Mobile Devices:

iPhone Risks and Forensic Tool Capability

BEN KNIGHT
B.C.I.S (AUT, New Zealand)

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

School of Computing and Mathematical Sciences

Auckland, New Zealand
2010

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

I would like to thank everyone that has supported this thesis. I would like to show my gratitude to my supervisor, Brian Cusack from AUT, whose encouragement, guidance and support from beginning to end has made this thesis possible.

I am grateful to everyone that has set aside their time and shared their expertise with me. Bram Mooij, a digital forensic and mobile device expert from the New Zealand Police shared his incredible industry experience at an early stage of this research. His assistance was invaluable in defining research scope and forming an understanding of the technical aspects of this topic. A thank you to my work colleagues Campbell McKenzie and Shane Mahoney from PricewaterhouseCoopers whose ideas and guidance helped refine areas of the research.

I would like to show my gratitude to the companies that provided free access to their software, including: Munro Murdock, Jenni Willis and Gavin Gustafson from Paraben Corporation, Sean Morrissey from Katana Forensics and Tania Pankova from Oxygen Forensic. Research would not have been possible without this resource. I would also like to thank my quality reviewers: Amanda McCracken, David Hills and Gareth Fletcher with helping track down typographical errors.

Lastly, thank you to my Master of Forensic IT colleagues for their continued ideas and enthusiasm. I wish you the best of luck with your own thesis submissions.

Abstract

The research evaluates the capability of software based tools that extract data stored on an Apple iPhone. A literature review is performed covering material on: mobile devices, iPhone, hard disks, networking connectivity, usage environments, data integrity, evidence volatility, data extraction methods and operating systems. Literature shows that iPhone data extraction is complex due to hardware and software limitations. Understanding the capability of the tool used to retrieve data is important in ensuring a sound investigation. Based on literature a research methodology is defined. A descriptive approach is selected. The research process is split into three phases: test iPhone capability, evaluate extraction tools and compare extraction tools. At each phase data is collected, processed and analysed. At the first stage a "catalog" of known data stored on the iPhone is collected. At the second phase an audit "journal" of procedure and "extraction log" of extracted data is collected. At the last phase a sample set of weighted scenarios are used to analyse tool capability. Research findings indicate 12,963 files were extracted from an iPhone and classified in the catalog. Operating system limitations restrict user access to the iPhone file system. A method of opening access, known as jailbreaking, can be used to bypass such restrictions. Of the files in the catalog the highest result obtained by an extraction tool is 797 from Oxygen Forensics Suite 2010 and the lowest result is 178 from Device Seizure. Scenario analysis indicates Oxygen Forensics Suite 2010 works better in case scenarios whereas non-forensic tools have more limitations. Discussion of findings indicates that SQLite and Property List files are common sources of data storage on the iPhone. Analysis into the iPhone operating system shows that Apple has put multiple controls to limit access to the stored data. There is potential for further research in expanding research into extraction tool capability.

Table of Contents

Chapter One - Introduction

Chapter Two - Literature Review

Chapter Three - Methodology

Chapter Four - Research Findings

Chapter Five - Discussion of Findings

Chapter Six - Conclusion

Appendix

List of Figures

List of Tables

List of Abbreviations

API	Application Programming Interface
ASAP	As Soon As Possible
CD	Compact Disc
CEO	Chief Executive Officer
CPU	Central Processing Unit
CSV	Comma Separated Values
dd	Disk Dump
ECID	Exclusive Chip ID
EDGE	Enhanced Data Rates for GSM Evolution
EEPROM	Electrically Erasable Programmable Read-Only Memory
FTK	Forensic Tool Kit
GB	Gigabyte
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HFS	Hierarchical File System
HSDPA	High-Speed Downlink Packet Access
JTAG	Joint Test Action Group
LAN	Local Area Network
MB	Megabyte
MD5	Message Digest
MMS	Multimedia Messaging Service
NAND	Not AND
NSP	Network Service Provider
NZD	New Zealand Dollars
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PLIST	Property List
RAM	Random Access Memory
SD	Secure Digital

SIM	Subscriber Identity Module
SMS	Short Message Service
SQL	Structured Query Language
SSH	Secure Shell
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

Chapter One

INTRODUCTION

1.0 INTRODUCTION

The Apple iPhone is a popular mobile device that has been sold globally to millions of people. Along with local and cellular network connectivity the iPhone also has an internal flash storage disk ranging from 8GB to 32GB. Depending on the requirements of a forensics case the information stored on an iPhone can be highly valuable. Every time a picture is taken on an iPhone the GPS information is embedded as part of the metadata of the file. Email can be setup to constantly push new messages to an iPhone and keep a local copy of the entire message. Third-party applications can download often private information from social networking websites. The flash disk in the iPhone is tightly integrated into all the other internal components and requires high levels of technical expertise to remove. Forensics often relies on being able to remove internal components. Hardware restrictions iPhone require forensic professionals to expand into innovative approaches for retrieving data. The physical removal procedure involves the risk of damaging internal components. The iPhone runs an OS (Operating System) called iOS. The OS is built off Mac OS X. Software access restrictions are built into the OS to prevent access to all the iPhone data.

Chapter one introduces the thesis topic and discusses the format of the following chapters. The problem area and motivation for researching this particular topic are discussed. Chapter one explains why this topic and problem area has been selected for research and why research into iPhone extraction tool capability will benefit forensic professionals. The research question is stated outright to introduce the scope of research prior to a review of literature.

In section 1.1 the problem area is discussed. The problem for this topic comes from limited understanding of tool capability and the need to develop robust expectations of extraction tools. In section 1.2 the motivation for doing this research is discussed. The tightly integrated form factor makes iPhone data extraction more complicated for the forensic professional. Ensuring the correct forensic process is followed ensures sound investigations. The structure of the thesis is discussed in section 1.3. The four main chapters are introduced and summarised. Section 1.4 states the research question and hypotheses that are discussed in greater detail in section 5.1. The research findings from chapter four are summarised in section 1.5.

1.1 PROBLEM AREA

Forensic tools have over the years become the industry standard, such as EnCase and FTK have been heavily scrutinised and validated for use in court. EnCase and FTK do not offer the ability to extract data from mobile devices, such as iPhone or Android devices. Data may still be analysed with these tools. However, successful extraction is a fundamental component to a sound forensic investigation.

An abundance of tools are being released into the forensic market that support the extraction of data stored on an iPhone. Extraction tools position themselves as either forensic or non-forensic. Limited information is provided as to the approach extraction tools use to extract data. The completeness and accuracy of the data that is extracted is often untested and unknown.

1.2 MOTIVATION

The iPhone is a popular smartphone that has been sold by Apple since 2007. 33.75 million units have been reported as being sold (Apple, 2009, p.1). Development into the operating system that runs on the iPhone is rapid and hardware revisions are being introduced to the market every year. The iPhone is popular with a range of people, from consumers to business. Popularity around the iPhone will create a requirement for forensic professionals to extract information from such devices.

The traditional procedure of removing a computer’s internal hard disk, connecting it to a write-blocker and using imaging software to copy a full physical forensic copy cannot be followed with an iPhone because the hardware is tightly integrated and has not been designed for simple removal. In addition to the limited hardware removal capability, the iPhone does not offer external access to the hard disk. The iPhone also has no external storage capability, such as an SD (Secure Digital) card slot.

The iPhone is a feature-rich device. There can be up to 32GB of data stored on an iPhone. The nature of an iPhone is that a user will often store large amounts of personal information on their iPhone. The relevance of personal information may differ in terms of a forensic investigation. In cases where an iPhone is known to have been used to store or transmit information relevant to a case the complete and accurate extraction of that information is critical to the outcome.

Some of the common features of an iPhone that could store relevant information includes: SMS (Short Message Service), call logs, address books, map searches, geo-tagged camera photos, third-party applications, email, calendars and audio recordings. Although the iPhone stores personal information, the ability to extract an entire data set may be restricted.

1.3 STRUCTURE OF THESIS

This thesis is split into five chapters: Chapter Two “Literature Review”, Chapter Three “Methodology”, Chapter Four “Field Findings” and Chapter Five “Discussion of Findings”. The five chapters progress from a review of literature around the topic area to a discussion of the findings from the field work.

Chapter two involves a review of literature in and around the topic of iPhone data extraction. Literature topics reviewed in Chapter two include: mobile devices, small scale digital devices, forensic acquisition, challenges associated with mobile devices, storage hardware, iPhone background, networking, methods of evidence extraction, data validation, Mac OS X and iPhone OS. Chapter two is split into five main sections Mobile Devices, iPhone, Networking, Extraction Tools and Mac OS X Forensics. Chapter two concludes with a summary of problems areas identified in the literature that are discussed earlier in the chapter.

Chapter three builds on the literature review in chapter two and discusses a proposed methodology based on findings in the literature. Chapter three begins with a review of five similar studies. These similar studies are on the topics of: HFS data recovery, forensic acquisition of mobile devices, legal, flash memory data recovery and mobile device analysis. Chapter three looks at the research design by first summarising the review of similar studies and then a review of problem areas. These are problem areas identified in literature. The research question is derived and with the research question are a series of hypotheses that will be tested after findings are collected. Four research phases are developed in chapter three and the whole research process is mapped out into a data map. Data requirements for the collection, processing and analysis of data are discussed in chapter three. The chapter concludes by discussing the expected outcomes based on the literature.

The methodology proposed in chapter three is followed in chapter four and research findings collected. Research findings are reported on in chapter four. The chapter begins by firstly clarifying changes made to the methodology specified in chapter three in the collection, processing and analysis of data. The research findings are reported based on the three research phases. Chapter four includes an analysis of the research that discusses the forensic procedure of the extraction process followed and the descriptive approach in reporting the findings. The final part of chapter four is a summary and visual presentation of the findings as reported earlier in the chapter.

The final chapter, chapter five, is a discussion of the findings reported on in chapter four. The chapter begins by answering the research question and sub-questions first identified in chapter three. The three hypotheses are tested and evaluated. Discussion in chapter five is split into five sections: iPhone software, jailbreaking, maintaining evidential integrity, research data and case environment. The chapter concludes the findings discussion by recommending possible areas for further research.

1.4 RESEARCH QUESTION AND HYPOTHESES

The research question is derived from the literature reviewed in chapter two. The research question and sub-questions are identified in section 3.2.3. The main question for this research is: “What is the capability of extraction tools for the extraction of information stored on an iPhone?” First identifying iPhone capability and then evaluating that against tool capability answers the research question. The two components used to answer the research question are a log of all the collected hash values and an analysis of a sample set of case scenarios. Four sub-questions are also derived from literature and first identified in section 3.2.3. The sub-questions for this research relates back to the more high-level main question. The first sub-question is: “What information is stored on an iPhone?” The second sub-question is: “What information can be extracted?” The third sub-question (child to sub-question 1) is: “What information is input by the user?” The fourth sub-question (also child to sub-question 1) is: “What information is system generated?”

Three hypotheses are developed for testing as part of this research. Like the research question, the hypotheses are assertions derived from literature. The hypotheses are first identified in section 3.2.4 and tested in section 5.1.2. The three hypotheses are labelled H1 to H3. H1 is “Extraction tools obtain a full physical copy”, H2 is “Extraction is complete, accurate and repeatable” and H3 is “Jailbreaking doesn’t modify user data”.

1.5 RESEARCH FINDINGS

Research findings are the result of field work being performed based on the methodology discussed in chapter three. The research findings reported in chapter four are split by the three research phases first identified in section 3.2.5. The three research phases are: Phase One: Test iPhone Capability, Phase Two: Evaluate Extraction Tools and Phase Three: Compare Extraction Tools.

In phase one data is collected as part of the catalog. The two sources of catalog data are an iTunes backup and a dd (Disk Dump) disk image. An iTunes backup is a logical extract of the iPhone files and a dd disk image is a bit-by-bit of the entire disk. A dd disk image is more complete but requires jailbreaking the iPhone.

Results indicate that software restrictions limit the ability to identify iPhone capability. A software restriction that limits access to the file system is the sandboxed environment that the iPhone runs in. There are two users associated with the iPhone, the *root* and *mobile* users. The *root* user has full access to the iPhone file system but the iPhone must be jailbroken before this user can be activated for use. The *mobile* user has restricted access to the file system. The mobile user can access third-party applications and a limited portion of the logical files stored on the iPhone.

Files extracted as part of the iTunes backup and dd disk images are hashed. From the iTunes backup 343 files are hashed and from the dd disk image 12,963 files are hashed. The dd disk image also includes unallocated space on the disk. The iTunes backup grew to a size of 7.4MB and the dd disk image to a size of 15.33GB. An iTunes backup is stored in a series of “.mddata” and “.mddata” files and the dd disk image is stored as a single file in dd format. There are 16 “importance rating” classifications developed as part of the catalog. The classifications have an accompanying rating from 0 to 2. A rating of 0 indicates low importance and 2 indicates high importance.

Phase two involves collecting a journal and extraction log. There are 11 findings identified as part of the journal. The journal contains three columns: date, action and result (Appendix C). Journal findings include issues and procedures identified during field work. Journal findings include: firmware downgrade blocking, write-blocking, radio blocking, security mechanisms, iTunes versions, storage medium and iTunes background processes. Firmware downgrade restrictions limit the firmware versions that can be restored onto an iPhone. Due to hash signing, only the current version of iOS can be restored onto an iPhone 3GS or iPhone 4. Results indicate that no viable write-blocking method could be identified. However, write-blocking may be possible. Radio blocking is possible by enabling the airplane mode on the iPhone. PIN code and encryption security mechanisms aren’t an issue with logical extraction.

The second source of data for phase two is the extraction log. MD5 hash values and file names are generated for the catalog and using the extraction tools being evaluated. Seven extraction tools are evaluated, with the number of hash values calculated ranging from 178 to 797 files. The smallest extract of 5.5MB was obtained using MobileSyncBrowser and the largest of 4.2GB was obtained by using Oxygen Forensics Suite 2010. Results indicate that forensic tools extract more files than non-forensic tools. The number of files extracted doesn’t vary significantly whether the iPhone is jailbroken or not.

The final phase involves comparing the extraction tools with a scenario analysis. Five scenarios are developed for comparison. The five scenarios are based on five main components that are common in forensic cases. The scenarios are a sample of potential scenarios. The five main components are: archiving, email extraction, document extraction, speed of extraction and tracking. Each scenario is evaluated against 17 requirements. The requirements are weighted on a rating between 0 and 3 based on the scenario, 0 being unimportant and 3 being essential. Oxygen Forensics Suite 2010 scored consistently high in all scenarios. MobileSyncBrowser and iPhone Explorer (both non-forensic tools) scored consistently low. No tool scored 100% in any of the scenarios.

1.6 CONCLUSION

The iPhone is a powerful mobile device. Integrated storage adds complexity to data extraction for forensic professionals as typical methods of removing the hard disk and attaching it to a copying device is not a simple procedure. The physical restrictions require tools to leverage software to extract the iPhone data. The capability of extraction tools depend on the access provided by the iPhone software and the extraction methodology. Expectations of extraction tools are that the tool implements common forensic functionality, such as data integrity checks, accuracy checks and validated storage. Forensic extraction tools implement common forensic functionality whereas non-forensic tools do not.

Chapter one has introduced the problem area and discussed the motivations for selecting this topic. Software restrictions and access limitations that limit a tool’s ability to extract data from an iPhone are discussed. The iPhone is a closed device, both from a hardware (no removal storage) and software respective (locked down operating system). The structure of the thesis is discussed and following chapters introduced that will follow the research process. The research question and hypotheses are stated outright to ensure context is defined at an early stage of research.

