic tools and techniques on WP7 phones, and the implications of WP7 phones for digital forensic investigators.

Chapter Five
Discussion

5.0 INTRODUCTION

Chapter 4 reported the findings from the experiments derived using the methodology defined in Chapter 3. Chapter 5 will discuss the results from the experiments by evaluating the hypothesis and sub hypotheses to answer the research question and sub research questions. The results from the experiments and the implications of the results for digital forensic investigators will then be discussed. Other aspects of Windows Phone 7 (WP7) which may have implications for digital forensic investigators such as the constant changing landscape of WP7 and the alternative tools available for extracting data will also be discussed, followed by a conclusion.

Section 5.1 will answer the research questions and sub research questions by using the results of the experiments from Chapter 4 to test the hypothesis and sub hypotheses. The research questions and hypotheses will be presented in a table format with arguments for (accepting) and against (rejecting) the hypothesis. Section 5.2.1 will discuss the results from the logical acquisition and analysis experiments, Section 5.2.2 will discuss the results from the physical acquisition experiments, and Section 5.2.3 will discuss the results from the physical analysis experiments. Section 5.3 will discuss the changes to the WP7 platform and mobile forensic tools, followed by Section 5.4 which will discuss some alternative tools which could be used to extract data from WP7 phone. Section 5.5 will discuss the implications of WP7 for a digital forensic investigator based on the literature, results from experiments, as well the alternative tools. Finally a conclusion is given in Section 5.6.

5.1 RESEARCH QUESTIONS AND HYPOTHESES

The research question and the hypothesis were derived in Chapter 3. The research question was used to form four sub research questions and the hypothesis was used to form four sub hypotheses. The experiments were conducted using the methodology derived in Chapter 3, and the findings from the experiments were

reported in Chapter 4. The findings reported in Chapter 4 will be used to test the hypotheses and to answer the research questions.

The research questions and associated hypothesis will be in a table format with arguments for and against the hypothesis given, and a summary given. The research question and hypothesis will be discussed in Table 5.1 and the sub research questions with the associated hypothesis will be discussed in Tables 5.2 - 5.5.

<table>
<tr><td colspan="2">Research Question (Q0):
What forensic data can be extracted from a WP7 phone using current tools and techniques used to extract forensic data from WM phones?</td></tr>
<tr><td colspan="2">Hypothesis (H0):
The current tools and techniques used to extract forensic data from WM phones are not capable of extracting forensic data from WP7 phones.</td></tr>
<tr><td>Argument For:
Of the WM tools tested, only XRY was able to extract any data from the WP7 phone. All other tools tested were unable to acquire any data from the WP7 phone.

The physical acquisition technique tested (JTAG), the data integrity of the dump file could not be verified.

None of the tools tested during the physical analysis experiments were able to extract any data from the dump files.</td><td>Argument Against:
User media files such as pictures and videos can be extracted from WP7 phones using XRY.</td></tr>
<tr><td colspan="2">Summary:
Based on the results from the experiments reported in Chapter 4, XRY was able to extract the user pictures and videos stored on the WP7 phone. All the other WM forensic tools tested were unable to extract any data from the WP7 phone. A physical dump was acquired from the WP7 phone, however the data integrity of</td></tr>
</table>

the dump could not be verified. The physical analysis experiment results indicate that the tools tested were unable to extract any data from the dump file, however because the data integrity of the dump file could not be verified, the results of the physical analysis experiments remain inconclusive. The physical acquisition and physical analysis results with be discussed in the respective sections. Based on the results from all the experiments conducted during the research, only XRY is able to extract data from the WP7 phone, and XRY is only able to extract the user picture and video files.

Table 5.1: Research Question and Hypothesis

Sub Research Question 1 (Q1): *Are current forensic tools and techniques used for logical acquisitions of WM capable of logical acquisitions of WP7 phones?*	
Sub Hypothesis (H1): *The current forensic tools and techniques used for logical acquisitions of WM are not capable of logical acquisitions of WP7 phones.*	
Argument For: Device Seizure was not able to successfully perform a logical acquisition of the WP7 phone. Oxygen Forensic Suite was not able to successfully perform a logical acquisition of the WP7 phone. MOBILedit! Forensic was not able to successfully perform a logical acquisition of the WP7 phone. Secure View was not able to successfully perform a logical acquisition of the WP7 phone. Encase was not able to successfully	**Argument Against** XRY was able to successfully perform a logical acquisition of the WP7 phone.

perform a logical acquisition of the WP7 phone.	
Summary: Of the literature for the WM forensic tools (both the tools tested and those not tested alike) discussed in Section 2.4.3, only XRY had published any support for WP7. Of the six tools tested for logical acquisition of the WP7 phone, only XRY was able to successfully perform a logical acquisition. The five other tools were unable to recognise the WP7 phone and so was unable to perform a logical acquisition. The results of the experiments were consistent with the literature. Based on the results from logical acquisition experiments and the literature, the majority of the current forensic tools used for logical acquisitions of WM are not capable of logical acquisitions of WP7 phones, with the exception of XRY.	

Table 5.2: Sub Research Question 1

Sub Research Question 2 (Q2): *What forensic data can be extracted from a WP7 phone using logical analysis tools and techniques currently used for WM phones.*	
Sub Hypothesis (H2): *The current forensic tools and techniques used for analysis of logical acquisitions of WM phones are not capable of analysis of logical acquisitions of WP7 phones*	
Argument For: The pictures and videos extracted by XRY are automatically copied to the PC when the WP7 phone is synced with Zune software (Section 2.4.2.1), however not in a forensically sound manner. Device Seizure was not able to successfully extract any data from the WP7 phone.	**Argument Against:** XRY was able to successfully extract picture and video files the WP7 phone.

Oxygen Forensic Suite was not able to successfully extract any data from the WP7 phone. MOBILedit! Forensic was not able to successfully extract any data from the WP7 phone. Secure View was not able to successfully extract any data from the WP7 phone. Encase was not able to successfully extract any data from the WP7 phone.	
Summary: Of the literature for the WM forensic tools (both the tools tested and those not tested alike) discussed in Section 2.4.3, only XRY had published any support for WP7. Of the six tools tested for logical analysis of the WP7 phone, only XRY was able to successfully extract any data from the phone. The results of the experiments were consistent with the literature. XRY was able to extract picture and video files stored on the WP7 phone. Based on the results of the logical analysis experiments, of the current forensic tools used for examinations of logical acquisitions of WM phones only XRY is able to extract data from the WP7 phone, and XRY is only able to extract the user picture and video files.	

Table 5.3: Sub Research Question 2

Sub Research Question 3 (Q3): *Are current tools and techniques used for a physical acquisitions of WM phones capable of physical acquisitions of WP7 phones?*
Sub Hypothesis (H3): *The current tools and techniques used for a physical acquisitions of WM phones are not capable of physical acquisitions of WP7 phones.*

Argument For:	**Argument Against**
Each physical dump file acquired by the Riff Box had a different hash value, and the data integrity of dump files were not verifiable. XRY was not able to successfully perform a physical acquisition of the WP7 phone. Device Seizure was not able to successfully perform a physical acquisition of the WP7 phone.	The Riff Box was able to perform a physical acquisition of the WP7 phone.
Summary: XRY and Device Seizure were not able to perform a physical acquisition of the WP7 phone. The Riff Box was able to perform a physical acquisition of the WP7 phone, but each acquisition (dump file) had a different hash. The data integrity of the dump files could not be verified (see Section 4.9). From a digital forensic standpoint where the forensic process has to be repeatable and verifiable, the dump files acquired by the Riff Box is not forensically sound. Based on the results of the physical acquisition experiments in Section 4.8, the current forensic tools and techniques used for a physical acquisitions of WM phones are not capable of physical acquisitions of WP7 phones.	

Table 5.4: Sub Research Question 3

Sub Research Question 4 (Q4): *What forensic data can be extracted from a WP7 phone using physical analysis tools and techniques currently used for WM phones.*	
Sub Hypothesis (H4): *The current tools and techniques used for analysis of physical acquisitions of WM phones are not capable of analysis of physical acquisitions of WP7 phones*	
Argument For:	**Argument Against**

None of the tools tested were able to extract any of the original test data from the WP7. All three of the dump files produced the same results.	The data integrity of the dump files could not be verified so the results may not be accurate.
Summary: Based on the results from the physical analysis experiments in Section 4.10, none of the tools tested were able to extract any test data from the dump files. However because the data integrity of the dump files could not be verified, the results may be inaccurate. Further research of the dump file, such as manually examining and rebuilding the dump file is required to determine the structure of the dump files and how compression is used. Rebuilding the dump file is beyond the scope of the research and remains a possibility for future work (see Section 3.5). Due to the data integrity of the dump files being unknown, the hypothesis remains undetermined.	