Section 1.1 discussed the problem area of this topic. The problem area includes the limitations that restrict forensic professionals from using common forensic methodologies. The requirement to use alternative methodologies means that capability of tools must first be established. The motivation for this research is discussed in section 1.2. The popularity of the iPhone and complexity of extracting data provide the motivation for researching this topic. Section 1.3 outlines the structure of the thesis. Section 1.4 states the research question and hypotheses that are discussed later in the thesis in section 5.1. Section 1.5 is a summary of research findings reported in chapter four later in the thesis.

Chapter Two

LITERATURE REVIEW

2.0 INTRODUCTION

Computers in the 1940s were the size of a large room and consumed as much power as several hundred modern personal computers (Penn Computing, 2010). A mobile device can perform many of the same tasks as a personal computer with a greater mobile form factor. An emerging subcategory of mobile devices is smartphones. Smartphones are hybrid device between a cellular phone and PDA (Portable Digital Assistant) (Punja & Mislan, 2008, p.1). Smartphones can be used to perform a wide range of business tasks and have capabilities approaching a desktop PC. Tasks a mobile device can do include those typical of a cellular phone, such as: calling and SMS (Short Message Service) messaging as well as personal computer tasks, such as: email, web browsing and listening to music. The Apple iPhone is a smartphone. Time Magazine named the iPhone invention of the year in 2007 (Grossman, 2007). The iPhone was first introduced to the public in 2007 by Steve Jobs, the CEO of Apple (Honan, 2007) and overtook Microsoft's smartphone market share in 2009 (Slivka, 2010).

Literature will be reviewed in chapter two to form a contextual basis for the research as a whole. Literature on several topics that relate to the iPhone forensics will be reviewed. The first area literature has been selected from is within the topic of mobile devices. Literature on mobile devices helps identify what data can be extracted from an iPhone and the tested methodologies for extraction of data. SIM (Subscriber Identify Module) cards are another area a forensic professional can find digital evidence. There are challenges involved with performing a robust forensic examination on a mobile device. Limitations with extraction tools make it difficult for an examiner to create a forensic copy of a mobile device while maintaining data integrity. Section 2.2 builds a timeline of the iPhone hardware and software technical changes since the first release in 2007 until April 2010 (the iPhone 4 had not been released at the time of writing). The iPhone exists in multiple environments: the physical environment, information systems environment and end user environment. These environments are defined in section 2.2.1.

The iPhone not only stores data but can also transmit it wirelessly over wireless, Bluetooth and 3G. The iPhone has hardware chipsets that allow it to support cellular communication protocols and wireless communication protocols. Section 2.3.1 discusses the communication protocols supported by the iPhone and compares them to the communication protocols used by cellular network providers in New Zealand. The iPhone can wirelessly transmit data to a cellular provider. As a result of the communication between the iPhone and cellular provider the cellular provider may store relevant digital evidence. As part of the imaging procedure of a mobile device, wireless communication should be blocked so changes can't be made to the data stored on the device. The iPhone supports a feature that Apple calls "remote wipe". Remote wipe allows a remote user to send a command to the iPhone instructing it to erase all data stored on the device using the MobileMe website, an iPhone application or Microsoft Exchange Server Management Console.

Section 2.4.1 discusses Brothers (2009) research on the five methods of extraction. The lower-level methods are less complex for a forensic examiner to perform but are less forensically robust as data integrity can't be maintained. The advantages and limitations of each method of extraction are discussed. Different methodologies for the testing and validation of extraction tools are reviewed in section 2.4.3 Finally, section 2.5 reviews literature on Mac OS X forensics. Apple based the operating system for the iPhone off Mac OS X so the iPhone OS and Mac OS X systems share similarities. The relationship between iPhone OS and Mac OS X means understanding Mac OS X forensic tools can assist forensic professionals with the extraction of data from an iPhone.

2.1 MOBILE DEVICES

Microsoft (2010, p.8) defines a mobile device as “A small computing device that is easily portable and can be used in various environments”. There are sub-classifications of mobile devices including: calculators, pagers, PDAs (Personal Digital Assistants), handheld gaming consoles, GPS (Global Positioning System) navigation, digital cameras, eBook readers, cellphones and smartphones.

The iPhone is a smartphone. A smartphone is a hybrid of a cellphone and PDA. Punja & Mislan (2008, p.1) states “Essentially, a mobile device can do much of what a computer or laptop can do, just on a smaller scale”. Smartphones are capable devices. Research into mobile device forensics has grown over recent years as researchers see the value in data stored on a mobile device.

2.1.1 Forensic Evidence on Mobile Devices

Punja & Mislan (2008, p.3) outline some of the types of evidence that can be extracted from a mobile device. The types of evidence outlined in the article include data found on a cellphone, including: contacts, call history and SMS (Short Message Service) messages as well as data found on a PDA, including: audio files, email and Internet history. The iPhone stores data that could be used as digital evidence. The difficult part of getting a forensic copy of the evidence stored on the iPhone for analysis is in the extraction as tools are currently limited to extracting a logical copy of the data.

A fundamental component for cellular communication of a smartphone is the SIM card. Forensic examination of SIM cards is not new as SIM cards have been used in cellphones for a long time but it’s still relevant for the iPhone as information can be stored on the SIM card. Casadei, et al., (2006, p.1-21) discuss a forensic tool for examining SIM cards called SIMbrush. Casadei, et al., (2006) outline the evidence that can be extracted from a SIM card as well as the limitations of SIM card forensics.

2.1.2 Challenges

Forensic professionals attempting to extract evidence from a mobile device are often faced with challenges. Challenges arise because of the small form factor that makes mobile devices so portable. “The cumulative experience of building several prototypes leads us to believe that mobile devices in the future will continue to integrate more function and cost less” (Narayanaswami, 2005, p.4). Unlike forensic examinations of a desktop or laptop personal computer where the hard disk is easily removable the storage components used in a mobile device are more difficult to remove as they’re soldered onto the logic board. Maintaining data integrity of a forensic copy is difficult when the storage components can’t be physically removed (Dankner, 2009, p.3). If the storage components can’t be removed for a forensic copy to be obtained another method of extraction needs to be used. A forensic copy of the internal flash memory could be made to removable storage if the mobile device supports removable media (Me & Rossi, 2008, p.2).

2.1.2.1 Storage

Manufacturers design mobile devices to fit hardware components in a small space. Fitting the hardware components in tightly means it’s more difficult to remove hardware components. A difference between a personal computer and a mobile device is the type of disk used for storage. In a personal computer, magnetic hard disks are used because they’re cost effective, provide a good level of performance and can store a lot of data. Modern mobile devices don’t use magnetic hard disks because they contain moving parts that can cause damage if dropped or similar (Figure 2.1). Flash memory stores data by storing an electrical charge in a floating gate of a transistor (Breeuwsma, et. al, 2007, p.1). Solid-state storage doesn’t involve moving parts and is more suitable for mobile devices.

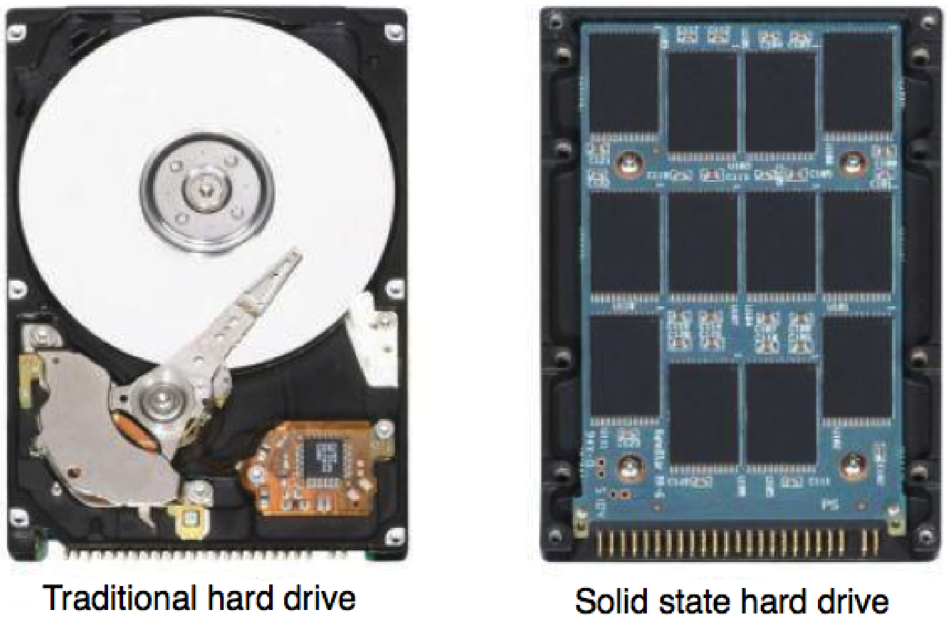

Figure 2.1: Magnetic Hard disk & Solid State Disk (PCTechGuide, 2009, p.1)

2.1.2.2 Maintaining Integrity

There are different techniques for maintaining integrity of data copied from a mobile device. Malinowski & Noble (2007, p.100) discusses an analysis of the best practices associated with maintaining integrity of digital evidence. The research by Malinowski & Noble (2007) isn’t specific to mobile devices but the outcomes are still valid. Calculating the hash value of copied files is a common way for forensic professionals to prove data integrity has been maintained. Calculating a hash value is only a valid approach if the procedure for extraction doesn’t involve making any changes to the data.

Danker et al. (2009, p.1) states, “Minimal research has been performed on how mobile phone forensic tools report hash values for individual data objects”. Danker et al. (2009) found that with MMS (Multimedia Messaging Service) messages hash values will change if transmitted. Another investigation technique that is known to be difficult on mobile devices is disk imaging. Danker et al. (2009) followed a simple but effective methodology to establish whether they could trust the hash value of objects transmitted over different mediums. The first step was to calculate the initial MD5 (Message Digest) hash of the file. They then sent the file over the transmission medium (e.g. MMS) and then recalculated the MD5 hash value to see if it had changed from the first value calculated. The methodology used by Danker et al. (2009) is based off previous research by Ayers et al. (2007) performed two tests as part of their research on data integrity. The first test involved checking the consistency of hashing by software tools over a whole case and the second test involved tested hashing individual objects to look for inconsistencies.

Ridder (2009, p.1-91) discusses the potential for vulnerabilities in the imaging software to allow someone to hide the data they don’t wish to be found by forensic professional. Forensic tools should be tested by forensic professionals prior to being used on a case.

2.2 IPHONE

The iPhone was first announced by Apple at Macworld 2007 and released to the public in the United States in June 2007 (Lurie, 2007). At the release of the iPhone, queues of people lined up for days so they could be the first to own one. The original iPhone was released locked to the AT&T cellular network and only supported EDGE (Enhanced Data Rates for GSM Evolution) networks and not the faster 3G (IMT-2000) technology.

Since the release of the original iPhone (also known as the “iPhone 2G”) there have been two revisions to the hardware. The first upgrade was released in July 2008 named the iPhone 3G (Palmer, 2008), just over a year after the release of the original iPhone. The major hardware improvements in the iPhone 3G were support for 3G, GPS navigation and increased Flash memory storage from 8GB to 16GB. The iPhone 3G was the first iPhone to be officially sold outside the United States. Apple announced they would be shipping the iPhone 3G to 22 countries, including New Zealand (Vodafone Group, 2008).

The third and most recent hardware revision was released in July 2009 (Sande, 2009), a year after the iPhone 3G called the iPhone 3GS. The ‘S’ stands for speed. The iPhone 3GS hardware upgrade introduced a 3-megapixel camera with video support, a faster processor and more RAM for improved performance.

As well as the three generations of iPhone hardware, Apple has also continued to update the firmware on the iPhone (Table 2.1). The first iPhone was released with version 1.0 of the firmware. Every hardware revision of the iPhone has been accompanied with a major firmware release. The first version of the firmware was released with a suite of applications developed only by Apple, including a web browser, music player, calendar and maps. There have also been minor firmware releases that have allowed Apple to deploy bug fixes and new features.

Despite the iPhone being locked to a particular cellular provider in many countries and restricted so only Apple approved applications are allowed to be installed on the device a determined hacker community have managed to find ways to unlock the iPhone so it doesn't have to run on a particular cellular provider's network and non-Apple approved applications can be installed. The iPhone can be unlocked ("jailbroken") by installing a modified firmware. Modifying the software on the iPhone to run on any network is called "unlocking" and allowing non-Apple approved applications is called "jailbreaking". "The term jailbreaking originates from a Unix practice of putting services in a restricted set of directories called a jail" (Zdziarski, 2008, p.10). As unlocking and jailbreaking works by modifying the software, every new firmware release by Apple requires the hacker community to once again spend time modifying the new firmware.

Device	**Firmware**	**Release Date**	**Key Features**
iPhone	1.0 – 1.1.5	29 June 07	▪ First iPhone released ▪ Available in the United States only ▪ Locked to the AT&T network ▪ Supported EDGE data only ▪ No support for third-party applications
iPhone 3G	2.0 – 2.2.1	11 July 08	▪ Hardware upgraded to support 3G ▪ Hardware upgraded to support GPS ▪ Availability opened up to 22 countries, including New Zealand ▪ Support for Microsoft ActiveSync ▪ Support for remote wipe

			▪ Introduction of AppStore, Apple approved third-party applications allowed
iPhone 3GS	3.0 – 3.1.3	17 June 09	▪ Improved performance with upgraded processor and RAM ▪ Upgraded camera from 2 megapixels to 3 megapixels and support for video recording ▪ Tethering support over USB or Bluetooth ▪ Support for cut, copy and paste
iPhone 4	4.0	n/a	▪ Beta announced April, release scheduled in June for iPhone and September for iPad ▪ Support for multitasking of applications

Table 2.1: iPhone Technical Release Timeline

2.2.1 Environments

The iPhone is comprised of three layered environments. The environments are classified as: physical, information systems and end user. The physical layer includes the hardware components that are used in the iPhone. The physical layer includes hardware components, such as the processor, flash memory and RAM (Figure 2.2). The user's information is stored as data at the information systems layer. A forensic examiner can extract the data stored at the information systems layer for analysis. The highest layer is the end user. The end user enters the information that is stored as data in the information systems layer. Information may also be entered by other means, such as the cellular chipset which may store the last known cellular location.

2.2.1.1 Physical

The physical environment defines the hardware components used to make up the iPhone. Apple doesn't typically design and manufacture hardware components used in the products they produce, except for the new Apple A4 CPU (Central Processing Unit) used in the iPad (Apple, 2010). Instead Apple purchases components that fit the requirements of their product from other manufacturers (Figure 2.2). Having an understanding of the iPhone storage hardware is comparable to knowing what make and model hard disk a personal computer has in it and the controller interface used to transfer data between the hard disk and other components in the computer.

Understanding the hardware components used in a device helps forensic professionals choose an appropriate extraction method.