Table 5.5: Sub Research Question 4

5.2 DISCUSSION OF FINDINGS

The results and findings from the experiments conducted during the research were detailed and reported in Chapter 4. Section 5.2 will discuss the findings from the different experiments and how results are related to a digital forensic investigation of a WP7 phone. Section 5.2.1 will discuss the results of the logical acquisition and analysis experiments, Section 5.2.2 will discuss the results from the physical acquisition experiments, and Section 5.2.3 will discuss the results from the physical analysis experiments.

5.2.1 Logical Acquisition and Analysis

Logical acquisition and analysis of WM phones are usually done using the same forensic tool. Of the many tools available which are capable of performing logical acquisitions and analysis of WM phones (see Table 4.4), only XRY had published support for WP7 phones. The results from the logical acquisition experiments and the logical analysis experiments (Sections 4.4 and 4.6 respectively) shows that

only XRY was able to extract any test data from the WP7 phone, confirming the published literature of the tools tested.

The results of the data extracted by XRY for WM based on Table 4.11 when compared with the data extracted by XRY for WP7 phones based on the logical acquisition and analysis experiments indicate that even though XRY is able to extract data from WP7, the types of data extracted is greatly reduced as shown in Table 4.13. XRY is able to extract data such as call logs, messages, emails and similar from WM, but can only extract user image and video files from WP7. As discussed in Section 4.7, the files extracted by XRY (user image and video files) are automatically copied to the PC when the WP7 phone is synced to the PC. XRY is able to extract no more data from the WP7 phone than what is automatically copied to the PC when the WP7 phone is synced with the PC. The comparison of the files extracted by XRY and those automatically copied to the PC is only to illustrate the limited data extractions of XRY on WP7, and not to suggest that syncing the WP7 phone to a PC is a suitable procedure for a digital forensic investigation of a WP7 phone. XRY provides a more forensically sound method of extracting data as well as other features useful to a forensic investigation such as logging and reporting capabilities.

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	

Table 5.6: Data Extracted by XRY

A possible reason for reason why the WM forensic tools were not able to extract data from the WP7 is the fact that WP7 does not use ActiveSync/WMDC to sync files with the PC as WM did (Section 2.3.1). ActiveSync/WMDC provided a connection between the WM phone and the PC to allow files to be synchronised between the WM phone and the PC. The connection made using ActiveSync/WMDC was utilised by most WM forensic tools to connect and acquire data from WM phones. WP7 uses Zune to sync files with the PC, and the

connect made between the WP7 phone and the PC provided by Zune may be sufficiently different enough to prevent the forensic tools from connecting to the WP7 phone. Although the results from the logical acquisition and analysis experiments showed that most tools were unable to connect to the WP7, the experiments did not show that the cause of the failure was due to the fact that WP7 does not use ActiveSync/WMDC.

5.2.2 Physical Acquisition

The physical acquisition experiments used XRY, Device Seizure, and the Riff Box to perform a physical acquisition of the WP7 phone. XRY and Device seizure are forensic tools which are capable of a physical acquisition of WM phones while the Riff Box is a device capable of a physical acquisition using the JTAG method. Section 5.2.2.1 will discuss the results of the physical acquisition experiments using the tools XRY and Device Seizure, and Section 5.2.2.2 will discuss the results of the physical acquisition experiments using the Riff Box.

5.2.2.1 Tools

Some tools such as XRY, Device Seizure, and UFED are capable of both a logical acquisition and a physical acquisition of a WM phone. Most forensic tools acquire a physical dump from a WM phone by copying an agent (a program) onto the WM phone (Klaver, 2010). The agent runs on the WM phone and dumps the data from the WM phone to the forensic tool. The agent is copied onto the phone using the ActiveSync/WMDC connection, and the data is dumped from the phone to the forensic tool using the same connection.

Because an ActiveSync/WMDC connection is required for forensic tools to perform physical acquisitions from WM phones, and no ActiveSync/WMDC connection is created with WP7 phones, the expected outcome would be that the forensic tools could not successfully acquire a physical dump from the WP7 phone. XRY and Device Seizure were tested during the physical acquisition experiments and both tools were unable to acquire a physical dump from the WP7 phone, which is consistent with the lack of the ActiveSync/WMDC connection.

However, the results from the physical acquisitions experiments shows that the tools were unable to acquire a physical dump from the WP7 phone, and not as to why the tools were unable to acquire a physical dump from the WP7

phone. Besides no longer using an ActiveSync/WMDC connection, WP7 has many other changes compared to WM (Section 2.3.1) such as not being able to run any programs designed for WM phones, using a different file system, and spreading the data across the phone's memory and the internal SD card. Any combination of these factors may have contributed to the results seen during the physical acquisition experiments.

The conclusion that XRY and Device Seizure are unable to acquire a physical dump from the WP7 phone can be drawn based on the results from the physical acquisition experiments. The reason(s) why XRY and Device Seizure were unable to acquire a physical acquisition from the WP7 phone cannot be established based on the results of the physical acquisition experiments, hence no conclusion can be drawn.

5.2.2.2 JTAG Method

The Riff Box was used to acquire a physical dump from the WP7 phone using the JTAG interface during the physical acquisition experiments. Three dumps were acquired by the Riff Box in total, and all dumps were acquired without any errors reported by the Riff Box. However all three dump files had different hash values and hence were all different to one another. As discussed in Section 4.5 even though the dump files are different, the dump files may be still valid and the data contained within the dump files may be the same.

The various methods of verifying the data integrity of the dump files were discussed in Section 4.5, and one method of determining if the dump files are valid or not is to analyse the dump files. If different data was extracted from the three dump files after an analysis, then the indication would be the data contained within the dump files are different, and hence not valid. If test data was extracted from any of the dump files after an analysis, then the indication would be that the dump file from which the test data was extracted was valid. However as the results of physical analysis experiments revealed that the data extracted from all three dump files were the same, but also that none of the data extracted from the dump files was part of the original test data loaded onto the WP7 phone.

Another method of verifying the dump file is to use another tool or technique to acquire a physical dump from the WP7 phone and compare the dump file with the dump file acquired using the Riff Box. Physical acquisition tools of

WM phones include using tools such as XRY, bootloader, JTAG, and chip extraction methods. As shown by the results from the physical acquisition experiments XRY and Device Seizure are unable to physically acquire a dump file from the WP7 phone, and at the time of writing no bootloader for the HTC HD7 phone was available which allowed physical acquisition of the phone. No other JTAG debuggers were available for testing during the research so no dump files can be acquired. The chip extraction method remains the most forensically sound method of acquiring data from the phone's memory (discussed in Section 3.1.4). However the chip extraction method was beyond the scope of the research due to the equipment required for the chip extraction being unavailable and the high risks involved as discussed in Section 3.5.

Because the data integrity of the dump files acquired using the Riff Box cannot be verified, no conclusions can be drawn from the results of the physical acquisition of the WP7 phone using the Riff Box.

5.2.3 Physical Analysis

Of the tools used during the physical analysis experiments, Encase and Scalpel were unable to analyse the dump files at all. The remaining tools were able extract some data from the dump files. Many of the files extracted were corrupt (cannot be opened) or incomplete, and a few files extracted were complete. However none of the files extracted by any of the tools was part of the test data. Most of the data extracted appeared to be part of the system files such as icons and ringtones rather than user files such as pictures, videos, or documents.

There could be several reasons why the tools tested were unable to extract any data from the dump files. One reason may be the fact that the data integrity of the dump files were unable to be established. The dump files may be corrupt or invalid so results from the analysis of the dump files are invalid. Another reason may be the fact that the file system used by WP7 is different to WM. WM uses the TFAT file system on some partitions of the memory where as WP7 uses TexFAT on some partitions of the memory (see Section 2.3.3.1). WM also uses the XPR compression for some files, whereas WP7 uses the XPH compression (see Section 2.3.3.1). The tools used for analysis may have been unable to analyse the newer file system and newer compression on WP7. Another possible reason is the spreading of the data between the phone's memory and the internal SD card.

While some WM phones had SD cards, the data on the SD card is independent of the phone's memory. With WP7 both the phone's memory and the SD card are used as a single storage with files spread across the two. Because the files are spread between the phone's memory and the internal SD card, a physical acquisition such as JTAG or chip extraction which only acquires the data from the phone's memory will be incomplete. How the files are spread and which files are spread is unknown, and so what files are acquired from the phone's memory and what files remains on the SD card is unknown.

As discussed in Section 3.1 some previous similar studies manually rebuilt the dump file to reconstruct the file system. A successfully reconstructed dump can verify that the data integrity of the dump file is valid. Even if unsuccessful, the process of a manually reconstructing the dump file may reveal details about the dump file such as partition tables, file system, and compression. Manually reconstructing a WP7 dump file may not be possible due to the spreading of files between the phone's memory and the internal SD card, since the dump file only contains data from the phone's memory, and not the internal SD card. For reasons discussed in Section 3.5 manually reconstructing is beyond the scope of the research and remains a possibility for future work.

Because the data integrity of the dump files cannot be verified, the results of the physical analysis experiments may be incorrect and hence also cannot be verified. The factors discussed above may be the reason(s) why the tools tested were unable to extract any test data from the WP7 phone. However based on the results, no conclusions can be drawn from the physical analysis experiments, and further research is required to determine the file structure of the dump files and why the tools tested were unable to extract any test data.

5.3 UPDATES TO WINDOWS PHONE 7 AND MOBILE FORENSIC TOOLS

Since WP7 was launched the WP7 landscape has been constantly changing, with newer WP7 phones being released, updates to the WP7 Operating System (OS), updates to the mobile forensic tools, as well as new tool released by the hacker community (discussed in Section 5.4). The fast and constant changing nature of both the WP7 landscape and the forensic tools is an important aspect to consider

when interpreting the results. Between the initial launch of WP7 to the time of completing the research, no less than six updates were released for WP7, including two major updates known as 'NoDo' and 'Mango' which added over 300 features updates to WP7 (Microsoft, n.d.-g). WP7 with the Mango updates are officially known as the WP7.5 because of the many changes. The WP7 used for testing for the research did not have the NoDo or the Mango updates as the research had already reached too mature a stage to implement the updates. Likewise the HTC HD7 phone has been replaced with the newer HTC HD7S phone. Many of the mobile forensic tools discussed in the research has also been updated. XRY, Oxygen Forensic Suite and MOBILedit! Forensic have all had never versions released during or after the experiments (see Table 5.7).

Due to the fast changing nature of WP7 and mobile forensic tools, the results can be considered a snapshot of the state of WM tools and techniques applied to WP7 phones at the time of the research. Further research is need to investigate how the changes to WP7.5 are impacting the forensic investigation process as WP7 has impacted the forensic investigation process.

Tool (used in research)	Version used in research	Latest Version
XRY Complete	6.0.1	6.1.1
Oxygen Forensic Suite 2012	3.7.0.1	4.0
MOBILedit! Forensic	6.0.0.1397	6.0.2.1503

Table 5.7: New Versions of Forensic Tools

5.4 ALTERNATIVE WINDOWS PHONE 7 TOOLS AND TECHNIQUES

Since WP7 was launched, the hacker community i.e. individual or groups of developers who are not part of the official WP7 community such as Microsoft (MS) or HTC. The tools developed by hackers or alternative tools come primarily from a forum of mobile developers known as XDA-Developers (XDA Developers, 2012). The alternative tools are beyond the scope of the research and were not tested as part of the research. The discussion of the alternative tools is to make forensic investigators and others working with WP7 forensics aware of the alternative tools, what data can be extracted from WP7 phone using the alternative tools, so further research may be done on the alternative tools.

According to the literature, the alternative tools are able to backup/restore WP7 phones, view/extract messages, view/copy files, and view/edit the registry,

none of which are achievable using current WM forensic tools and techniques. The suitability of the alternative tools for a forensic investigation requires further research to establish. Establishing the suitability of the alternative tools for a forensic investigation may be useful to an investigator given the ability of the tools to extract data from WP7. Research into how the tools are able to extract data from a WP7 phone may also be of interest to a forensic investigator or forensic tool developer.

One of the most powerful of the alternative tools is Windows Phone Device Manager (WPDM) and TouchXperience (TX) by (Schapman, 2011b). WPDM is an application which runs on the PC while TX is an application which runs on the WP7 phone. When WPDM and TX are connected, WPDM allows the user to view, copy, and modify files on the WP7 phone, backup and restore the WP7 phone, and many other features (see Appendix for a full listing of the features of WPDM). TX has a file explorer, which allows the user to view, copy, and modify files on the WP7 phone directly. WPDM was used by a member of XDA-Developers to extract SMS messages from WP7 phones (XDA Developers, 2011b). The method involved copying the file 'store.vol' from the WP7 phone to the PC and running a perl script (the complete steps of how to extract SMS messages from WP7 is given in the appendix). While the method was not tested as part of the research, the example of extracting SMS messages from WP7 illustrates how WPDM can be utilised to aid a forensic investigation.

Another application from the same author as WPDM and TX is Registry Editor for Windows Phone 7 (Registry Editor) (Schapman, 2011a). Registry Editor is an application which runs on the WP7 phone and allows the user to view and modify the registry on the on the WP7 phone. How well Registry Editor works with WP7 and the suitability of Registry Editor for a forensic investigation requires further research.

5.5 IMPLICATIONS FOR DIGITAL FORENSIC INVESTIGATORS

The changes made to WP7 compared to WM outlined by the literature in Chapter 2 may have an impact on a digital forensic investigation. Some of the impacts on a forensic investigation were confirmed by the experiments in Chapter 4. The alternative tools discussed in Section 5.4 may also have an impact on a digital

forensic investigation. The results from the experiments conducted in Chapter 4 and the alternative tools have implications for a digital forensic investigator working with WP7 phones. The implications of using WM forensic tools on a WP7 forensic investigation will be discussed in Section 5.5.1, the implications of using WM forensic techniques on a WP7 forensic investigation will be discussed in Section 5.5.2, and the implications of using alternative tools and techniques on a WP7 forensic investigation will be discussed in Section 5.5.3.

5.5.1 Windows Mobile Forensic Tools

Of the WM tools discussed in the research, as indicated by the literature and verified by the experiments, only XRY was able to extract any data from the WP7 phone. So for digital forensic investigator using 'standard' tools (those discussed in articles by NIST and those used in published studies), XRY is the only tool which will extract any data from WP7 phones. However XRY will only extract the user's media files, which are pictures, movies, and music, all of which could be extracted by syncing the WP7 phone with the PC using Zune. While XRY is a more forensically sound method of extracting data compared to syncing the phone with the PC, the comparison illustrates the limited extraction capabilities of XRY. When used on WM phones, XRY is able to extract data such as call log, contacts, messages, and others, as well as being able to perform a physical acquisition of the WM phone. Whereas with WP7, XRY only able to perform a logical acquisition, and is only able to extract the user's media files (see Table 4.18).

For digital forensic investigators using standard forensic tools, the current limitations means XRY is the only tool available to extract data from a WP7 phone, and the only data which could be extracted are the user's pictures, videos, and music files.

5.5.2 Windows Mobile Forensic Techniques

The WM forensic techniques discussed in the research were the Bootloader method, the JTAG method, and the chip extraction method. Based on the research, no bootloader capable of a physical acquisition was available for WP7 phones at the time of writing. The JTAG method and the chip extraction method used on WM phones should be applicable to WP7 phones since WP7 phones use the same types of memory chips are WM phones. The JTAG method was tested using the

Riff Box and the results of the experiments were inconclusive as the data integrity of the dump file acquired by the Riff Box could not be verified.

Even if a successful physical dump of the WP7 phone's memory was acquired, there may still exist issues for the forensic investigator, namely the spreading of the files across the phone's memory and the internal SD card, and the newer files system, and the newer compression (TexFAT and XPH respectively). The spreading of the files across the phone's memory and the internal SD card means that the dump of the phone's memory will not contain the files stored on the SD card. Data stored on the SD card cannot be acquired by removing the SD card and reading the card using standard methods such as an SD card reader (discussed later). How the files are spread is unknown and was not verified during the research, and more research is required to establish the mechanism of how the files are spread and which files are stored on the phone's memory and which files are stored on the internal SD card. Nevertheless, the forensic investigator should be aware the spreading of the files is occurring in WP7 and take the fact into account when conducting a WP7 forensic investigation. Similarly the file system and compression used by WP7 have changed compared to WM. The file system used by WP7 is TexFAT as opposed to TFAT used by WM, and the compression used by WP7 is XPH as opposed to XPR used by WM. The effects of TexFAT file system and XPH compression on forensic tools were not established during the research, however the forensic investigator should be aware of the new file system and compression used on WP7 and take the new file system and new compression into account when conducting a WP7 forensic investigation.