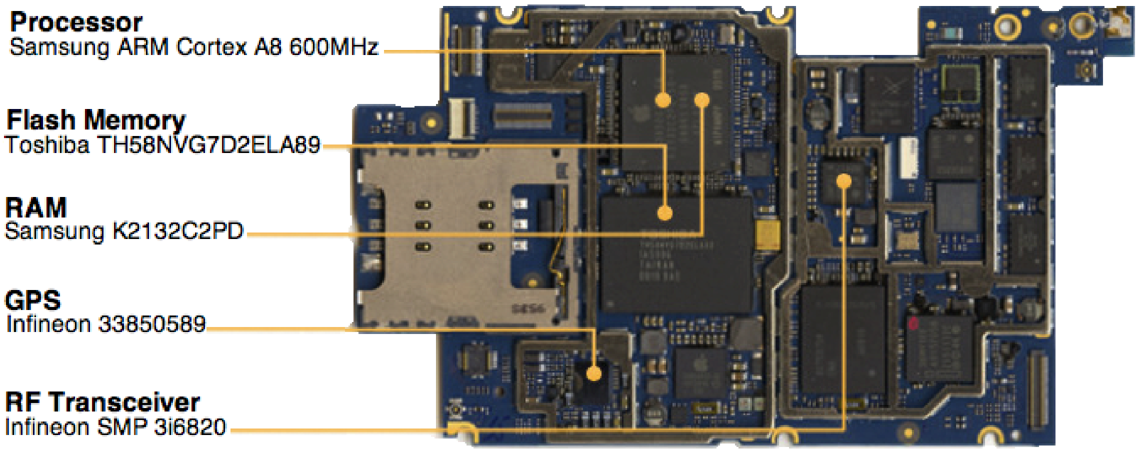

Figure 2.2: iPhone 3GS Logic Board (iFixit, 2010, p.2)

2.2.1.2 Information Systems

A layer up from the physical environment is the information systems layer. The information systems layer defines everything that happens with the software on the iPhone, from the low-level operating system functions to data storage. Apple have developed the iPhone OS to provide seamless interaction for the end user between information systems and the physical environment. The information systems collect and store data such as GPS coordinates, web browsing activity and SMS communication. The physical environment offers forensic professionals options for data extraction, and the information systems layer, offers forensic professionals data for analysis (Dankner, 2009, p.2).

2.2.1.3 End User

The highest-level environment is the end user environment. The end user environment layer defines the real world situations where the iPhone is used. The iPhone is a diverse mobile device that has seen popularity in business and home environments. However, the iPhone isn't built strong enough to be used in tough environments, such as manufacturing or construction. Data stored on the iPhone is either user generated or system generated. The end user layer defines data input by the user. An example of user input data is the content of a text message. In comparison, the timestamp information stored with a text message is system generated. User generated data is often stored on the iPhone for an unknown period of time. The data can still be accessible when even the user believes that the data has been deleted.

2.3 NETWORKING

The iPhone is usually connected to a network either through a cellular provider or a local network. The networking features of the iPhone pose a risk for forensic professionals as network connectivity can allow remote sources to tamper with the data on the device. Evidential information can be stored at the cellular provider. There is no guarantee that evidence stored by a cellular provider is complete and accurate.

2.3.1 iPhone Network Connectivity

Like many mobile devices the iPhone comes with multiple hardware components that support different networking protocols. Each protocol is used for a different purpose. The hardware components used in the iPhone can be split into two distinct categories: cellular and wireless. Cellular protocols are used to enable the iPhone to communicate with the cellular provider. Wireless protocols are typically used for personal networking, such as connecting to a WLAN (Wireless Local Area Network) or using a Bluetooth headset. Cellular protocols have greater range of distance as they're designed to provide a user with a constant connection even if they're moving around or are not in a common location to them. Wireless protocols however have a much shorter range but often offer higher throughput speeds. Wireless protocols are designed to provide the user with the flexibility to access a LAN (Local Area Connection) as they would on their personal computer or enable them to use to wireless peripherals.

Apple has continued to upgrade the hardware used in the iPhone and improved the amount of support for network protocols. The original iPhone was released locked to the AT&T network in the United States so the hardware components only needed to support the GSM (Global System for Mobile Communications) and EDGE protocols that the AT&T network uses. However, the announcement that the iPhone 3G would be shipped to more countries and used on different networks meant that Apple had to add support for additional protocols. The major upgrade in the iPhone 3G network protocols was support for UMTS (Universal Mobile Telecommunications System) and HSDPA (High-Speed Downlink Packet Access) (Table 2.2).

Device	Cellular Protocols	Wireless Protocols
iPhone	GSM/EDGE (850, 900, 1800, 1900MHz)	Wi-Fi (802.11b/g) Bluetooth 2.0 + EDR wireless technology
iPhone 3G	UMTS/HSDPA (850, 1900, 2100MHz) GSM/EDGE (850, 900, 1800, 1900MHz)	Wi-Fi (802.11b/g) Bluetooth 2.0 + EDR wireless technology
iPhone 3GS	UMTS/HSDPA (850, 1900, 2100MHz) GSM/EDGE (850, 900, 1800, 1900MHz)	Wi-Fi (802.11b/g) Bluetooth 2.1 + EDR wireless technology

Table 2.2: Network Protocols Supported by the iPhone

In New Zealand there are three cellular network providers: Vodafone, Telecom XT and 2degrees. Vodafone is the official retailer of the iPhone in New Zealand. Vodafone’s slower 2G network uses GSM at 900MHz in most areas and 1800MHz in high demand areas, such as shopping smalls or central business districts. Vodafone also has a 3G network that uses UMTS and HSDPA for data transmission at 2100MHz in most areas but they’re starting to deploy 900MHz as it has better range (Vodafone, 2009). The iPhone does not support all the different frequency bands used by Vodafone (Table 2.3). The original iPhone doesn’t support 3G due to the lack of a UMTS/HSDPA chipset. However, even the iPhone 3G and iPhone 3GS don’t support UMTS/HSDPA at 900MHz so if an iPhone attempts to connect to one of these cellular towers it will drop down to GSM at slower 2G speeds. Vodafone runs two separate networks, a GSM 2G network and a UMTS/HSDPA 3G network. The two Vodafone networks provide redundancy if one network goes down.

Telecom may not be the official retailer of the iPhone but the iPhone 3G and 3GS both work on the XT network. The iPhone 3G and 3GS work because the XT network uses the same 3G technology as Vodafone however at a different frequency band. The XT network uses UMTS/HSDPA at 850MHz in most areas to provide wider coverage and 2100MHz in higher density areas. Like on the Vodafone network the iPhone 3G and 3GS support 2100MHz but on the XT network the iPhone 3G and 3GS also supports 850MHz, unlike 900MHz used by Vodafone. Support for UMTS/HSDPA 850MHz means the iPhone is more likely to have better coverage when connected to the XT network. XT is a purely 3G network so there's no 2G network to failover to if the 3G network goes down or the network is out of range.

The third cellular network: 2degrees, is the newest provider on the market. 2degrees started providing cellular service to customers in August 2009 (3 News, 2009) and are known for providing cheaper callings and SMS rates. Like Vodafone, 2degree also uses GSM at 900MHz and 1800MHz but is the only provider to support EDGE for data transmission. 2degrees has an agreement with Vodafone that if a 2degrees customer is outside the range of a 2degrees cellular tower the customer can seamlessly connect to the Vodafone network at no additional cost to the user. 2degrees is upgrading their network to support 3G speeds that uses UMTS/HSDPA technology (2degrees, 2009).

Network	Protocol / Band Frequency
Vodafone NZ	GSM 900MHz (2G) GSM 1800MHz (2G) UMTS/HSDPA 900MHz (3G) UMTS/HSDPA 2100MHz (3G)
Telecom XT	UMTS/HSDPA 850MHz (3G) UMTS/HSDPA 2100MHz (3G)
2degrees	GSM 900MHz (2G) GSM 1800MHz (2G) EDGE (2.5G) UMTS/HSDPA 2100MHz (3G)

Table 2.3: New Zealand Cellular Provider Protocols and Frequency Bands

2.3.2 Volatility of Cellular Provider Evidence

Not only can valuable evidence be stored on the iPhone itself but due to the connectivity mechanisms discussed in section 2.3.1 there can also be evidence stored by the cellular provider. Any situations where the iPhone has had to communicate with the cellular provider could be an instance where evidence could be held at the cellular provider. Such communication could include: MMS, call history and Internet usage (Shafik, et. al, 2008, p.11). Evidence may have been erased off the iPhone or the examiner may be using an extraction method that could miss some evidence. The cellular provider could be a source of evidence in addition to evidence obtained from the iPhone. Obtaining evidence from a cellular provider may be outside any existing legal allowances, such as a warrant and may require an additional warrant be served (NIJ, 2007, p.10). Another limitation of digital evidence stored by the cellular provider is that it may not be complete or accurate. Information stored by the cellular provider is managed by the cellular provider who has no commitment to ensuring their data is unchanged. Time is a constraint when working with digital evidence, especially evidence stored by the cellular provider.

When Apple released the 2.0 version of the firmware for the iPhone one of the major features introduced was remote wipe. Remote wipe allows the owner of an iPhone to send a command to their device to tell it to securely erase the data off the device (Apple, 2009). The command is sent over the cellular network so the owner doesn’t need to have physical access to the iPhone to run the command. Remote wipe is designed to allow the owner to wipe their personal information off their phone if they have lost it or it has been stolen. The time it takes to wipe an iPhone depends on the model. The iPhone 3GS can be wiped within minutes because it supports hardware encryption and therefore only needs to delete the encryption keys. The original iPhone or iPhone 3G write zeros over the whole disk and this can take several hours (Frakes, 2009).

When acquiring an iPhone there is the possibility someone will attempt to interfere with the investigation by activating the remote wipe feature. Fortunately the remote wipe feature can only be activated as long as the iPhone can communicate with the cellular provider. The connection to the cellular provider can be broken by removing the SIM card, putting the device into a Faraday bag or turning off the device (Gratzer, et. al, 2006, p.5). The latter option may not be the best option depending on the situation because turning off the device involves interacting with the device and the battery can’t be easily removed from an iPhone. Turning off the device would delete any potential evidence stored in memory (Dankner, 2009, p.8). The iPhone supports powering through a USB cable connected to a computer or mains power.

2.4 EXTRACTION TOOLS

Extraction tools can be either hardware or software based and are used to extract data from a device. Extraction tools often perform the extraction process in different ways. The procedure that a tool uses is important in forensics because the data extracted must be used as evidence in court. For data to be used as evidence a forensic professional must be able to show the data has not been altered during the extraction process. Data that can be used as evidence is said to be “forensically sound” (Casey, 2009, p.49-50).

2.4.1 Methods of Extraction

Brothers (2009) outline five levels of extraction from mobile devices (Figure 2.3). The bottom layer is considered to require the least amount of technical expertise however is the least forensically sound approach. The top layer is the most complex to perform correctly but yields a forensically sound disk image.

The bottom layer of the model is labelled “manual”. A manual approach involves manually reviewing a mobile device by using it as the user would by pushing buttons and navigating the GUI (Graphical User Interface). Manual extraction may be simple to perform and possible on almost all devices but manual extraction is slow, easy to miss certain areas (such as deleted items) and not at all forensically sound. Using a device makes changes to the data and therefore can’t be trusted as evidence. Manual extraction is only suitable in situations where integrity of the data isn’t important or in a life-threatening situation when time is extremely limited.

The layer above manual extraction is labelled “logical”. The logical layer involves copying the logical files to another location. Logical extraction is quick to perform and still doesn’t require a high level of technical expertise. The method is repeatable however still can’t be considered forensically sound as changes may be made to the data on the device during the coping process (Westman, 2009, p.7). Logical extraction is the most common method for extracting information from an iPhone as there is an abundance of tools that can do it (Hoog, 2009).

The next three layers are all physical extraction methods. Physical extraction is more technically involved but provides more forensically sound results. The first physical layer is labelled “hex dump”. Hex dumping involves uploading a modified bootloader to the device and having the device boot off the new bootloader. The bootloader can create an environment suitable for a forensic extraction. The environment can be used to access disks in read-only mode and therefore a forensically sound bit-by-bit copy of the data can be made that includes areas a logical copy would miss, such as deleted data. Hex dumping a mobile device can be considered similar to booting a computer off a boot CD and acquiring an image of the hard disk while the computer is running. Brothers (2009, p.8) state hex dumping is the fastest growing segment in the cellphone forensic tool marketplace. Unfortunately despite the huge advantages of hex dumping most implementations are complex and require a high level of technical expertise. Hex dumping for data extraction came out of the hacker community (Brothers, 2009, p.8).

The next layer up from Hex Dump is also a physical extraction method. The physical method is labelled “chip-off” and involves physically removing the flash chip so the chip can be read (Figure 2.3). The chip-off method is potentially dangerous as it involves de-soldering internal hardware components that could be permanently damaged and destroy any evidence. The chip-off method is forensically sound and is the most likely approach to retrieve all the data on the device. The chip-off method is where we will be in three years (Brothers, 2009, p.9).

The final extraction method “micro read” requires the most technical expertise to perform and is also forensically sound and will work on almost all chips, including damaged chips. The micro read method involves using an electron microscope to view the state of the memory on the device. Due to the high cost involved with the microscopic reading method its best suited to high value devices or damaged chips.

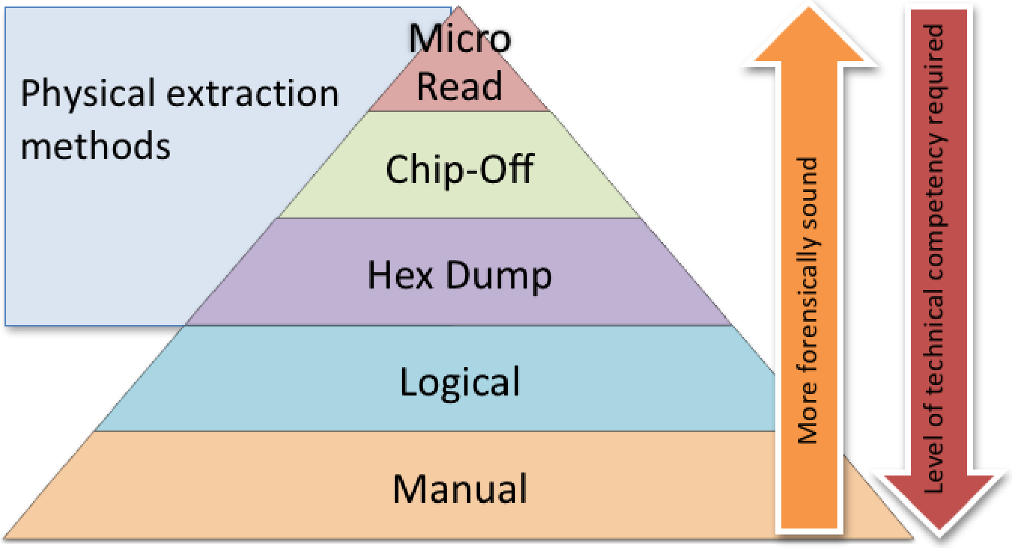
Physical extraction methods
Micro Read
Chip-Off
Hex Dump
Logical
Manual
More forensically sound
Level of technical competency required

Figure 2.3: Tool Analysis Pyramid – Adopted from Brothers, (2009, p3)

2.4.2 Data Extraction from an iPhone

Hogg & Gaffaney (2009) discovered that as of June 2009 the tools available to forensic professionals for extraction, analysis and reporting of evidence on an iPhone are limited. Hogg & Gaffaney (2009) performed testing on an older iPhone 3G running firmware version 2.2. Potentially tools work better with the new iPhone 3GS running the latest firmware. Hogg & Gaffaney (2009, p.4) outline the areas they evaluated with the tools. Six different tools were evaluated: WOLF by Sixth Legion, UFED by Cellbrite, Device Seizure by Paraben, MacLockPick by SubRosaSoft, MDBackupExtract by BlackBag Tech and the physical bit-by-bit image procedure developed by Jonathan Zdziarski. The results from this evaluation show that tools that appear to support the iPhone are still limited and generally only support a logical extraction of data. Some tools support more features if the iPhone being examined is already jailbroken. The only exception to exclusively providing a logical extraction is the physical bit-by-bit procedure developed by Jonathan Zdziarski that uses a hex dump method to collect a physical image of the iPhone disk.