Another aspect of WP7 for forensic investigators to note is the internal SD card used by WP7. Many WM phones and smartphones have a removable memory card (which may be SD or may be another type). The memory card can be removed to be examined independent of the phone. The SD card used by WP7 is not removable, and is locked (discussed in Section 2.3.3.1). If the WP7 was disassembled and the internal SD card removed, the SD card would not be readable by a card reader. Although investigation of the WP7 internal SD card was beyond the scope of the research, the internal SD was removed from the WP7 phone during the research and the SD card was verified to be locked. The WP7 internal SD card can be unlocked by using a phone running the Symbian OS, such as many Nokia phones (Ziegler, 2010). However when the card is unlocked, all

the data on the card is lost. The locking method used by WP7 on the internal SD card and how to recover the files stored on the SD card requires more research to established. Forensic investigators should be aware of the fact that the internal SD card of WP7 phones are locked, and conventional methods of reading the SD card cannot be used to read WP7's internal SD card.

Digital forensic investigators working with WP7 phones need to be aware of the changes discussed above and to take the factors into consideration. While many of the points discussed require further research, the changes to WP7 outlined by the literature and the results from the experiments from the research indicate that the current WM techniques require modifications before the techniques can be successfully applied to WP7 phones.

5.5.3 Alternative Windows Phone 7 Tools And Techniques

Based on the literature for the alternative tools, the alternative tools are able to extract more data from a WP7 than the WM forensic tools and techniques discussed and tested in the research, and may be useful for forensic investigators when dealing with WP7 phones.

The alternative tools could potentially fill the gap in a forensic investigation by extracting the data which the established WM forensic tools and techniques are unable to extract. However a few issues exist when using the alternative tools for forensic investigations. Firstly many alternative tools will not simply run on a WP7 phone. WP7 was designed to only run approved applications downloaded from the MarketPlace (Microsoft, n.d.-a), which many of the alternative tools are not, and so workaround methods need to be employed in order to run many of the alternative tools. Many of the workarounds will void the phone's warranty and may damage the phone. For example, the TX application will only run on WP7 phones made by HTC, and not other brands, limiting the tool's use to only HTC WP7 phones. The TX application also requires the WP7 phone to be 'unlocked' and the TX application 'sideloaded' (XDA Developers, 2011a), both of which are described on the XDA-Developers forum. The effects of unlocking a WP7 on a digital forensic investigation requires further research to determine, however generally with a forensic investigation the smaller the digital footprint left on the phone, the better. So unlocking the WP7 phone then loading an untested application in order to extract forensic data is not ideal. Another issue

with using alternative tools is the reliability and suitability of the alternative tools for use in a digital forensic investigation. The forensic investigator should be aware that the reliability and suitability of the alternative tools for use in a forensic investigation has not been tested, and should be diligent in following forensic guidelines such as those from NIST and ACPO discussed in Chapter 2 to ensure suitability of the tools for a forensic investigation and the forensic soundness of any extracted data using the alternative tools. An example of an alternative method tested for suitability in a digital forensic investigation is the bootloader method used by Rehault (2010) discussed in Section 3.1.2. The bootloader method was originally posted on the XDA-Developers forum and was used by the author to extract forensic data from the WM phone.

5.6 CONCLUSION

Chapter 5 discussed the findings from the experiments conducted in Chapter 4 with regards to the hypotheses defined in Chapter 3 to answer the research questions. The results from the experiments conducted in Chapter 4, the ever changing landscape of the WP7 platform, and the alternative tools available for WP7 were also discussed. Finally the implications of the results from the experiments, the changes to the WP7 landscape, and the alternative tools would have to a digital forensic investigator were discussed.

Based on the results from the experiments conducted during the research, all but one of the current WM forensic tools and techniques tested were unable to extract any data from a WP7 phone. Of the WM forensic tools tested, only XRY was able to extract data from the WP7 phone. The data extracted by XRY from the WP7 phone is less than what XRY is capable of extracting from a WM phone. All other WM forensic tools tested were unable to extract any data from the WP7 phone. The Riff Box was able to acquire a physical acquisition of the WP7 phone using the JTAG method, however the data integrity of the physical dump acquired was unknown and further research is required to confirm the results. Of the tools tested for during the physical analysis experiments, none of the tools were able to extract any data from the dump files. However due to the data integrity of the dump files being unknown, the results from the physical analysis experiments are inconclusive and requires further research.

The changes to WP7 hardware (new handsets), software (new WP7 OS), forensic tools, and alternative tools during the course of the research were discussed. Although many of the changes to WP7 and the updates to WM forensic tools were not tested, and the alternative were also not tested during the research, digital forensic investigators and future researchers should be aware of the impact these factors may have on a digital forensic investigation, and incorporate these factors into the forensic investigation or future research.

Chapter 6 will conclude the research with a summary of the research conducted and the significant results which has been discovered. Limitations to the research will be discussed to determine specific areas of research that were hindered during the research. Areas of further research will be outlined followed by a conclusion.

Chapter Six
Conclusion

6.0 INTRODUCTION

The introduction of the Windows Phone 7 (WP7) also introduced many major changes to the Microsoft (MS) mobile Operating System (OS) compared the previous version - Windows Mobile (WM). The changes to WP7 were identified in the literature review (Chapter 2), along with the current forensic tools and techniques used on WM. The literature reviewed identified the problems areas in WP7 and digital forensic investigations, namely the how well the WM forensic tools and techniques would work on WP7 phones. Chapter 3 formulated the research questions and hypotheses, as well the methodology to conduct the research in order to test the hypotheses and answer the research questions. The experiments outlined by the methodology were conducted and the results and findings were reported in Chapter 4. Chapter 5 analysed and discussed the results from the experiments to test the hypotheses and answer the research questions. Chapter 5 also discussed the various aspects of the research and the implications for a digital forensic investigator working with WP7.

The WM forensic tools and techniques were established by the literature review in Chapter 2 and the reviews of similar published studies in Chapter 3. The WM forensic tools and techniques were divided into two types of data extraction, logical and physical. The logical and physical types of data extraction were divided into two further stages, acquisition and analysis as described in the forensic process model discussed in Chapter 2, resulting in four different parts - logical acquisition, logical analysis, physical acquisition, and physical analysis. Research questions, hypotheses, and experiments were developed in Chapter 3 to address four parts of the WM tools and techniques indentified. The findings from the experiments were reported in Chapter 4 and were discussed in Chapter 5, along with the implications of the findings and other aspects of WP7 for a digital forensic investigator.

Chapter 6 will conclude the research by presenting a summary of the findings in Section 6.1, a discussion of the limitations of the research in Section 6.2, and a discussion of the future research in Section 6.3.

6.1 SUMMARY OF FINDINGS

Test data was generated based on the data extracted from WM phones and loaded onto the WP7 phone. WM forensic tools and techniques were applied to the WP7 phone to test what data can be extracted. The results from the logical acquisition experiments showed that of the tools tested, only XRY was able to acquire any data from the WP7 phone. The remaining tools tested were unable to acquire any data from the WP7 phone. Because XRY was able to acquire data from the WP7 phone, the hypothesis H1 that "*The current forensic tools and techniques used for logical acquisitions of WM are not capable of logical acquisitions of WP7 phones*" was rejected, allowing the research question Q1 of "*Are current forensic tools and techniques used for logical acquisitions of WM capable of logical acquisitions of WP7 phones?*" to be answered with "XRY was able to perform a logical acquisition of the WP7 phone".

The results from the logical analysis experiments showed that of the tools tested, only XRY was able to extract any data from the WP7 phone. However the data extracted from the WP7 phone by XRY is much less that what XRY can extract from WM phone as shown in Table 4.13. Even though XRY's data extraction capabilities on WP7 is much less than those on WM, the results were able to reject the hypothesis H2 that " *The current forensic tools and techniques used for analysis of logical acquisitions of WM phones are not capable of analysis of logical acquisitions of WP7 phones* " and showed that at least XRY was able to extract some data from WP7 phones. With hypothesis H1 being rejected, the research question Q2 of "*What forensic data can be extracted from a WP7 phone using logical analysis tools and techniques currently used for WM phones*" can be answered with "User files such as pictures and videos can be extracted from a WP7 phone using XRY".