Device	Generation	Disk Size	Flash NAND
iPhone	1st Gen	4GB	Samsung K9HBG08U1M
		8GB	Samsung K9MCGD8U5M
iPhone 3G	2nd Gen	8GB	Toshiba TH58NVG6D1DTG82
iPhone 3GS	3rd Gen	16GB	Toshiba TH58NVG7D2ELA89
		32GB	n/a
iPod Touch	1st Gen	8GB	2x Toshiba TH58NVG5D4CTG20
	2nd Gen	8GB	Micron MLC chip 29F64G08TAA
		16GB	n/a
	3rd Gen	32GB	2x Samsung K9HDG08U5M-LCB0
iPad	1st Gen	16GB	2x Samsung K9LCG08U1M-LCB0
		32GB	n/a
		64GB	n/a
iPad 3G	1st Gen	16GB	n/a
		32GB	n/a
		64GB	n/a

Table 2.4: Flash Memory Used in Apple Devices (iFixit, 2010)

2.4.3 Testing and Validation

Ayers, et al (2007, p.8-15) performed an evaluation of common forensic toolkits for the extraction of data from mobile devices. “Forensic software tools acquire data from a device in one of two ways: physical acquisition or logical acquisition” (Ayers, et al.,2007, p.11). Ayers, et al (2007) further state that tools not designed for forensic purposes are questionable because they must be thoroughly evaluated before use and can potentially overwrite, append to, or cause information loss. Ayers et al (2007, p.16) follow a simple methodology for testing to gauge the capability of forensic tools (Figure 2.4). The process would start by first applying a scenario then the contents of the phone and SIM would be acquired using the tool being evaluated. The result would be examined to determine whether evidence could be recovered as expected.

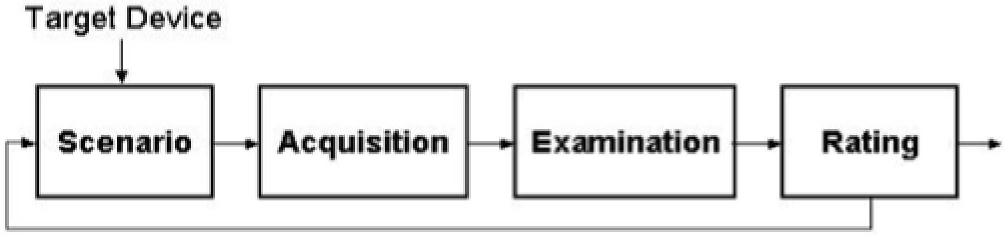

Figure 2.4: Tool Assessment (Ayers, et al, 2007, p.16)

Hoog & Gaffaney, (2009, p.1-100) evaluate software tools used to examine the iPhone. Hoog & Gaffaney, (2009) provide detail on the evaluation process and ranks each tool based on set criteria. The extraction method that scored the highest was the "Zidariski Technique". It's interesting that Hoog & Gaffaney, (2009) came to the conclusion that a proof of concept technique is more effective than any of the pre-packaged commercial extraction tools evaluated.

2.5 MAC OS X FORENSICS

One aspect of digital forensics that is closely linked to the iPhone is Mac OS X forensics. The iPhone runs a modified version of Mac OS X and as such means there are a number of similarities between the two operating systems. One of the major similarities is the file system. Both Mac OS X and the iPhone OS use variants of the HFS (Hierarchical File System) file system. The iPhone uses HFS/X (fifth generation HFS) file system format (Hogg & Gaffaney, 2009, p.69) and Mac OS X uses HFS+. Performing a forensics analysis on a HFS+ formatted hard disk is not new. Burghardt & Feldman (2008, p.76-82) go into detail on the HFS+ file system. A topic that relates closely to the iPhone is the discussion of recovering deleted items from a HFS+ formatted disk. Burghardt & Feldman (2008, p.76) states "Applications for recovering deleted files on Mac OS HFS and HFS+ file systems historically have had limited success compared to recovery tools on other common file systems". Burghardt & Feldman (2008) then continue to state that forensic examination of the HFS+ file system is still an immature field and results can be sporadic. The limited recovery is an unfortunate fact and will no doubt impact the success of recovering deleted items from an iPhone disk image. It does appear the field is improving capability with the latest tools, such as AccessData FTK (Forensic Tool Kit) 3 that offers improved Mac OS X support.

2.5.1 iPhone Operating System

The iPhone OS and Mac OS X share a common heritage. Many of the underlying technologies are the same. However, the iPhone OS was designed to meet the needs of a mobile environment (Apple, 2009). The iPhone has hardware components that are used for interactivity with the device, such as a multi-touch display and accelerometer. Apple has updated the Xcode tools suite to support development of software for the iPhone with the iPhone SDK (Software Development Kit). Xcode allows developers to run their application in an iPhone simulator or transfer their application to an iPhone for testing. As illustrated in Table 2.1 the iPhone firmware has seen multiple revisions. With each revision to the firmware the SDK is updated to allow developers to update their applications to support the changes in the new firmware.

Multiple service layers make up the iPhone OS (Figure 2.5). The first two service layers are labelled by Apple as "Core OS" and "Core Services". Core OS and Core Services layers contain fundamental interfaces for iPhone OS including accessing files, low-level data types and networking sockets (Apple, 2009). The upper layers offer more advanced technologies. The service layer labelled "Media" contains support for graphic and audio features, such as OpenGL ES, Quartz and Core Audio. The highest service layer contains all the services that provide the user with interaction with the operating system. The highest service layer is labelled "Cocoa Touch" by Apple and is an iPhone implementation of "Cocoa" services used in Mac OS X. Cocoa Touch adds support for mobile device specific features, such as multi-touch.

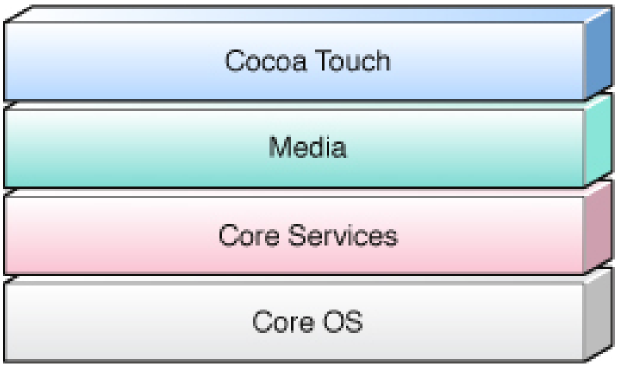

Figure 2.5: iPhone OS Technology Layers (Apple, 2009, p.2)

2.6 SUMMARY OF PROBLEM AREAS

The iPhone has been on the market since mid-2007. The iPhone has gone through four hardware revisions. Unfortunately previous studies have shown the tools that claim to support extraction of data off an iPhone are still limited in capability. Section 2.4.1 discusses the five methods of extraction outlined by Brothers (2009). Most extraction tools that advertise iPhone support can only perform extraction at the logical level. Logical extraction is a common method of extraction because providing a logical copy is easy to implement but means the digital evidence is not complete and accuracy can’t be confirmed. For forensic professionals understanding exactly how the tools they use work is an essential part of the job. Testing and validating extraction tools helps identify how tools extract data. Tools should be tested with test data to ensure the result is as expected and any abnormalities must be investigated. Pre-packaged commercially available forensic tools don’t always provide the best result. Other methods of extraction should be tested and compared to pre-packaged software so the best option is selected. An example of a method that is known to be effective but isn’t a pre-packaged tool is the hex dump method developed by Jonathon Zdziarski.

Software tools are often limited to a logical copy because that’s all that can be copied without physical access to the flash chip. With access to the Flash NAND, an EEPROM (Electrically Erasable Programmable Read-Only Memory) reader could be used to dump the entire contents off the chip in a forensically robust manner for analysis. Although the chip-off procedure is a risky procedure, it may be the only option if a forensic examiner is presented with a device that is already damaged but the Flash NAND is still intact.

Apple has designed the software on the iPhone to strip the user and software developers of a lot of access. The limitations imposed by Apple make it difficult for developers of forensic tools to obtain a physical copy of the iPhone. Commercially available forensic tools do what iTunes can do and create a backup of the logical files on the iPhone. Hacker communities have found ways to penetrate these limitations and bypass the safeguards. The iPhone comes with multiple networking pathways, including WiFi, Bluetooth and cellular connectivity. All the networking technologies pose a risk for forensic professionals because as long as the iPhone is able to communicate through these pathways the data on the iPhone could potentially be tampered with remotely. The risk of tampering is high because of the remote wipe feature implemented by Apple. As well as mitigating the risk of tampering, an examiner needs to be able to continue with the investigation if the remote wipe feature has been activated prior to acquisition of the iPhone.

2.7 CONCLUSION

The Literature review chapter has defined mobile devices and discussed how the Apple iPhone fits into the smartphone category of modern portable devices. Performing a forensic examination of a mobile device has some similarities and differences to a modern personal computer. Such differences can make accessing the storage components difficult as well as maintaining the integrity of the information extracted.

The Literature that defines the iPhone has been reviewed to create an understanding of what the device can do and therefore what can be expected from an evidential perspective. Apple continues to upgrade the hardware used in the iPhone as well as the software that runs on the device. The continued upgrade of the iPhone hardware and software means extraction tools must stay up-to-date. The three major environments that the iPhone works at are discussed, including the physical hardware components, information systems and end user environment.

The current market for extraction tools is constantly changing. The less technical expertise required by the examiner to perform a particular extraction method, the less forensically sound an approach is. Research around extraction tools for the iPhone was reviewed and it was found that most tools only allow extraction at a logical level and are unable to perform a physical extraction. The final section discussed Mac OS X forensics and outlined some of the similarities between Mac OS X and the iPhone OS. The similarities between the operating systems help professionals understand the iPhone platform and the current capability for data extraction and analysis. Many tools for Mac OS X could be adopted to support the iPhone.

Chapter Three

METHODOLOGY

3.0 INTRODUCTION

Chapter two has reviewed literature relevant to iPhone extraction tool capability. The literature has highlighted areas of iPhone data extraction that will be looked at as part of the field work. Previous research has helped identify what approaches worked well in similar research topics. Selecting the most suitable methodology for this research will help ensure research goals are met and the most value comes out of this research. The methodology is an integral component in defining how research will be conducted, how the results will be delivered and discussed. Chapter three takes the information collected from chapter two to build a robust methodology for this research that will ensure optimal results.

A review of published methodologies used in similar studies (Section 3.1) a descriptive methodology. The review is conducted to answer the research question (Section 3.2.3). Heusser (2005, p.1) asks "Does the model describe how things are generally done around here (descriptive model), or does it tell the staff exactly how to do the work, every time (prescriptive model)?". Heusser (2005, p.1) is discussing the descriptive methodology in the context of a work environment (or use system) and how the comparison relates to research. A characteristic of a descriptive methodology is that every aspect of the research is defined and explained. A descriptive approach will help ensure the research is easy to follow and provides the most valuable impact. In comparison an analytical approach would be more complex and results would require additional explanation.

In section 3.1, five similar studies are reviewed that relate to the extraction of data from an iPhone. Analysis of similar studies assists in deriving best practices for research. The research methodologies reviewed in section 3.1 helps identify research processes that work effectively and can be adopted as part of the research methodology. Section 3.2.3 discusses the derived research question and sub-questions for the research (with reference to Section 2.6). The scope of this research is to evaluate the capability of extraction tools for obtaining data stored on an iPhone. However, as part of the research the capability of the iPhone must first be evaluated so as to provide a comparison. In section 3.2.5 the research model is discussed and broken down into four phases: test iPhone capability, evaluate tools, compare tools and provide recommendations for forensic professionals. In section 3.3 the data requirements for the four research phases is discussed. Data will be collected in the form of: expert feedback from industry experts, a catalog of iPhone information systems, an extraction log of extracted files and hash values, journal of evaluation process and performance data that includes scenarios to test extraction tool capability.

3.1 REVIEW OF SIMILAR STUDIES

In section 3.1 five similar studies are reviewed. The studies were selected because they come from reputable sources and follow robust methodology. The results of the studies identify potential areas where additional research could be performed. Each study relates to extraction of data from an iPhone. The studies selected are not specific to the iPhone but mobile devices and Apple technologies. The studies were selected because the research covers topics related to data extraction and mobile devices. Section 3.1.1 looks at research by Burghardt & Feldman (2008) on improving the recovery of files stored on a HFS+ (Hierarchical File Structure) formatted disk. An improved algorithm for data recovery is tested. Section 3.1.2 discusses research by Me & Rossi (2008) into an alternative methodology for data extraction from a mobile device by storing the acquired data on removable storage. Section 3.1.3 investigates the United States legal system and the importance of robust evidence regarding mobile device examination. Section 3.1.4 discusses data extraction from Flash memory; independent of the file system. Different methods are tested and the feasibly discussed. Lastly, section 3.1.5 looks at descriptive research by Punja and Mislan (2008) that covers the forensic extraction and analysis of mobile devices.

3.1.1 Using the HFSD Journal for Deleted File Recovery

Burghardt & Feldman (2008, p.76-82) discuss the recovery of deleted files from a HFS+ formatted hard disk. The article is scientifically technical but the goal is clear, to improve the chance of data recovery. Burghardt & Feldman (2008, p.76) state the data recovery field requires more accurate file recovery tools. The need for improved tools has been identified by a survey performed in 2005 (Burghardt & Feldman, 2008, p.76). The value of the article comes from the new technique developed for file recovery that addresses some of the limitations introduced by other techniques. Improved file recovery algorithms help increase the chances of file recovery from an iPhone. However, there are still limitations with this approach.

Section 2 of the article "Methodology" explains how the research methodology was implemented and how each phase of the research was conducted. The methodology is split into four phases (Sections 2.1 – 2.4). The first phase "Accessing the Catalog File" is a prerequisite to implementing the approach. Initialisation tasks are performed on the disk. The next section phase "Employing the HFS+ Journal for File Recovery" involves implementing the algorithm for file recovery. The algorithm works by following a six-step procedure. The third phase "Determining Recovery Potential" involves classifying recovery potential by looking at the status of the allocation bits in the Volume Bitmap file corresponding to each deleted file (Burghardt & Feldman, 2008, p.3). The possible classifications of recovery potential are: good, partial and poor. The classification defines the process required for file recovery and the potential for complete recovery. The final phase "Additional Reliability Criteria" involves performing additional analysis to enhance the accuracy of the technique.

Burghardt & Feldman (2008, p.82) found the improved algorithm was able to recover a substantial amount of data from a HFS+ formatted disk and are confident the algorithm yields a more accurate and complete result than other techniques. The technique is defined as a "viable method" and Burghardt & Feldman (2008, p.82) state they're able to successfully recover files even if blocks are separated into multiple fragments. However, some limitations are discussed with the procedure. Such limitations include: a lack of a timestamp on deleted files, the full path can't be retrieved, recovery can’t be guaranteed and testing indicates that the timeframe a file can’t be recovered is variable. The variable recovery window means a forensic professional cannot predict where a file is recoverable until attempted.