The physical acquisition experiments tested the tools XRY and Device Seizure, and the Riff Box which uses the JTAG method to perform a physical acquisition. XRY and Device Seizure were both unable to acquire any physical data from the WP7 phone. The Riff Box using the JTAG method was able to acquire a physical dump of the WP7 phone's memory. A total of three dump files were acquired using the Riff Box with all three files having different hash values (file signatures). There may be reasons for the dump files having different hash

values while containing valid data. Three dump files were acquired to test the data integrity of the dump files. If when analysed all the dump files yielded different results, then the indication is that the data integrity of the dump files are not valid. If on the other hand the test data loaded onto the WP7 phone was extracted from one of the dump files, then the data integrity of that that dump file would be considered valid. However, as shown by the results from the physical analysis experiments (discussed later) all three dump files yielded the same results, and none of the results yielded was part of the test data loaded onto the WP7 phone, so the data integrity of the dump files remain unknown. Because the data integrity of the dump files is unknown, the results for the Riff Box using the JTAG method of acquisition is inconclusive. With the mixed results of the physical acquisition experiments, the hypothesis H3 of "*The current tools and techniques used for a physical acquisitions of WM phones are not capable of physical acquisitions of WP7 phones*" was undetermined, and hence the research question Q3 of "*Are current tools and techniques used for a physical acquisitions of WM phones capable of physical acquisitions of WP7 phones?*" could not be answered.

The physical analysis experiments applied a series of tools (list in Table 4.14) to each of the dump files acquired from the physical acquisition experiments. The results from the physical analysis experiments were consistent with all three dump files, and showed that none were able to extract any of the test data from any of the dump files. However, because the data integrity of the dump files could not be verified, the results from the physical analysis experiments were inconclusive. Due to the inconclusive results the hypothesis H4 of " *The current tools and techniques used for analysis of physical acquisitions of WM phones are not capable of analysis of physical acquisitions of WP7 phones* " was undetermined, and hence the research question Q4 of "*What forensic data can be extracted from a WP7 phone using physical analysis tools and techniques currently used for WM phones*" could not be answered.

The sub hypotheses H1 - H4 were used to test the hypothesis H0 of "*The current tools and techniques used to extract forensic data from WM phones are not capable of extracting forensic data from WP7 phones*". Even though H3 and H4 were undetermined, H1 and H2 were used to reject the hypothesis H0 since test data was extracted from the WP7 phone. Likewise the sub research questions Q1 - Q4 were used to answer the research question Q0 of "*What forensic data can*

be extracted from a WP7 phone using current tools and techniques used to extract forensic data from WM phones?". Based on the answers from sub questions Q1 and Q2, the research question Q0 can be answered that "User files such as pictures and videos can be extracted from a WP7 phone using XRY". However, because of Q2 and Q3 were unanswered, the answer to Q0 can be considered partially answered.

Though some results from the research were inconclusive, leaving some sub hypotheses undetermined and some sub research questions unanswered, overall the results illustrated the impact that WP7 has on a digital forensic investigation. The majority of the WM forensic tools tested were unable to extract any data from the WP7, both with logical physical methods. The only tool which was able to extract any data from the WP7 was XRY. However XRY was able to extract less data than what could be extract from a WM phone using XRY.

6.2 LIMITATIONS OF RESEARCH

The limitations of the research were identified and discussed Section 3.5 as part of the methodology for the research. Other limitations of the research have resulted from the changes and updates to the WP7 platform, the forensic tools, and the alternative tools which were released during the research.

A limitation of the research was identified by the results of the physical acquisition experiment using the Riff Box. The Riff Box was able to acquire a physical dump of the WP7 phone's memory, however the data integrity of the dump file could not be verified. The results of the physical analysis experiments using three different dump files were unable to confirm the data integrity of the dump files. The data integrity of the dump files being unknown meant that the sub hypotheses H3 and H4 could not be determined and hence the sub research questions Q3 and Q4 could not be answered. One possible way of verifying the data integrity of the dump files is to use a different tool to acquire a dump file and comparing the dump files acquired by the different tools. Another JTAG tool could be used to acquire data from the WP7, or the chip extraction method could also have been used. The chip extraction method is the most forensically sound method of extracting data from the phone's memory. However due to time and

resource constraints, other JTAG or chip extraction tools were not tested during the research.

Another way possible way of verifying the data integrity of the dump file would be to manually reconstruct the dump file as described in Chapter 2. Manually reconstructing the file system from the dump file requires the forensic examiner to manually analyse the dump file. First by reconstructing the partitions contained in the dump file, then reconstructing the file system of each partition, which allows the files contained in each partition to be reconstructed. Should the files be reconstructed successfully, the data integrity of the dump file can be considered forensically sound. Should the file reconstruction be unsuccessful, the process of manually reconstructing the files may reveal errors in the dump file, or information about the dump file such as partition information or encryption used. For the reasons explained in Section 3.5, manually reconstructing the dump file was not done during the research.

6.3 FUTURE RESEARCH

Section 6.3 discusses possible future research both to extend the current research and into other aspects of WP7 forensics.

WP7 was constantly changing during the course of the research. The WP7 phone, the WP7 OS, and some of the WM forensic tools used during the research had been updated with newer versions. Research into the affects of new WP7 phones, new WP7 OS (currently WP7.5), and the new WM forensic tools are possibilities for further research.

An aspect of the research where further research is possible is the physical analysis experiments. The physical dump file was acquired from the WP7 during the research using the Riff Box which implemented the JTAG method. The data integrity of the dump file acquired however could not be verified during the research. Another physical acquisition method such as the chip extraction method may be able to acquire a dump file where the data integrity can be verified. If the dump file acquired using the chip extraction method can be compared with the dump file acquired using the JTAG method, the comparison may point to what caused the differences between the hash values of the dump files acquired using the JTAG method. If the data integrity of the dump file can be verified, then the

results from both the physical acquisition and physical analysis experiments may conclusive enough to verify the sub hypotheses H3 and H4, and answer the sub research questions Q3 and Q4.

Another aspect of the research where further research is possible is to manually rebuild the physical dump file. During the research, only tools were used to analyse the dump files and no manual reconstruction of the dump file was done as manual reconstruction of the dump file was beyond the scope of the research (see Section 3.4.4). Manual reconstruction of the dump file may identify aspects of the dump not verified during the research, such as how files are spread between the phone's memory and the internal SD card, the file system used for each partition, and the compression used in each partition.

The alternative tools discussed in Section 5.4 is also another possibility for further research. The alternative tools are able to extract more data from a WP7 phone than the current WM forensic tools and techniques. However, many issues exist with using alternative tools for a digital forensic investigation. Some alternative tools will only work with certain brand of phone (such as HTC), and some require the WP7 phone to be unlocked and other software such as the WP7 Developer Tools (Microsoft, n.d.-f) may be required. The ability to only run on some phones, unlocking the phone, and requiring specific software may limit the situations where the alternative tools may be used. The forensic soundness of the data extracted using the alternative tools also require research to establish.

6.4 CONCLUSION

The research has focused on extracting data from a WP7 phone using forensic tools and techniques currently used to extract data from WM phones. The results from experiments conducted during the research was reported, analysed and discussed to evaluate the compatibility of current forensic tools and techniques with WP7, and the implications of WP7 for digital forensic investigators.

Chapter 6 concluded the research into the implications of WP7 for digital forensic investigators by reviewing the findings from the research and the implications of the research findings for a digital forensic investigator. The limitations of research and possible areas for further research were reviewed to put the research findings into the context of WP7 and digital forensics

The research findings suggests the majority of the forensic tools currently used to extract data from WM phones are unable to extract any data from WP7 phones with the exception of XRY which is able to extract user media files such as pictures and videos from the WP7. Some of the research findings such as physical acquisition of WP7 and analysis of the physical dump file acquired from WP7 are inconclusive and requires further research.

References

AccessData. (2006). *MD5 Collisions - The Effect on Computer Forensics*

Android. (n.d.). *Android.com*. Retrieved 16 Jun, 2011, from http://www.android.com/

Association of Chief Police Officers. (n.d.). *Good Practice Guide for Computer-Based Electronic Evidence Version 4.0*.

Ayers, R., Jansen, W., Cilleros, N., & Daniellou, R. (2005). *Cell Phone Forensic Tools: An Overview and Analysis*.

Backtrack. (2011). *Backtrack*. Retrieved 18 Dec, 2011, from http://www.backtrack-linux.org/

Breeuwsma, M., Jongh, M. d., Klaver, C., Knijff, R. v. d., & Roeloffs, M. (2007). Forensic Data Recovery from Flash Memory. *SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, 1*(1).