Burghardt & Feldman (2008, p.76) have identified an area that they believe current procedure is lacking and they have designed an alternative that has been tested and results provided. The research links closely to data extraction. Similarly to recovering deleted files from the HFS+ file system, extraction tools follow methodologies that are currently limited. Further research can help identify and test different methods for feasibility so tools can adopt the best methodologies. The article is also relevant to the iPhone because the iPhone runs a generation of the HFS file system and therefore the improved file recovery algorithm could be adopted to improve recovery of deleted files from an iPhone.

3.1.2 Internal Forensic Acquisition for Mobile Equipment

The article by Me & Rossi (2008, p.2) proposes an “alternative methodology”. The methodology involves the use of removable storage to store a forensically robust physical copy of a mobile phone running Symbian OS. There are established methods for extracting the data from a SIM card or removable storage media but extraction can be difficult from internal Flash memory. The method works by performing an acquisition using a software tool developed by Me & Rossi (2008, p.2). The software tool uses built-in API (Application Programming Interface) calls to copy extracted data from the mobile phone while in read-only mode. The software tool performs three tasks in order to complete the copy process in a forensically robust manner. The first task is to perform the extraction. The second task is to log everything that occurs during the extraction process and the last task is to calculate the hash values of all the files copied using the MD5 (Message Digest) scheme.

The procedure of data extraction can be broken down into several steps that (Me & Rossi, 2008, p.3) describe as an iterative approach (Figure 3.1). Me & Rossi (2008, p.3) found the alternative methodology was more successful than other methods that are limited to a logical copy of the data. However, an issue with the methodology is that the software tool has been developed for Symbian OS and would need to be rewritten for different versions of Symbian OS and different mobile operating systems. Me & Rossi (2008, p.3) also had issues accessing some files due to the system's security features, such as the SMS (Short Message Service) database. Testing shows further development is required for the proposed methodology to work on devices running different operating systems, such as the iPhone OS or Android.

The methodology described in the article is relevant because the article shows researchers are looking for alternative methods to acquire data from internal Flash memory and also expand the amount of data copied to a physical copy. The proposed methodology is a possible solution that mitigates the issue of the internal Flash memory not being easily physically removable. The methodology is a viable approach in terms of being able to return a device back as the method causes no physical damage. Unfortunately for the iPhone the proposed methodology is not suitable. Even if similar software was designed for the iPhone OS the iPhone does not come with a separate slot for removable media so there would be no destination media for the tool to copy the extracted data to. However, despite the lack of a removable media, the methodology is still relevant as the method could be adopted so that a supported storage medium is used as the destination, instead of removable media.

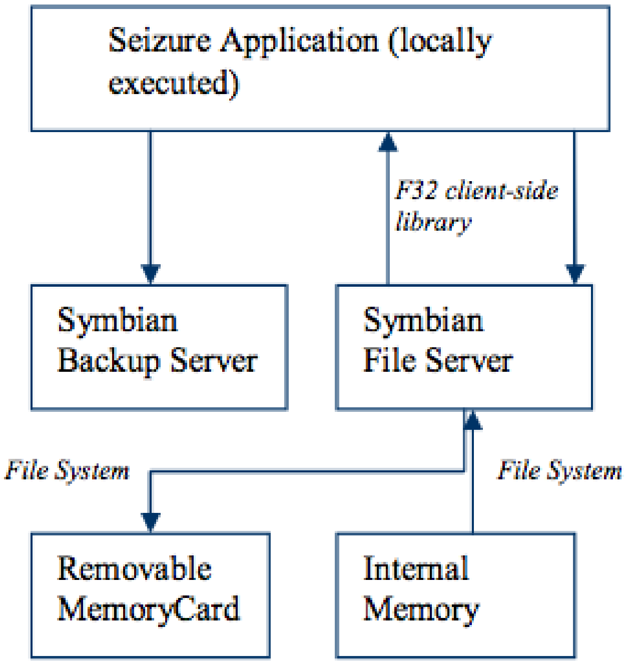

Figure 3.1: The Proposed Architecture (Me & Rossi, 2008, p.2)

3.1.3 Prevalence, Use, and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small-Scale Digital Devices

The article is a study of how important mobile phones are in criminal cases and what type of criminal cases mobile phones are common in. Losavio, et al (2006, p.291) defines the importance by performing a survey of 55 law enforcement officers and then based observations off the results of the survey. In the survey the law enforcement officers were asked about mobile phone involvement in cases they have been involved with.

Losavio, et al (2006, p.5) follows a simple approach to research phases. The first phase was the survey given to law enforcement officers. Losavio et al (2006, p.292-294) then allocated the results of the survey and plotted the responses on bar graphs. The final phase involved providing recommendations for the United States legal system to ensure the robustness of mobile phone evidence. The recommendations are put into context in the case of Gariner versus United States where laws were required to change as a result of the outcome of the case. The case highlighted the issue with lay analysis and expert analysis. Lay analysis is analysis performed by an average user with no specialist knowledge whereas expert analysis is performed by someone with expert knowledge and is preferable as the evidence analysed by an expert is more likely to be accurate, complete and follow tested procedure. However, Losavio, et al (2006, p.2) do mention that the survey results identify that law enforcement officers find access to an examiner with expert knowledge in a timely manner difficult.

The research found that although lay analysis is still important and will continue to be used in court, expert analysis is important due to the complexity of mobile devices. A forensic professional with specialist knowledge in the subject matter should be used to ensure sound evidence.

As mentioned in the article, digital forensics is a specialist field that falls outside the abilities of a normal computer user. Understanding how mobile devices are used in criminal cases helps assist forensic professionals in devising robust procedures around data extraction. A limitation of the article is that Losavio et al (2006, p.291-296) focus only on the legal system in the United States. There is the potential that the situation of mobile phone use in criminal cases is different in New Zealand and other countries.

3.1.4 Forensic Data Recovery from Flash Memory

Breeuwsma, et al (2007, p.3) discusses methods for recovering data from flash memory for forensic purposes. Breeuwsma, et al (2007, p.4) considers an approach to file recovery at a low-level. Three low-level extraction methods for flash memory extraction are evaluated in the article. The extraction methods include the use of flasher tools, JTAG (Joint Test Action Group) and physical extraction. Breeuwsma, et al (2007, p.16) identify that all three methods provide a physical copy of the data on flash memory that includes deleted data. Methods for performing low-level analysis on unsupported file systems are discussed.

In section 3 of the article Breeuwsma, et al (2007, p.3) goes through the three methods evaluated in the research. The first method is the use of flasher tools. Different flasher tools are tested for completeness and appropriateness for forensic use. The second method evaluated is JTAGs. Two test modes are evaluated: extest and debug mode. The final method evaluated is physical extraction. The best way to physically remove the flash chip without damaging the chip is investigated.

With flasher tools there is no general method for extraction (Breeuwsma, et al (2007, p.4). Flasher tools can be used for forensic purposes but the reason flasher tools exist is for debugging and diagnostics. Some mobile phone models only allow a partial copy to be made using a flasher tool. A limitation of using a JTAG for forensic extraction is flash memory itself is not JTAG enabled but the processors that are attached to the flash memory often are. If the processors aren't JTAG enabled the JTAG method can't be used for data extraction.

The article discusses robust methods for Flash memory data recovery that extraction tools could adopt. The methods discussed in the paper expand extraction tool capability beyond logical extraction. Some of the methods are more feasible than others but improvements could enhance any of the methods. Although the article is technical the research followed a robust methodology in investigating different extraction methods. However, based on the details in the article identifying what devices the methods were tested on is difficult. Further research in testing the three methods with a wide variety of mobile devices, including the iPhone, could help identify how viable the methods are for extraction.

3.1.5 Mobile Device Analysis

Punja & Mislan (2008, p.1) took a descriptive approach in the research. The article outlines fundamental concepts for a data forensic practitioner (Punja & Mislan, 2008, p.2). Common mobile technologies are evaluated and characteristics discussed. To provide a basis for the research Punja & Mislan (2008, p.1) defines what a “mobile device” is in terms of the article. A mobile device doesn’t include USB flash disks but cellphones, PDAs and smartphones. To put the research into context cellular networks are defined. A method of definition to provide context is used throughout the article.

Although the article follows a descriptive methodology the research methodology can be split into three phases: investigating what evidence can be extracted, where the evidence can be extracted from and how it should be analysed. Punja & Mislan (2008, p.3) investigate what evidence an examiner can expect from a mobile device. Potential digital evidence includes: audio files, calendar entries, call history, contacts, email, pictures and SMS. The research goes into detail on forensic procedures on a Blackberry and iPhone. Punja & Mislan (2008, p.11) discuss the iPhone and detail what evidence can specifically be extracted from the internal Flash memory. The potential evidence differs from the initial list of evidence provided in the article. The next phase involves evaluating where evidence can be extracted from, such locations include: internal Flash memory, removable storage media, SIM card and NSP (Network Service Provider). Each location of evidence is defined in the context of mobile devices and recommendations for extraction are provided. The final phase is an evaluation of analysis techniques. Toolkits have been tested for capability to perform forensic tasks on mobile devices and provide a set of recommendations for professionals wanting to perform a similar investigation.

Punja & Mislan (2008, p.3) have identified that recovery of deleted data is challenging and is dependent on several aspects an analysis tool uses, including: file system, vendor installed files, configuration and technical skill of the examiner. From the evaluation of analysis tools Punja & Mislan (2008, p.11) find that there is no one tool that can analyse all mobile devices and that there is a lack of tools that support a physical copy of the data. However, toolkits are in development that will perform a physical copy and thus provide the ability to recover deleted data.

The value in the article is in the descriptive methodology. The article relates to iPhone forensics and the recommendations help form a basis for correctly evaluating an extraction tool. In the research it is identified common areas evidence can be found on a mobile device and specifically where to look for evidence on an iPhone. Punja & Mislan (2008, p.11) state that current tools are limited in capability.

3.2 RESEARCH DESIGN

The research design will define the approach that has been selected for this research. Literature has been reviewed and the methodologies investigated. The strengths and weaknesses of the methodologies used by other researchers have been investigated. To ensure the best possible value in this research a methodology that will effectively help in answering the research question and sub-questions has been selected. A descriptive methodology will ensure findings can best benefit forensic professionals in understanding the capability of the tools they're using and possible areas further development could occur.

Five similar studies were reviewed in section 3.1 to establish how published researchers investigate similar topics. The studies share many similarities with the research. The published methodologies reviewed will derive the approach that will be used in the research. Following the review of similar studies is a report of the problem areas discussed in section 2.6. Software restrictions implemented by Apple are an issue for both data extraction and obtaining all the information required to perform a thorough comparison of extraction tools. Procedures will need to be followed in order to mitigate any roadblocks caused by software restrictions. Any additional procedures will need to be well documented. Accuracy of forensic tools is an issue. However, if proper research procedure is followed any tool reports an inaccurate result should be identified. Sections 3.2.1 and 3.2.2 derive the research question in section 3.2.3. The research question is derived from reviewed literature and encapsulates the entire research. Along with the research question several hypotheses are identified in section 3.2.4. The hypotheses identified in section 3.2.4 are testable assertions that will be tested as part of the research. The final section, section 3.2.5, breaks the research down into four phases: Phase 1: Test iPhone Capability, Phase 2: Evaluate Extraction Tools, Phase 3: Compare Extraction Tools and Phase 4: Recommendations.

3.2.1 Review of Similar Studies

Five similar studies were reviewed in section 3.2. Each study focused on extracting digital evidence. Me & Rossi (2008), Losavio, et al (2006), Breeuwsma, et al (2007) and Punja & Mislan (2008) focused their research on mobile devices whereas the research performed by Burghardt & Feldman (2008) is not specific to mobile devices but could be adopted for the iPhone. Data recovery is part of research performed by Burghardt & Feldman (2008), Me & Rossi (2008), Losavio, et al (2006) and Punja & Mislan (2008). The difficulty with physically removing the internal Flash memory means that extraction of data is limited to a logical copy. A physical copy contains a more complete extraction.

Recovery of deleted data is a common aspect to data extraction. Burghardt & Feldman (2008) performed research into an alternative algorithm to improve the recovery of deleted data. Me & Rossi (2008) looked at three low-level file recovery mechanisms: flasher tools, JTAG and physical extraction. The feasibility of the mechanisms being used on an iPhone is unknown. Burghardt & Feldman (2008) tested a recovery algorithm for the HFS+ file system format. Results show the algorithm improves data recovery on the HFS+ file system but there are still associated limitations. The algorithm adopted for the HFS+ file system could be used to improve the chances of data recovery on an iPhone formatted with the HFS/X file system. Losavio, et al (2006) mention that better tools are still required to improve data recovery accuracy.

Losavio, et al (2006) investigated the use of mobile phones in criminal cases in the United States. The data collection method used by Losavio, et al (2006) was a survey of 55 law enforcement officers. Losavio, et al (2006) identified an issue with lay analysis versus expert analysis in the United States legal system. Analysis of a mobile phone is considered to require an expert to examine. Burghardt & Feldman

(2008), Me & Rossi (2008), Breeuwsma, et al (2007) and Punja & Mislan (2008) performed an analysis of extraction tools. Burghardt & Feldman (2008) and Me & Rossi (2008) tested a software tool developed as part of their research. Breeuwsma, et al (2007) not only tested forensic tools but non-forensic tools to be used for forensic purposes. However, Breeuwsma, et al (2007) found that often non-forensic tools can't be validated as the tools haven't had the same level of scrutiny put in place to ensure accuracy of result. The software tools are tested for feasibility of performing the expected tasks, whether the task is data extraction or data recovery.

A common finding by Me & Rossi (2008), Breeuwsma, et al (2007) and Punja & Mislan (2008) is that the physical removal of a storage chip makes it easier for a forensic examiner to perform a full acquisition. A SIM card is a removable component used in many mobile phones. Me & Rossi (2008) identify that there are many forensic tools that can perform an effective acquisition of a SIM card. However, forensic tools are unable to take a full physical copy of the mobile device's internal Flash memory using a simpler method. Me & Rossi (2008) identifies that logging extracted files and performing a hash analysis of the extracted files can improve the accuracy of testing forensic tools.

3.2.2 Review of Problem Areas

In section 2.6 the issue with continued upgrades to both the hardware used in the iPhone and software firmware are discussed. In the three years the iPhone has been available there have been three major upgrades and more minor upgrades. Each upgrade requires forensic tools be updated to adopt the changes. The developers of forensic tools advertise support for the iPhone. Tool developers often aren't clear what level of data a forensic tool can extract from an iPhone. Tool features may claim that the forensic tool is able to extract common information, such as: contacts, SMS, call history and bookmarks. However, there is limited clarity whether the information is the logical files or a full physical copy including deleted information. Understanding capability of forensic tools is essential before a tool can be used for any real world extraction

Forensic tools must also be tested prior to use in a real case. As per normal forensic practice the result from the forensic tool must be complete, accurate and repeatable. The result of the extraction should always match regardless of how many times the process is performed. If the result does not match, the tool is not performing correctly and can’t be validated. Identifying the trustworthiness of a forensic tool is part of evaluating capability. Capability not only includes identifying what data can be extracted but whether the extract is trustworthy based on extensive testing.