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3 ed.): Academic Press.

Casey, E., Bann, M., & Doyle, J. (2010). Introduction to Windows Mobile Forensics. *Digital Investigation, 6*(3-4), 136-146. doi:10.1016/j.diin.2010.01.004

Cellebrite. (2011). *UFED Ultimate*. Retrieved 11 Nov, 2011, from http://www.cellebrite.com/forensic-products/forensic-products/ufed-ultimate.html

Compelson Labs. (2011). *MOBILedit! - PC Suite for all phones*. Retrieved 16 Jun, 2011, from http://www.mobiledit.com/home.htm

EXIF.org. (2011). *EXIF and Related Resources*. Retrieved 18 Dec, 2011, from http://www.exif.org/

Facebook. (2011). *Facebook*. Retrieved 1 Nov, 2011, from http://www.facebook.com/

FlexiSPY. (2011). *FlexiSpy*. Retrieved 16 Nov, 2011, from http://www.flexispy.com/

Flynn, D. (2010). *Microsoft: "No Windows Phone 7 upgrade for Windows Mobile 6.x devices"*. Retrieved 16 Jun, 2011, from http://apcmag.com/microsoft-no-windows-phone-7-upgrade-for-windows-mobile-6x-devices.htm

Gartner. (2010). *Gartner Says Worldwide Mobile Phone Sales Grew 17 Per Cent in First Quarter 2010*. Retrieved 16 Jul, 2011, from http://www.gartner.com/it/page.jsp?id=1372013

Gartner. (2011a). *About Gartner*. Retrieved 29 Nov, 2011, from http://www.gartner.com/technology/about.jsp

Gartner. (2011b). *Gartner Says Android to Command Nearly Half of Worldwide Smartphone Operating System Market by Year-End 2012*. Retrieved 29 Nov, 2011, from http://www.gartner.com/it/page.jsp?id=1622614

Grispos, G., Storer, T., & Glisson, W. B. (2011). A comparision of forensic evidence recovery techniques for a Windows Mobile smart phone. *Digital Investigation, 8*, 23-36. doi:doi:10.1016/j.diin.2011.05.016

Hengeveld, W. J. (2010a). *Analyzing The WM7 HTC Mondrian Rom*. Retrieved 17 Nov, 2011, from http://itsme.home.xs4all.nl/projects/xda/wm7.html

Hengeveld, W. J. (2010b). *ITSUTILS*. Retrieved 11 Oct, 2011, from http://itsme.home.xs4all.nl/projects/xda/tools.html

Herrera, C. D. (2007, 15/11/2009). *Versions of Windows CE / Windows Mobile*. Retrieved 16 Jun, 2011, from http://www.pocketpcfaq.com/wce/versions.htm

Herrera, C. D. (2008). *ActiveSync 3.x and 4.x Versions FAQ*. Retrieved 16 Jun, 2011, from http://www.pocketpcfaq.com/faqs/activesyncversions.htm

Hess, A. (2010). *DISASSEMBLED: Windows Phone 7, Memory Management and microSD Cards*. Retrieved 18 Dec, 2010, from http://www.theunwired.net/?item=disassembled-windows-phone-7-memory-management-and-microsd-cards

HTC. (2011a). *HTC Smartphones*. Retrieved 12 Nov, 2011, from http://www.htc.com/nz/smartphones/

HTC. (2011b). *Unlock Bootloader*. Retrieved 12 Nov, 2011, from http://htcdev.com/bootloader/

HTC. (n.d.). *HTC - Products - HTC HD2 - Specification*. Retrieved 16 Jun, 2011, from http://www.htc.com/asia/product/hd2/specification.html

IEEE Standards Association. (n.d.). *IJTAG - Internal Joint Test Action Group*. Retrieved 11 Jan, 2012, from http://standards.ieee.org/develop/wg/IJTAG.html

ISO, &. (2010). *9241-210* [Ergonomics of human-system interaction].

Jansen, W., & Ayers, R. (2007). *Guidelines on Cell Phone Forensics*.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*.

Kim, K., Hong, D., & Ryu, J.-C. (2008). Forensic Data Acquisition from Cell Phones using JTAG Interface.

Klaver, C. (2010). Windows Mobile advanced forensics. *Digital Investigation, 6*(3-4), 147-167. doi:10.1016/j.diin.2010.02.001

Markiewicz, J.-K. (2005). *Difference between SmartPhone and the PocketPC*. Retrieved 30 Nov, 2011, from http://social.msdn.microsoft.com/Forums/en-US/windowsmobiledev/thread/8bea7401-d702-4063-8d59-7a95c787c9f2/

Micro Systemation. (2011). *WHAT IS XRY?* Retrieved 16 Jun, 2011, from http://www.msab.com/xry/what-is-xry

Microsoft. (2003). *Microsoft Unveils Windows Mobile 2003 Software for Pocket PCs*. Retrieved 16 Jun, 2011, from http://www.microsoft.com/presspass/press/2003/jun03/06-23mobile2003ppclaunchpr.mspx

Microsoft. (2006). *Database Conversion Wizard Power Toy*. Retrieved 16 Nov, 2011, from http://www.microsoft.com/download/en/details.aspx?DisplayLang=en&id=7846

Microsoft. (2010a). *Microsoft and Partners Unveil Windows Phone 7 Global Portfolio*. Retrieved 2011, 14 Apr, from http://www.microsoft.com/presspass/press/2010/oct10/10-11mswp7pr.mspx

Microsoft. (2010b). *Microsoft Unveils Windows Phone 7 Series*. Retrieved 16 Jun, 2011, from http://www.microsoft.com/presspass/press/2010/feb10/02-15mwc10pr.mspx

Microsoft. (2010c). *Windows Phone Forums - Access to call/SMS/MMS(etc) history*. Retrieved 16 Jun, 2011, from http://social.msdn.microsoft.com/Forums/en-US/windowsphone7series/thread/6b2469b9-0bb6-4503-bc73-364812a1c277/

Microsoft. (2011a). *Messenger*. Retrieved 1 Nov, 2011, from http://explore.live.com/messenger

Microsoft. (2011b). *Windows Phone 7 Secure Digital Card Limitations*. Retrieved 16 Jun, 2011, from http://support.microsoft.com/kb/2450831

Microsoft. (n.d.-a). *Get apps from Marketplace*. Retrieved 16 Nov, 2011, from http://www.microsoft.com/windowsphone/en-us/howto/wp7/apps/find-and-buy-apps-in-marketplace.aspx

Microsoft. (n.d.-b). *Install ActiveSync*. Retrieved 16 Jun, 2011, from http://www.microsoft.com/windowsphone/en-us/howto/wp6/sync/installing-activesync.aspx

Microsoft. (n.d.-c). *Microsoft Office Outlook Hotmail Connector overview*. Retrieved 14 Jul, 2011, from http://office.microsoft.com/en-us/outlook-help/microsoft-office-outlook-hotmail-connector-overview-HA010222518.aspx

Microsoft. (n.d.-d). *Sync files with my phone*. Retrieved 16 Jun, 2011, from http://www.microsoft.com/windowsphone/en-us/howto/wp7/music/sync-files-with-my-phone.aspx

Microsoft. (n.d.-e). *Windows Phone*. Retrieved 16 Jun, 2011, from http://www.microsoft.com/windowsphone/en-ww/default.aspx

Microsoft. (n.d.-f). *Windows Phone Developer Tools 7.1 Beta*. Retrieved from http://www.microsoft.com/downloads/en/details.aspx?FamilyID=77586864-ab15-40e1-bc38-713a95a56a05&displaylang=en

Microsoft. (n.d.-g). *Windows Phone update history*. Retrieved 16 Jun, 2011, from http://www.microsoft.com/windowsphone/en-us/howto/wp7/basics/update-history.aspx

Miller, P. (2010). *Steve Jobs drops knowledge on earnings call: calls out Google and RIM, says 7-inch tablets are 'DOA' (Update: complete Jobs audio!)*. Retrieved 16 Jun, 2011, from http://www.engadget.com/2010/10/18/steve-jobs-drops-knowledge-on-earnings-call-calls-out-google-an/

Mobile Spy. (2011). *Mobile Spy*. Retrieved 11 Oct, 2011, from http://www.mobile-spy.com/support.html

Moore, T. (2006, 26-28 June 2006). *The Economics of Digital Forensics*. presented at the meeting of the Fifth Workshop on the Economics of Information Security, Cambridge, UK.