As discussed in section 3.2.1 the difficulty involved with physically removing the internal Flash memory makes it difficult for forensic professionals to create a full physical copy of the data. A problem identified in section 2.6 is that the iPhone is designed in such a way that under normal circumstances the iPhone isn’t supposed to be opened and the internal components removed. Regardless of the difficulty with physically removing the internal components, physical removal of the internal Flash memory is a possible method of data extraction and should be evaluated and compared to alternative methods. Physical removal is a promising method of extraction as the method is similar to the traditional methods of data extraction from a hard disk. Understanding the feasibility of physical removal ensures the most common mobile device data extraction techniques are evaluated.

As discussed in section 2.6 Apple release the iPhone OS in a restricted state so only pre-approved applications are allowed to be installed. As discussed in section 2.2 the software restriction can be bypassed by jailbreaking the iPhone. However, jailbreaking makes changes to the data on the iPhone. Procedures that modify data are not ideal for forensic purposes. The software restrictions put in place by Apple make it difficult for forensic tools to load software onto the device that could grab a copy of the physical data. Understanding exactly what is changed during the jailbreaking process is useful when looking at methods that involve using the jailbreaking method. If jailbreaking can be confirmed to not modify any of the user data then jailbreaking may be a viable solution to bypass Apple’s software restrictions.

3.2.3 The Research Question

Section 2.1 shows that the iPhone is a member of an emerging subcategory of mobile devices called smartphones. A smartphone holds potential evidence as discussed in section 2.1.1. A smartphone stores a combination of information found on a PDA as well as information found on a mobile phone. The information stored on an iPhone can be valuable in a forensic investigation so all the information should be extracted in a forensically robust manner. Extracting information from a mobile device has been described as not being a simple task and requires a high level of technical skill from the forensic examiner. Section 2.4 discusses that extraction tools can either be software or hardware based and often follow different methodologies to perform the extraction process. Extraction tools must be evaluated for accuracy and completeness of extraction. Evaluation and testing of the extraction tools provide an understanding of capability.

In section 2.4.1 the five methods of extraction (Brothers, 2009, p.3) are discussed. Methods of extraction vary from the less forensically robust approach of manual extraction to the more complex and most forensically robust approach of microscopic reading. Requirements can be used to benchmark a tools capability.

Section 2.2 defines the iPhone from the physical hardware to software and protocols. For an accurate evaluation to occur the information stored on an iPhone must first be identified so there is a baseline to evaluate extraction tools against. There is the potential for a tool to be limited if the tool is unable to extract all data. The research question for the research is: What is the capability of extraction tools for the extraction of information stored on an iPhone?

3.2.4 Hypotheses

Forensic tools that advertise support for extracting data from an iPhone do so at the logical level. The extraction obtained by forensic tools doesn’t contain deleted data unless a full physical copy is obtained. The extracted data obtained by forensic tools is complete, accurate and the procedure required to obtain the result is repeatable. Improving forensic tools to being able to obtain a full physical copy would still provide a complete, accurate and repeatable result.

Jailbreaking is a procedure that opens access to the iPhone file system without modifying any of the user data stored on the iPhone. Forensic tools could utilise the jailbreaking method to obtain a forensically robust full physical copy of an iPhone.

3.2.5 Research Phases

The research consists of four phases (Figure 3.2). The first phase is to test the capability of the iPhone. Capability includes a detailed evaluation of what data is stored on the internal Flash memory and any other storage components. Understanding the capability of the iPhone is important to evaluating the potential opportunity for digital evidence. The hardware components that store data or could store data will be identified and a catalog of the information systems collated. The catalog will be used to test the capability of extraction tools.

Phase two (Figure 3.2) requires phase one to be complete. Phase two involves testing and evaluating of extraction tools that advertise support for the iPhone. To properly evaluate extraction tools an iPhone will be loaded with sample evidence that will mirror a real world case as closely as possible as well as providing a known baseline for analysis. Part of phase two will be to follow proper acquisition procedures to ensure the handling of the device doesn’t impact the results of the evaluation. The sample evidence will be the same for each extraction tool and reloaded prior to evaluating the next extraction tool. Each extraction tool will be evaluated against the iPhone capability identified in phase one and the known data on the device.

Phase three (Figure 3.2) involves a comparison of the extraction tools evaluated in phase two. The comparison will be based off weighted requirements from common scenarios identified by expert opinion. Each tool will be compared against each other in terms of feasibility to extract data from an iPhone in a particular scenario. The goal of the comparison is to assist forensic professionals choose which tool meets the most requirements in each scenario. The comparison will also help identify which extraction tool is the most versatile overall.

Phase four (Figure 3.2) of the research is a set of recommendations for both forensic professionals of iPhones as well as developers of forensic tools. The recommendations for forensic professionals will include best practices for extracting data from and iPhone and recommendations for ensuring the data extracted is accurate and suitable for the particular scenario. The recommendations for developers of forensic tools will be based off the results of the evaluation and comparison.

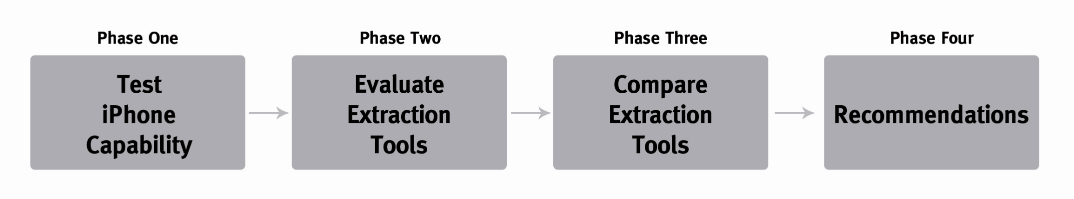

Figure 3.2: Research Phases

3.2.6 Data Map

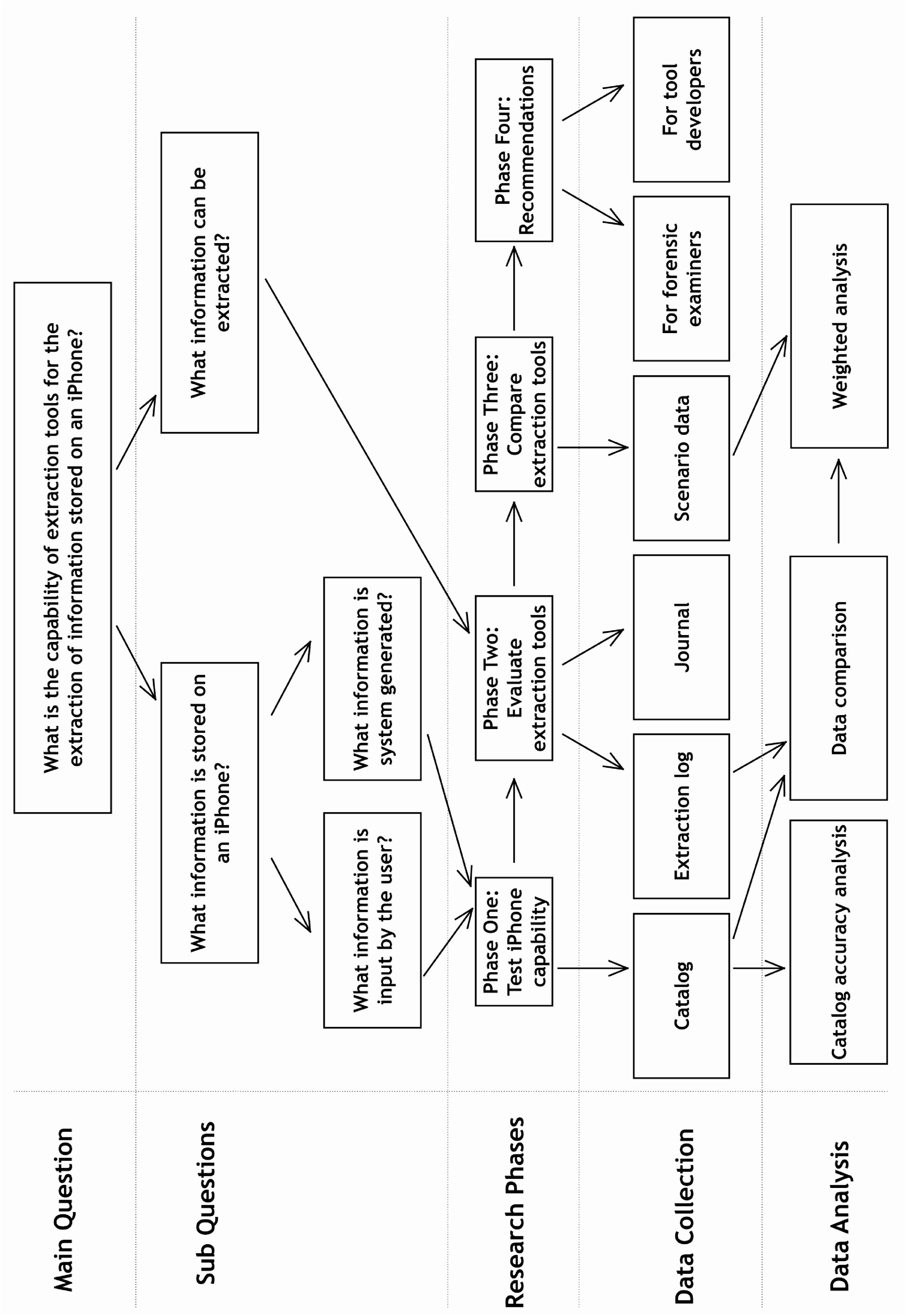
Main Question
What is the capability of extraction tools for the extraction of information stored on an iPhone?
Sub Questions
What information is stored on an iPhone?
What information can be extracted?
What information is input by the user?
What information is system generated?
Research Phases
Phase One: Test iPhone capability
Phase Two: Evaluate extraction tools
Phase Three: Compare extraction tools
Phase Four: Recommendations
Data Collection
Catalog
Extraction log
Journal
Scenario data
For forensic examiners
For tool developers
Data Analysis
Catalog accuracy analysis
Data comparison
Weighted analysis

Figure 3.3: Data Map

3.3 DATA REQUIREMENTS

There are four sources of data for the research. Firstly, the catalog is a list of all the data sources on the iPhone. The catalog provides a baseline for comparison. Secondly, the extraction log includes a list of files copied during extraction and a hash value of those files. Thirdly, the journal contains comprehensive documentation of every action during the evaluation. The journal ensures all processes are repeatable. The final source of data is scenario data. The scenarios have weighted requirements based on expert opinion. The comparative analysis of the scenario requirements against each tool will provide an understanding of capability in common scenarios.

The data must first be collected. The catalog will be collected using both a software restricted and jailbroken iPhone to obtain a complete list of data sources. The catalog is collected during phase one of the research. The extraction log and journal will be generated during phase two of the research and later used for analysis. Scenario data will be collected during phase three and will provide the basis for comparative analysis of extraction tools.

3.3.1 Data Collection

Data will be collected from four separate areas of the research and later processed into the correct format for data analysis. The first area data will be collected is in a catalog. The catalog will be collected in phase one (Figure 3.2) of the research. The catalog will store a complete list of all the known sources of data on an iPhone. The data sources that will be included in the catalog include: the SMS database, web-browsing history, contacts and call history. The property data of each data source will be included, such as: file location, hash value, file type, expected file size, firmware version and a typical usage description. Collecting data for the catalog is a complex task as there are many firmware versions that have been released by Apple since 2007. To simplify the collection of catalog data and to fit within budget constraints only firmware supported by the iPhone 3GS will be investigated. The software restrictions discussed in section 2.2 make it difficult to obtain all the information required for the catalog. For the purposes of completeness the catalog data will first be collected on a non-jailbroken iPhone and then any missing data will be identified on a jailbroken device.

During phase two of the research an independent extraction log will be kept of the files copied during the extraction process as well as a MD5 hash value of the data will be calculated. The extraction log will be used to compare against the catalog in phase three to determine extraction tool capability against known data sources. Me & Rossi (2008, p.2) performed an extraction and analysis of a mobile phone using software developed as part of the research. Me & Rossi (2008, p.4) included a logging function in the software tool that logged all events that occurred during the extraction. An MD5 hash value of the data was also calculated to ensure data integrity as part of data collection. Logging will be implemented in such a way that each file that is copied from the iPhone will be recorded, along with any additional property data that can be obtained. Property data that will be recorded includes: file size, date created, date modified and file type. Hashing will be performed both on each individual files copied as well as a hash value of the collective data. Collected hash values will later be used as part of the data analysis. Many of the extraction tools support their own implementation of logging and hashing. However, there are no standards among the tools and no way to ensure the result is accurate. Keeping data collection independent of the tool will ensure the results of the evaluation are consistent among all tools. The results of the logging and hashing of tools that support logging and hashing will be recorded so as to provide a comparison with the independent result.

To ensure the research is repeatable like other forensic procedures, a journal of every action performed during evaluation will be kept. The journal will also contain system configuration information. The journal should provide a forensic examiner with enough system configuration and procedure information to perform the same process and get the same result. The information that will be included in the journal includes: system configuration, required prerequisites, installation procedure and extraction procedure. System configuration data will be recorded into the journal in the first instance. Any action performed as part of the evaluation will be logged for later data processing.

Scenario data will be used in phase three of the research. The scenario data will be used to determine extraction tool capability when used in common scenarios. Each scenario will have a set of weighted requirements based on expert opinion. Weighted scenario requirements will include: time constraints, need for the device to work after examination, technical ability and financial requirements.

3.3.2 Data Processing

The information in the catalog will need to be processed in such as way that it is used as a baseline to compare against the extraction log. As discussed in section 3.3.1 the catalog will store information about the data sources on the iPhone. As part of the processing of the catalog the file name, location and hash value will be extracted from the catalog. The process of extracting out the information relevant only to the extraction log will be performed for each firmware version. The catalog and extraction log need to be in a similar format so an effective one-to-one analysis can be performed.

The extraction log will contain raw data log and hash data from the evaluation. The raw data will be imported into a CSV (Comma Separated Values) format that can be imported into a database for analysis.

The journal is a standalone set of data that won’t be used in analysis but to validate procedure. The journal will be reformatted into an easy to follow document, similar to a software manual. The goal is that a forensic examiner could obtain a valid extraction by using the same procedure used in evaluation.

Scenario data will be prioritised and a sample of the most common scenario requirements will be selected based on expert opinion. The selected requirements will be used to identify extraction tool capability during the data analysis.

3.3.3 Data Analysis

The first level of data analysis will be an examination of the accuracy of the catalog data. The catalog data must be as accurate as possible in order for an accurate analysis of extraction tool capability. The catalog data will differ based on iPhone firmware version. The first stage of catalog analysis will be to compare the different firmware versions and confirm that the changes in the catalog match the expected changes. The differences in the catalog data will be compared against the known changes released by Apple to ensure the two sources match. An analysis of firmware versions will provide confirmation that the catalog data collection was performed accurately and can therefore be used in further analysis.

The second level of analysis will be a comparison between the catalog and extraction log data. The catalog data contains file details and hash values for all data sources on the iPhone. If the extraction tool is able to extract a complete and accurate set of data then the catalog should exactly match the extraction log. A hash analysis will be performed with each hash value collected in the extraction log checked against a known set of hash values. The hash analysis will be used to identify files that have been modified from the original data uploaded to the iPhone. As well as checking hash values the files logged in the extraction log will be compared against a known list of files. A comparison of the logged files will identify any files missing from the extraction or any additional files copied as part of the evaluation process. The catalog data and extraction log will be independently compared against the log and hash information generated by the extraction tool. The additional analysis will identify any differences between the extraction log and information generated by the extraction tools.