MSDN. (2009). *Where are SMS messages stored - Windows mobile 6*. Retrieved 16 Jun, 2011, from http://social.msdn.microsoft.com/Forums/en/vssmartdevicesvbcs/thread/afa50ddc-faab-4944-bd95-b16ff3f53a59

MSDN. (2010a). *TexFAT Overview*. Retrieved 11 Jul, 2011, from http://msdn.microsoft.com/en-us/library/ee490643.aspx

MSDN. (2010b). *TFAT Overview*. Retrieved 11 Jul, 2011, from http://msdn.microsoft.com/en-us/library/aa915463.aspx

MSDN. (2011, 23 Sept). *User Experience Design Guidelines for Windows Phone*. Retrieved 1 Nov, 2011, from http://msdn.microsoft.com/en-us/library/hh202915(v=vs.92).aspx

Multi-com.pl. (2011). *Multi-COM*. Retrieved 18 Dec, 2011, from http://www.multi-com.pl/index.php/en_US,details,id_pr,8424,menu_mode,categories.html

Netherlands Forensic Institute. (2007). *TULP2G*. Retrieved 1 Nov, 2011, from http://tulp2g.sourceforge.net/

Notebooks.com. (2010). *A brief history of Windows Mobile*. Retrieved 18 Oct, 2011, from http://notebooks.com/2010/04/12/a-brief-history-of-windows-mobile/

Oxygen Software. (2011). *Oxygen Forensic Suite 2012*. Retrieved 18 Dec, 2011, from http://www.oxygen-forensic.com/en/

Paraben. (2011). *Device Seizure v4.6*. Retrieved 16 Jun, 2011, from http://www.paraben.com/device-seizure.html

Peters, G. (2011). *HTC HD7 Gets Android via Cooked Chinese ROM (Video)*. Retrieved 16 Jun, 2011, from http://pocketnow.com/tech-news/htc-hd7-gets-android-via-cooked-chinese-rom-video

Polimenov, A. (2010a). *Hardware requirements for Windows Phone 7 Part 2*. Retrieved 16 Jun, 2011, from

http://www.silverlightshow.net/items/Hardware-requirements-for-Windows-Phone-7-Part-2.aspx

Polimenov, A. (2010b). *WP7: Hardware requirements for Windows Phone 7 Part 1*. Retrieved 16 Jun, 2011, from http://www.silverlightshow.net/items/WP7-Hardware-requirements-for-Windows-Phone-7-Part-1.aspx

Polimenov, A. (2010c). *WP7: UI Concepts of Windows Phone 7*. Retrieved 16 Jun, 2011, from http://www.silverlightshow.net/items/UI-Concepts-of-Windows-Phone-7.aspx

Ramabhadran, A., &. (2008). *FORENSIC INVESTIGATION PROCESS MODEL FOR WINDOWS MOBILE DEVICES*.

Randolph, N., & Fairbairn, C. (2010). *Professional Windows Phone 7 Application Development: Building Applications and Games Using Visual Studio, Silverlight, and XNA*: Wiley.

Rehault, F. (2010). Windows mobile advanced forensics: An alternative to existing tools. *Digital Investigation, 7*(1-2), 38-47. doi:10.1016/j.diin.2010.08.003

Schapman, J. (2011a). *Registry Editor for Windows Phone 7 Beta Testing*. Retrieved 17 Nov, 2011, from http://forum.touchxperience.com/viewtopic.php?f=20&t=593

Schapman, J. (2011b). *TouchXperience*. Retrieved 31 Jan, 2012, from http://www.touchxperience.com/

Stroh, M. (2010). *Windows® Phone 7 Plain & Simple*: O'Reilly.

Susteen Inc. (2011). *Secure View 3*. Retrieved 18 Dec, 2011, from http://mobileforensics.com/

Thurrott, P. (2010). *Windows Phone 7 Secrets*: Wiley.

Tilly, C. (2007). *A Brief History of Windows CE*. Retrieved from http://www.hpcfactor.com/support/windowsce/

Warren, T. (2010). *Ballmer: Apps written for WP7 work on all Windows Phones, unlike Android*. Retrieved 16 Jun, 2011, from http://www.neowin.net/news/ballmer-apps-written-for-wp7-work-on-all-windows-phones-unlike-android

Warren, T. (2011). *Microsoft responds to HTC HD2 Windows Phone 7 ROMs*. Retrieved 16 Jun, 2011, from http://www.winrumors.com/microsoft-responds-to-htc-hd2-windows-phone-7-roms/

XDA Developers. (2010). *New Update on the Windows Phone 7 ROM Leak*. Retrieved 16 Nov, 2011, from http://www.xda-developers.com/windows-mobile/news-update-on-the-windows-phone-7-rom-leak/

XDA Developers. (2011a). *[BETA][PUBLIC] Windows Phone Device Manager for WP7 [24/01/12]*. Retrieved 31 Jan, 2012, from http://forum.xda-developers.com/showthread.php?t=965788

XDA Developers. (2011b). *Extract SMS on WP7*. Retrieved 17 Nov, 2011, from http://forum.xda-developers.com/showthread.php?t=1072796

XDA Developers. (2011c). *[ROM][MULTILANG] 09.06.11 HD2O© v1.14 WP7 BUILD 7.0.7392.0 NODO COPY&PASTE [online]*. Retrieved 16 Jun, 2011, from http://forum.xda-developers.com/showthread.php?t=953078

XDA Developers. (2011d). *Working App to Backup Windows Phone 7 via ZUNE ANY TIME*. Retrieved 10 Jan, 2012, from http://forum.xda-developers.com/showthread.php?t=1103011

XDA Developers. (2011e). *XPH compression library ported from WP7 (Mango)*. Retrieved 12 Jan, 2012, from http://forum.xda-developers.com/showthread.php?t=1263314

XDA Developers. (2012). *Main Page*. Retrieved 31 Jan, 2012, from http://forum.xda-developers.com/wiki/Main_Page

Yahoo. (2011). *Messenger*. Retrieved 1 Nov 2011, 2011, from http://messenger.yahoo.com/

Ziegler, C. (2010). *Windows Phone 7's microSD mess: the full story (and how Nokia can help you out of it)*. Retrieved 18 Jun, 2011, from http://www.engadget.com/2010/11/17/windows-phone-7s-microsd-mess-the-full-story-and-how-nokia-ca/

Appendices

APPENDIX A: EQUIPMENT SPECIFICATIONS

Window Phone 7 Phone

Manufacturer	HTC
Carrier	T-Mobile
Model	HD7
OS	Windows Phone 7
OS Version	7.0.7392.0
Firmware Revision Number	2250.09.11801.531
Hardware Revision Number	0002
Radio Software Version	5.51.09.11a_22.31.50.09U
Radio Hardware Version	A.12.0.D4
Bootloader Version	1.18.2250.0 (111116)
Chip SOC Version	2.2.5.0
Serial Number	HT0APRY00901
IMEI	354004040040853

Table A1: Windows Phone 7 Specifications

PC1

Manufacturer	Gigabyte
Model	M61PME-S2P
BIOS	F2
OS	Windows 7 Professional 32 Bit Service Pack 1
OS Version	6.1.7601 Service Pack Build 7601
Processor	AMD Phenom 9650
RAM	4GB
Serial Number	unknown
Description	MFIT Lab Standalone PC (PC22)

Table A2: PC1 Specifications

PC2

Manufacturer	Cyclone Computers
Model	DG41TY
BIOS	TYG4110H.86A.0031.2009.0626.1405, 26/06/2009
OS	Windows 7 Enterprise 64 Bit
OS Version	6.1.7600 Build 7600
Processor	Intel Core2 Duo E8400
RAM	4 GB
Serial Number	71866
Description	MFIT Lab PC4

Table A3: PC2 Specifications

PC3

Manufacturer	Cyclone Computers
Model	DG41TY
BIOS	TYG4110H.86A.0031.2009.0626.1405, 26/06/2009
OS	Windows 7 Enterprise 64 Bit
OS Version	6.1.7600 Build 7600
Processor	Intel Core2 Duo E8400
RAM	4 GB
Serial Number	71858
Description	MFIT Lab PC3

Table A4: PC3 Specifications

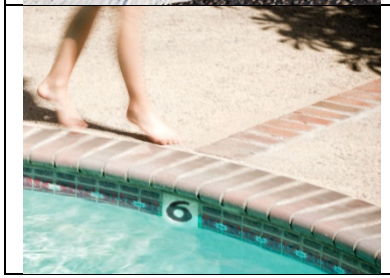
JTAG Riff Box

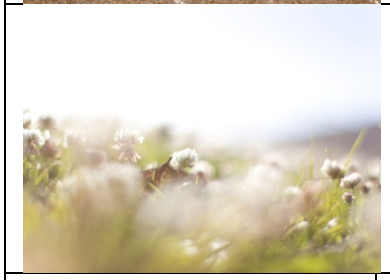
Manufacturer	Rocker Team
Model	Riff Box
Firmware	1.30
Serial Number	FF.679E:0DDB-01F1:1A45
JTAG Manager Version	1.38

Table A5: JTAG Riff Box Specifications

APPENDIX B: DATA EXTRACTED BY XRY

Picture	Name	Type	Size	MetaData	Path	MD5
	sample_photo_01.jpg	Jpeg	116.47 KB	ExifDTOrig: 2010:07:11 15:09:17 ExifDTDigitized: 2010:07:11 15:09:17 ExifDTOrigSS: 05 ExifDTDigSS: 05	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	271028BA951124AE696B33B7E2589261
	sample_photo_02.jpg	Jpeg	75.13 KB	ExifDTOrig: 2010:07:12 13:33:52 ExifDTDigitized: 2010:07:12 13:33:52 ExifDTOrigSS: 00 ExifDTDigSS: 00	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	0F4676FCB918016CE6F617F5535C301A
	sample_photo_03.jpg	Jpeg	35.02 KB	ExifDTOrig: 2010:07:13 14:06:30 ExifDTDigitized: 2010:07:13 14:06:30 ExifDTOrigSS: 00 ExifDTDigSS: 00	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	B5422B02793E06714235FE131EEE87B7
	sample_photo_04.jpg	Jpeg	72.64 KB	ExifDTOrig: 2010:07:14 14:06:18 ExifDTDigitized: 2010:07:14 14:06:18 ExifDTOrigSS: 00 ExifDTDigSS: 00	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	C4FF4AF0AC421F6F40F66672FD3FCB06

Picture	Name	Type	Size	MetaData	Path	MD5
	sample_photo_05.jpg	Jpeg	79.12 KB	Orientation: 1 XResolution: 72.000000 YResolution: 72.000000 ResolutionUnit: 2 SoftwareUsed: Adobe Photoshop CS2 Windows DateTime: 2010:05:14 15:09:54 ExifDTOrig: 2010:07:15 15:09:54 ExifDTDigitized: 2010:07:15 15:09:54 ExifDTOrigSS: 00 ExifDTDigSS: 00 ExifColorSpace: 65535 ExifPixXDim: 800 ExifPixYDim: 600 JPEGInterFormat: 4532 JPEGInterLength: 6264	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	D188A40F81BD1EE6483461627EC00DFF
	sample_photo_06.jpg	Jpeg	192.87 KB	ExifDTOrig: 2010:07:16 10:27:58 ExifDTDigitized: 2010:07:16 10:27:58 ExifDTOrigSS: 00 ExifDTDigSS: 00	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	D8CDB146CF1E16130A347026B7323921
	sample_photo_07.jpg	Jpeg	83.52 KB	ExifDTOrig: 2010:07:17 12:37:06 ExifDTDigitized: 2010:07:17 12:37:06 ExifDTOrigSS: 00 ExifDTDigSS: 00	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	6E97850927AB39102FD5267187441CF4

Picture	Name	Type	Size	MetaData	Path	MD5
	sample_photo_08.jpg	Jpeg	178.74 KB	ExifDTOrig: 2010:07:18 13:39:24 ExifDTDigitized: 2010:07:18 13:39:24 ExifDTOrigSS: 00 ExifDTDigSS: 00	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	636B37FA2F7C36C632B03088FF5F6CB3
	sample_photo_00.jpg	Jpeg	60.36 KB	ExifDTOrig: 2010:07:19 10:10:16 ExifDTDigitized: 2010:07:19 10:10:16 ExifDTOrigSS: 00 ExifDTDigSS: 00	HD7/Storage/Pictures/{4915925E-FB2A-11DE-AE1C-DD6355D89593}	105AB8BD82336AED98B30D4B97E07278
	WP_000000.jpg	Jpeg	725.46 KB	EquipMake: HTC EquipModel: HD7 Orientation: 6 XResolution: 72.000000 YResolution: 72.000000 ResolutionUnit: 2 SoftwareUsed: Windows Phone OS 7.0 DateTime: 2011:10:04 18:29:11 Artist: YCbCrPositioning: 1 ExifISOSpeed: 100 ExifVer: 48 50 50 48 ExifDTOrig: 2011:10:04 18:29:11 ExifDTDigitized: 2011:10:04 18:29:11 ExifCompConfig: 1 2 3 0 ExifFPXVer: 48 49 48 48 ExifColorSpace: 1 ExifPixXDim: 2592 ExifPixYDim: 1944 GpsVer: 2 2 0 0 GpsLatitudeRef: S	HD7/Storage/Pictures/{9ae241c6-e6cc-4080-a2ba-245e0f7c47c5}	EB51215740969F1EFCE6F730484084FD

Picture	Name	Type	Size	MetaData	Path	MD5
				GpsLatitude: 36.000000 50.000000 57.553000 GpsLongitudeRef: E GpsLongitude: 174.000000 45.000000 52.957000 GpsAltitudeRef: 0 GpsAltitude: 0.000000 GpsGpsMeasureMode: 2 GpsGpsDop: 3000.000000 JPEGInterFormat: 684 JPEGInterLength: 18290		
	WP_000001.jpg	Jpeg	885.06 KB	EquipMake: HTC EquipModel: HD7 Orientation: 1 XResolution: 72.000000 YResolution: 72.000000 ResolutionUnit: 2 SoftwareUsed: Windows Phone OS 7.0 DateTime: 2011:10:04 18:29:50 Artist: YCbCrPositioning: 1 ExifISOSpeed: 700 ExifVer: 48 50 50 48 ExifDTOrig: 2011:10:04 18:29:50 ExifDTDigitized: 2011:10:04 18:29:50 ExifCompConfig: 1 2 3 0 ExifFPXVer: 48 49 48 48 ExifColorSpace: 1 ExifPixXDim: 2592 ExifPixYDim: 1944 GpsVer: 2 2 0 0 GpsLatitudeRef: S GpsLatitude: 36.000000 50.000000 57.553000 GpsLongitudeRef: E GpsLongitude: 174.000000 45.000000 52.957000	HD7/Storage/Pictures/{9ae241c6-e6cc-4080-a2ba-245e0f7c47c5}	7D4C9BF31C2D73E44188A68E96BBDDA1

Picture	Name	Type	Size	MetaData	Path	MD5
				GpsAltitudeRef: 0 GpsAltitude: 0.000000 GpsGpsMeasureMode: 2 GpsGpsDop: 3000.000000 JPEGInterFormat: 684 JPEGInterLength: 21889		

Table B1: Pictures Extracted By XRY

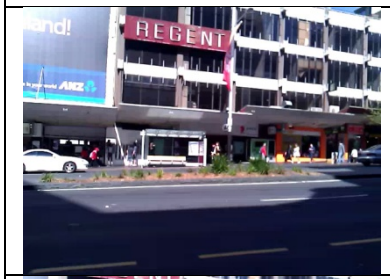
Video	Name	Type	Date	Size	Length	Path	MD5
	WP_000002.mp4	Mp4	7/10/2011 2:35:36am UTC	795.56 KB	3 Seconds	HD7/Storage/Pictures/{9ae241c6-e6cc-4080-a2ba-245e0f7c47c5}	D1442F3FD1F6AE87178ABA44BCCF3699
	WP_000003.mp4	Mp4	7/10/2011 2:35:58am UTC	3.74 MB	14 Seconds	HD7/Storage/Pictures/{9ae241c6-e6cc-4080-a2ba-245e0f7c47c5}	294F7B407D6CA9658E2A9BA7CE6F23AE

Table B2: Videos Extracted By XRY

APPENDIX C: PHYSICAL ACQUISITION

Dump Files Acquired Using JTAG Riff Box

File Name	Size	Date	MD5 Hash	Notes
hd7 2.bin	540,672 KB	10/10/2011 6:09pm	FD0271102F2D69AA3913D365E9DB8E9A	
hd7 3.bin	540,672 KB	10/10/2011 6:51pm	5DB8786460B5078589C124D569E6CC27	
hd7 4.bin	540,672 KB	10/10/2011 7:44pm	BE7F17C50492C9E7DCAEAC94A3990E6F	

Table C1: Dump Files Acquired Using JTAG Riff Box