The third level of data analysis is a weighted analysis of scenario data requirements. As discussed in section 3.3.1 the scenario data contains a list of requirements. As part of the data analysis the scenario requirements will be weighted based on expert opinion. Each scenario will consist of the same 20 weighted requirements so the results are as consistent as possible across all scenarios. The variance in each scenario will be in the weighting. The weighting will be numbered from one to five, one being not an important requirement and five being an essential requirement. An example of how the weighting system will work could be in the scenario of a kidnapping. One of the selected 20 requirements may be that the extraction tool can perform the extraction in a timely manner. In the scenario of a kidnapping the requirement may be weighted highly (towards a five weighting) but if the scenario was file recovery of stolen property, time may not be as important (under a three weighting) compared with being able to recover all files (towards a five weighting). The expectation is that a weighted analysis will provide a comparative analysis of the extraction tools. Extraction tool capability will be derived from the results of the weighted scenario comparative analysis.

3.3.4 Data Presentation

The data analysis will provide the most value if the results are presented in an appropriate and effective manner. The results of the catalog accuracy examination will be presented in the simple table containing: “data source”, “catalog data” and “Apple data”. Any rows that don’t match will be highlighted as mismatched so there is a reference if there are unexpected results in later analysis.

Results of the comparative analysis of the catalog data and extraction log will be presented in a similar way to the catalog accuracy examination. The results will be presented in two separate tables, one for log data and another for hash value data. The log data table will contain the columns: “catalog file data”, “extraction log file data”, “exists” and “mismatch”. The hash table will contain the columns: “catalog hash value”, “extraction log hash value”, “exists” and “mismatch”. The files that either don’t exist or mismatch will be highlighted and for each instance a description of why there are inaccuracies will be attached if possible.

The results of the weighted data analysis will require more complex data presentation. The results will be graphed in two ways: according to the 20 requirements and by scenario. The first graph will be a bar graph that includes each requirement (1 to 20) on the x-axis and total weighting versus the obtained result on the y-axis. The second graph will display the same information but with averages instead of totals. The first two graphs will visualise the difference between expected result and actual result for the 20 requirements. The second group of graphs will include two more bar graphs with the scenarios on the x-axis. The first graph will include the total weighting on the y-axis and second graph will include the average over all extraction tools.

The final data that will be presented is the recommendations. The recommendations will be split into “recommendations for forensic professionals” and “recommendations for developers of forensic tools”. “Recommendations for forensic professionals” will be split by scenario. Based on the results of each scenario a set of recommendations will be developed. “Recommendations for developers” will be split by extraction tool.

3.4 LIMITATIONS

There are countless tools adding support for data extraction from an iPhone. As part of the research eight extraction tools (five Mac based and three Windows based) have been selected for evaluation. The eight tools have been selected based on two criteria: the estimated popularity in the digital forensics field and the method of extraction implemented by the tool. A limited selection of extraction tools should minimise the amount of time required to perform an evaluation with a wide spread of extraction methods and still provide valuable results.

The extraction tools selected don't require additional hardware to perform the extraction operation. Tools that require additional hardware are often highly expensive and more specialised than software based options. Software based extraction tools cover a wide range of extraction methods. An example of a specialised extraction method that requires additional hardware and expert knowledge is physical extraction (chip-off). Physical extraction is able to bypass some of the software restrictions that limit software based tools but the equipment is costly.

Scenarios will be selected based on expert opinion and will be a sample of the most common scenarios an iPhone could be a valuable piece of evidence. Sample scenarios will be used as a guide for comparison.

3.5 EXPECTED OUTCOMES

As discovered from literature, the current state of capability of extraction tools for the extraction of data from an iPhone is limited. The first expected outcome is that based on the results of the evaluation the findings of previous researchers will be correct in saying tools are limited. A limitation discussed in literature is the lack of being able to obtain a full physical copy. An expected outcome is that commercial tools evaluated in the research will only extract a logical copy of the files but the Jonathan Zdziarski method will provide a full physical copy. However, the Jonathan Zdziarski method will be time consuming and difficult to implements, especially on the latest firmware version.

Obtaining the catalog data will be complex due to the software restrictions implemented by Apple in the software firmware. The restrictions will mean the iPhone will need to be jailbroken in order for the catalog data to be complete. However, a complete catalog should be able to be obtained and should match the Apple data. An expected outcome of the extraction tool evaluation is that no tool will match the catalog data exactly. There will be several factors that will influence the results, including the lack of a physical copy. Tools may be able to extract some of data. The Jonathan Zdziarski method should best match the catalog. The method that will be used to generate the catalog data and the Jonathan Zdziarski method share similarities. Both methods utilise jailbreaking to open access and SSH to remotely access the device.

An expected outcome of the weighted scenario analysis is that the results will be similar to the catalog analysis. An expectation is that the extraction tools that provide the most complete extraction will also be the most complex to set up and therefore the time required to perform the extraction will be greater. There is also the expectation that no one extraction tool will be suitable in every scenario. Some extraction tools will meet particular requirements but in doing so will lack in other areas. Understanding what scenarios an extraction tool works well in will assist forensic professionals in choosing the most suitable tool depending on their case.

3.6 CONCLUSION

Based on literature in similar research areas there has been a need identified for research into the capability of extraction tools for the iPhone. Results of similar studies show that there are complexities to performing extractions of mobile device data and even with a copy of the data there are still limitations to overcome. Digital forensics is a precise field where testing and validation is essential. The research will involve testing the capability of extraction tools against the known capability of the iPhone. Extraction tools will be evaluated following a research methodology and data will be collected, processed, analysed and finally presented to provide an affective result.

In section 3.1 five similar studies that relate to the extraction of data from an iPhone have been reviewed. The knowledge obtained from the review in section 3.1 includes tested methodology for performing research as well as improved process in related areas. Section 3.2.3 discussed the research question and defined the scope of the research. The research will look at the capability of research tools for the extraction of information stored on an iPhone. As part of the evaluation of capability the iPhone will be analysed to find what information is stored on the internal Flash memory. The analysis will provide a baseline to compare the results of the extraction provided by each tool against. In section 3.2.5 the four phases that make up the research are discussed. The four phases involves first evaluating iPhone capability and then extraction tool capability both against the iPhone capability as well as a common set of scenarios. In section 3.3 the data requirements are discussed: collection, processing, analysis and presentation. Data will be collected in a catalog, extraction log, journal and as scenario data for comparative analysis. There are limitations involved with this research. Section 3.5 discusses the limitations. There is a limitation with the access to tools as well the way Apple have deployed the software on the iPhone. The software is restrictive and an unauthorised procedure must be followed in order for full access to the file system to be granted.

Chapter four will report on the research findings from field work. The research findings will be reported based on the three research phases.

Chapter Four

RESEARCH FINDINGS

4.0 INTRODUCTION

The number of tools that advertise support for the iPhone and indeed many of the Apple mobile devices, including the iPod Touch and iPad is continuing to grow. Extraction tools are designed for forensic evidence extraction and also iPhone user's wanting access to the files stored on their device without the need to synchronise with iTunes. The requirements for extraction for a forensic examiner are often different to an iPhone end-user. A forensic examiner is interested in whether a tool will provide an accurate, complete extraction that maintains evidential value. An end-user on the other hand is more likely to just be interested in gaining access to their data. Tools used for forensic purposes continue to evolve and grow as the push from practitioners becomes stronger.

Research work has been completed in the field following the methodology outlined in Chapter 3. Data collection, data processing and data analysis has been performed and the results outlined in section 4.2. Chapter four will outline the raw findings from the field work following the descriptive methodology outlined in Chapter 3. The raw results from chapter four will provide the basis of discussion in Chapter 5. Findings in chapter four are designed to assist forensic professionals in understanding the strengths and weaknesses associated with using a certain extraction tool.

Chapter four is split into four major sections. In section 4.1 changes to the specified methodology outlined in Chapter 3 are discussed. Section 4.1 clarifies changes to the methodology that could potentially cause the collected data to be different. Section 4.2 is a complete report of the findings from the field work. Section 4.2 is split by the three phases identified in section 3.2.5, with the exception of phase four. Phase four has been removed and moved to Chapter 5, as outlined in section 4.1. Section 4.2 includes a summary of the field findings and reference to appendices where larger data sets are kept. Findings are reported in a descriptive manner following the methodology outlined in section 3.2. The next section, section 4.3, is an analysis of the descriptive approach in section 4.2 and issues with the forensic procedure. The issues in section 4.3 are derived from the journal kept as part of phase two. The final section, section 4.4, is a summary and visual presentation of the raw findings outlined in section 4.2.

4.1 CHANGES TO SPECIFIED METHODOLOGY

Changes to specified methodology are changes made to the methodology described in section 3.3 that could cause different data than expected to be collected. Changes discussed in sections 4.1.1 to 4.1.3 aren't a complete change to the specified methodology, just minor changes that had to be made to continue progressing with data collection. The data went through three phases: data collection, data processing and data analysis. Unforeseen limitations meant several changes needed to be made to the data collection procedure. Catalog data could only be collected while the iPhone was in a jailbroken state. Due to firmware downgrade restrictions implemented by Apple only the latest firmware at time of the field work (3.1.3) could be used. Two common write-blocking methods were tested and neither can be utilised to ensure the computer couldn't write to the iPhone disk. Only hash values calculated by the md5deep tool were used for analysis. The hash values generated by the extraction tool were discarded due to only a limited portion of the tools supported hashing.

4.1.1 Data Collection

Collection of the catalog data differed slightly from the process outlined in section 3.3.1 due to the software restrictions on non-jailbroken iPhones. Based on the instructions and files supplied by Jonathan Zdziarski in his book "iPhone Forensics" the same process was attempted with the newer 3.1.3 firmware but was unsuccessful due to firmware downgrading limitations. Without physically removing the integrated flash storage or jailbreaking the iPhone no method of obtaining a list of the stored files could be identified. To mitigate the software restriction issue a known source of data was selected, an iTunes backup. An iTunes backup contains a limited portion of the active files stored on the iPhone. The iTunes backup may not include all files stored on an iPhone.

In section 3.3.1 firmware versions supported by the iPhone 3GS are discussed and the methodology states that all firmware versions will be tested. The iPhone used for testing was already running the latest stable version (3.1.3) of the iPhone OS. There was no way to downgrade the iPhone to an earlier firmware due to hashing restrictions denying the install of old firmware. There is a mechanism to safeguard an iPhone for downgrading but only while the iPhone is running the particular firmware version. For this research the capability of extraction is concerned with how much of the full disk image an extraction tool can support, not the firmware versions supported by each tool. However, testing different firmware versions could also provide valuable results.

In section 3.3 the method of maintaining evidential integrity by use of write-blockers was selected. During the data collection phase of the field work two common write-blocking solutions were tested and found to not support the iPhone. However, extracted data is stored in read-only DMG files and tested for hash validity to ensure no further risk of changes occurs. MD5 hash checks were performed on sample original data and data stored in the read-only DMG files to confirm the data did not change. Separate DMG files were created for each set of collected data for every extraction tool.

In preparation for creating the most robust set of sample evidence for evaluation the process of wiping the test iPhone and then installing the latest firmware was performed, as discussed in section 3.3. The wiping procedure was not a complete wipe but a zero-out of the unallocated clusters (free space). The iPhone was restored with a fresh copy of the firmware then jailbroken so the wipe tool could be executed. The unallocated clusters were wiped using a third-party tool (iWipe) and the iPhone restored again to a non-jailbroken state with the latest firmware (3.1.3).

4.1.2 Data Processing

There were no changes to the data processing component of the field work. Most data was output in the correct format by the md5dep tool. The only file property details of the data that needed to be extracted were the file name from the full file path.

4.1.3 Data Analysis

In section 3.3.3 hash information generated by the extraction tool was discussed. Section 3.3.3 states that hash information generated by the tool would be compared with hash information generated independently of the tool. Only some of the tested tools supported hashing so the only hash information generated was by the md5deep tool.

In terms of the research phases outlined in section 3.2.5 changes were made to the final phase “Phase Four: Recommendations”. After completing the first three phases it was identified that phase four should not be included as part of discussion in data collection, data processing or data analysis and would be included in chapter 5.

The scenario analysis changes from that outlined in section 3.3.3. Expert opinion wasn’t used to identify the scenarios or requirements. Instead those details were identified by the results of the extraction log analysis.

4.2 FIELD FINDINGS

Three phases were followed during the field work: Phase One: Test iPhone Capability, Phase Two: Evaluate Extraction Tools and Phase Three: Compare Extraction Tools. Each phase relates to a particular milestone of the field findings and includes relevant findings. Phase one involved testing the capability of the iPhone and creating a catalog based on a dd disk image and iTunes backup. Phase two involved evaluating extraction tools by keeping a journal for audit purposes and extraction log. The journal is a collection of all actions and corresponding results of those actions performed during the field work. The journal provides an audit of the process followed and helps identify procedures and best practices identified during evaluation. The extraction log is a complete list of all files identified as part of the catalog and files extracted by each tool. Five extraction tools were able to be included in the extraction log as the tool supported extracting of raw (original) files. The final phase was a comparison of extraction tools based on weighted scenario analysis. Five scenarios were developed for comparison with corresponding requirements and ratings.

4.2.1 Phase One: Test iPhone Capability

As discussed in section 4.1.1 software restrictions implemented in the iPhone OS make it difficult to extract a complete list of the active logical files without jailbreaking the device. The catalog is a set of baseline data that can be used to identify an extraction tool's ability to extract a full physical disk image. The two sources of data used to generate the catalog are outlined in section 3.3.1, iTunes backup and dd disk image.

An iTunes backup was the first source of catalog data to be collected. An iTunes backup is a set of the data that has been copied off the iPhone to the local computer for the purposes of a backup. A backup of an iPhone running firmware version 3.1.3 or lower is stored in a series of ".mddata" and ".mdinfo" files. An iTunes backup from a device running iOS 4.0 or higher no longer appends mddata or mdinfo to the file name but the same information is still extracted. For the purposes of creating the catalog the files contained within the iTunes backup files were extracted using a tool called "iPhone Backup Extractor" by Padraig (2010). The tool iPhone Backup Extractor is able to parse the data stored in iTunes backup files for firmware versions from iOS 4.1 and below. As part of the catalog data collection the extracted data was saved into a read-only DMG file and checked for accuracy by calculating the MD5 hash values of the original files created by iTunes and the files stored in the read-only DMG. The process of extracting the iTunes backup data was completed on the test iPhone both while in a non-jailbroken and jailbroken state. The iTunes backup grew to a size of 7.4MB (Table 4.3). The number of extracted files in both situations (jailbroken and non-jailbroken) was 343 (Appendix B).

The second source of data that was used in the catalog was a dd disk image of the rdisk0s2 partition of the test iPhone in a jailbroken state. A dd disk image is a complete bit-by-bit copy of all the data stored on a disk (or partition). A dd disk image includes files not necessarily accessible by iTunes or extraction tools that only support logical active files. A dd disk image includes the unallocated clusters. A dd disk image can only be taken while the iPhone is in a jailbroken state or by following the Jonathan Zdziarski method due to the software restrictions discussed in section 4.1.1. There are two packages that must be installed in order to create a dd disk image and store the image in a destination location. The software packages required are: OpenSSH (allows a user to connect to a command line session of the iPhone) and nc (netcat, tool for sending a stream of bits). An iPhone application that is installed during the jailbreaking process called “Cydia” can be used to install these two packages. An Internet connection was required to download the packages for installation. Installing the packages makes changes to the data on the phone. The dd disk image of the second partition of the iPhone was taken while the partition as mounted in read-only mode. An MD5 hash value was calculated of both the original partition while in read-only mode and the copied dd disk image. Despite several attempts the MD5 hash values never matched. The process of copying the dd disk image took on average of three hours to complete. The image generated by the procedure grew to a final size of 15.33GB (Table 4.3) in size. The number of active logical files stored in the dd image is 12,963 (Table 4.4).

The final part of constructing the catalog for analysis was classification of “importance rating” ranging from 0 to 2. Files classified as ‘0’ are deemed to be unlikely to store user data that could be useful in an investigation and files classified as ‘2’ were deemed highly likely to contain user data. The classifications that were identified to be importance rating ‘0’ include: jailbreak files and iPod Music (Table 4.1). Importance rating ‘1’ includes files classified as: AppStore or Apple Apps (Table 4.1). The classified importance rating ‘2’ include: AddressBook, Cache, Calendar, Call History, Camera, Cookies, Mail, Maps, OS, Safari and SMS (Table 4.1). Files classified as rating ‘2’ are highly likely to include user data. The files identified as importance rating ‘2’ are also more likely to be backed up as part of the iTunes backup process as the information stored in these files are what makes an operating system unique for the user because of the high levels of personal information stored. From the dd disk image 786 files were classified as rating ‘0’, 10873 rating ‘1’ and ‘1304’ rating ‘2’. From the iTunes backup 3 files were identified as rating ‘0’, 195 were classified as ‘1’ and 71 as rating ‘2’ (Appendix B).

Classification	Rating	dd (Jailbroken)	iTunes Backup	iTunes Backup (Jailbroken)
Jailbreak	0	237	0	0
iPod Music	0	549	3	3
AppStore	1	7491	195	195
Apple Apps	1	3382	0	0
AddressBook	2	3	0	0
Cache	2	144	4	4
Calendar	2	1	0	0
Call History	2	1	0	0
Camera	2	1	1	1
Cookies	2	3	0	0
Mail	2	16	1	1
Maps	2	2	2	2
Notes	2	2	1	1
OS	2	1118	56	55
Safari	2	11	5	5
SMS	2	2	1	1

Table 4.1: Catalog by Classifications

4.2.2 Phase Two: Evaluate Extraction Tools

Phase two involved creating two sets of data, in the form of a journal and extraction log. The journal provides an audit of the process followed during data collection. Journal findings include: procedure, best practices and lessons learnt. The extraction log information was collected using the md5deep tool. The file property details obtained include: file size, MD5 hash value and full path of each extracted files from each tool.

4.2.2.1 Journal

Finding	Page
Firmware downgrade blocking	1
Writeblocking iPhone through USB	2
Faraday bag to block communication	2
Airplane mode	2
Screen lock set to “never” to avoid disconnection of WiFi	3
Bypassing security mechanisms	2
Compatible iTunes version installed	2
Extracted file storage medium	3
Jonathan Zdziarski method in book doesn’t work with 3.x	3
Firmware 4.0 makes changes to iTunes backup format	1
Kill “iTunes Helper” process on local computer running iTunes	2

Table 4.2: Summary of Journal Findings

To provide an audit of the procedures followed during field work and to ensure repeatability of all procedures a journal was kept. For each action performed as part of the field work, a corresponding journal entry was written. The findings from the journal are procedures, best practices and lessons learnt during the time spent evaluating the extraction tools. A summary of findings is in Table 4.2. The full journal can be found in Appendix C.

The first lesson learnt identified in the journal was that Apple has implemented a hardware based firmware kill-switch based on a hash check into the iPhone 3GS and subsequent hardware upgrades. The original iPhone and iPhone 3G are unaffected. The kill-switch allows Apple to decide which firmware a user is allowed to install by acting as a middleman, allowing or denying firmware restoration. The kill-switch prevents outdated firmware from being installed onto an iPhone once Apple has stopped "signing" the firmware. Signing is a process Apple performs whenever an iPhone restores or updates the firmware. During the installation process iTunes communicates with Apple servers over the Internet to confirm whether the firmware can be installed. The only way to bypass the limitation is to save the ECID SHSH unique hash file generated by Apple while they still sign the firmware version. Once Apple has stopped signing the firmware, there is no going back.

Two attempts were made to write-block the data on the iPhone by use of write-blocking hardware and software as per forensic procedure. Firstly, a Tableau UltraBlock USB T8 hardware write-blocker was tested. The write-blocker could detect the iPhone as "Apple Inc" but the computer was unable to detect the phone. The second writeblocking method tested was FastBloc SE by Guideance Software as part of EnCase 6.16.2. FastBloc SE also failed to detect the iPhone. The iPhone requires a two-way connection in order to connect to the computer over USB. Write-blocking should be possible and is a possible area for further research.

Although none of the tested write-blocking techniques worked with the iPhone, forensic procedure was followed to minimize possible changes made to the extracted data. The first procedure was the use of "airplane mode" to block radio communication. The use of airplane mode is equivalent to putting a device into a

Faraday bag. However, unlike a Faraday bag, airplane mode requires interaction with the device and therefore makes changes to the data. The second procedure identified was the killing of the "iTunes Helper" process on the local computer. When iTunes is installed a process called iTunes Helper is installed and set to constantly run in the background. The process stays inactive until an Apple device is plugged into the computer. When an Apple device is plugged in to the computer, iTunes Helper will tell iTunes to open and begin synchronising (if iTunes is configured to automatically synchronise). Ending the iTunes Helper process prior to any forensic work on an iPhone helps prevent iTunes attempting to synchronise with the phone and potentially make changes to the data.

The standard MD5 tool (md5sum) that comes preinstalled on Mac OS X 10.6 Snow Leopard can't recursively calculate MD5 hash values. The md5deep tool was used to utilise the capability of md5sum but with the added ability to generate hashes recursively for import into the extraction log.

A best practice identified during evaluation is to first confirm the most recent version of iTunes supported by the tool as well as the version of iTunes required for the installed firmware version to be accessed. Old versions of iTunes are unable to detect newer iPhones and because all the tools evaluated utilised Apple's USB diskrs and therefore iTunes for extraction it's essential the correct version of iTunes is installed or the extraction will fail. The version of iTunes installed for all test extractions was 9.1.1 64-bit.

As outlined in the journal (Appendix C) the way in which extraction tools store extracted data varies. Forensic tools stored extracted data in a database whereas non-forensic tools extracted the raw files. The method of storing evidential data is up to the developer of the tool.

Device Seizure stores extracted data in a database with the extension ".PDS". When the raw files are extracted out of the tool original file names are lost. Instead each file is named "Binary" with a corresponding number. Other files extracted include: ".hash" and ".property" files containing information about the corresponding binary number. Mobilyze was the only forensic tool evaluated that didn't store the extracted data in a database but instead inside a folder containing all the extracted evidence in raw format along with the case data. Mobilyze stores evidence files inside a folder package with the extension “.mobilyze”. Oxygen Forensics Suite 2010 stores extracted evidence in a database. The database storage location can be changed by the user and is set globally for all cases on that computer. The contents of a particular case can be split from the main database into a separate file called a “backup file”. During testing the procedure of creating a backup file failed. MOBILedit! also stores the extracted data in a database but doesn’t provide the functionality to extract the raw data so could not be used as part of the data analysis. Similarly MacLockPick could only read information from common files but not extract the raw files from the device.

The two non-forensic tools evaluated extracted the raw files directly and didn’t utilise storage in a database. MobileSyncBrowser required user input to manually extract the contents of each of the nine categories. iPhone Explorer provided a browser view of the files the tool could view and those files could be extracted by copy and pasting into a folder on the computer.

4.2.2.2 Extraction Log

The extraction log contains three components of information for each extracted file: file size, MD5 hash value and full path (Appendix B). As discussed in section 4.1.1 the extracted files from each tool were saved in read-only DMG files that were validated for accuracy. The output from the md5deep tool was processed into the extraction log. The first step was to mount the read-only DMG and then run the command md5deep –r –z * from the root of the mounted DMG. The -r switch tells the command to run recursively and the -z switch tells the command to include the file size in bytes as part of the output. The only log that generated incomplete results is the extraction log from the dd disk image as it doesn’t contain the file size. As part of the analysis, hash information in the extraction log was compared with each other as well as the two sources of catalog data. The VLOOKUP function was used in Excel to check both the existence of a matching MD5 hash value or file name in an entire list of extracted files. The file name of each file was extracted from the full path with an Excel formula.

Extraction Tool	Size (MB)
dd (Jailbroken)	15330
Oxygen Forensics	4260
Oxygen Forensics (Jailbroken)	4260
iPhone Explorer	4250
Device Seizure	24.5
Mobilyze	7.5
Mobilyze (Jailbroken)	7.5
iTunes Backup	7.4
iTunes Backup (Jailbroken)	7.4
MobileSyncBrowser	5.5

Table 4.3: Size of Extracts

Both the MD5 hash value and file name of each extracted file was evaluated. When comparing the extraction tools based on hash value with the two catalog data sources the results indicate limited difference between the tested extraction tools. No tool was able to extract a large portion of the total known data. Of the 549 files extracted by Device Seizure from a non-jailbroken iPhone, 214 of them matched the iTunes Backup and 157 matched the dd image, leaving 335 and 392 files not identified in the catalog remaining respectively (Table 4.4). Mobilyze extracted a total 346 files. Of those files, 340 matched the iTunes backup and 247 the dd disk image, leaving 6 and 99 files remaining respectively (Table 4.4). Oxygen Forensics Suite 2010 extracted the most of the evaluated extraction tools with 903 total files extracted, 353 of which matched the iTunes backup and 782 the dd image (Table 4.4). The two non-forensic extraction tools evaluated were: iPhone Explorer and MobileSyncBrowser. The first tool, iPhone Explorer, extracted a total of 560 files, only 13 of which matched the iTunes backup but 535 matched the dd image. MobileSyncBrowser extracted a total of 336 files, 254 of which match the iTunes backup and 174 match the dd image (Appendix B). Based on the results of the comparative results based on MD5 hash value, Oxygen Forensics Suite 2010 offers the most complete extract when compared with the catalog. Oxygen Forensic Suite 2010 was able to extract 99.13% of the same data in an iTunes backup but only 6.14% of the active logical data stored in a dd disk image (Table 4.4).

Extraction Tool	Total	Rating ‘0’	Rating ‘1’	Rating ‘2’
dd (Jailbroken)	12963	786	10873	1304
iTunes Backup	269	3	195	71
Device Seizure	178	1	124	52
Mobilyze	269	2	195	71
Oxygen Forensics	797	531	195	71
iPhone Explorer	555	531	0	24
MobileSyncBrowser	198	2	124	71

Table 4.4: Number of Hash Values Not Jailbroken

The results of the extracting data from a jailbroken iPhone are similar to the non-jailbroken results. Jailbroken results couldn’t be obtained for: Device Seizure, iPhone Explorer or MobileSyncBrowser as the tools failed to acquire an image correctly. Mobilyze extracted a total of 346 files, 340 of which match the iTunes backup and 246 the dd disk image (1 file less than non-jailbroken). Oxygen Forensic Suite 2010 also extracted the same number of files when the iPhone is jailbroken and the files match at 353 with iTunes again but 781 with the dd image (also 1 file less) (Table 4.5).

Extraction Tool	Total	Rating ‘0’	Rating ‘1’	Rating ‘2’
dd (Jailbroken)	12963	786	10873	1304
iTunes Backup	268	3	195	70
Mobilyze	268	2	195	70
Oxygen Forensics	796	531	195	70

Table 4.5: Number of Hash Values Jailbroken

Files classified as rating ‘0’ are considered to be unlikely to contain personal information relating to the iPhone user. Files classified under rating ‘0’ are typically system-generated files that are used in the running of the operating system and store minimal user data. Two tools extract a significant portion of the rating ‘0’ data, iPhone Explorer and Oxygen Forensics Suite 2010. Both tools extract 531 out of 786 (68%) files classified as rating ‘0’ (Table 4.5). The remaining tools extracted between 1 and 3 files. The files extracted by iPhone Explorer and Oxygen Forensics Suite 2010 are MP3 music files stored as part of the music player on the iPhone.

Files classified as rating ‘1’ are files that could potentially contain personal information relating to the user of the iPhone. Rating ‘1’ includes built-in and third party application files. Rating ‘1’ includes executable application files as well as preferences and data stored used by applications, such as a contact list for the

Facebook application. The results of rating ‘1’ are more consistent among all the extraction tools. Of the 10873 files classified as rating ‘1’ the average number extracted is 157 (1.44%) (Table 4.5). The only tool that was unable to extract any rating ‘1’ files was iPhone Explorer.

Rating ‘2’ contains more specific classifications as a file classified as a rating ‘1’ is highly likely to contain personal information about the iPhone user. The classifications within rating ‘2’ are: AddressBook, Cache, Calendar, Call History, Camera, Cookies, Mail, Maps, Notes, Operating System (OS), Safari (Web Browsing) and SMS (Text Messages). 1304 files were classified as rating ‘1’ and the results range from 24 (1.84%) to 71 (5.44%) (Table 4.5). Some of the highly relevant files didn’t match based on hash but did on file name.

Classification	**Rating**	**dd (Jailbroken)**	**iTunes Backup**	**iTunes Backup (Jailbroken)**
Jailbreak	0	237	0	0
iPod Music	0	549	3	3
AppStore	1	7491	195	195
Apple Apps	1	3382	0	0
AddressBook	2	3	0	0
Cache	2	144	4	4
Calendar	2	1	0	0
Call History	2	1	0	0
Camera	2	1	1	1
Cookies	2	3	0	0
Mail	2	16	1	1
Maps	2	2	2	2
Notes	2	2	1	1
OS	2	1118	56	55
Safari	2	11	5	5
SMS	2	2	1	1

Table 4.6: Catalog by Classification

Of the seven extraction tools selected for evaluation five sets of data were collected for data analysis. There are several contributing factors that meant not all the extraction tools could be processed and analysed as outlined in section 3.3. MacLockPick doesn’t extract the original files but copies the information from some areas of interest, such as the address book, SMS history and call history. MOBILedit! does not provide the ability to extract the original files stored in the tool’s database. If the raw files could not be extracted the result could not be processed by md5deep.

4.2.3 Phase Three: Compare Extraction Tools

To form a basis of comparison five scenarios were formulated to compare the evaluated extraction tools. Ten common forensic case scenarios were used as a comparative baseline to evaluate the capability of the extraction tools. These scenarios were selected on the basis of commonality as well as the likelyhood an iPhone could be involved in the given scenario. The five scenarios are a guide and not a comprehensive list of all possible scenarios. Every forensic examination is different. Results are collected both while the test device is in a jailbroken and non-jailbroken state (where the tool is able to support a jailbroken device).

The first selected scenario ("Scenario A") is: "An iPhone needs to be imaged for archiving" (Table 4.7). Archiving was selected as a task because when archiving the completeness of the data is more important than the time it takes to perform the extraction. The second selected scenario ("Scenario B") is: "A fraudster used their iPhone for email when away from the office. Their iPhone has been seized and needs to be searched for email not on their computer or the server" (Table 4.7). Email can be an important source of information in an investigation. Tools were evaluated on their ability to extract email. The third scenario ("Scenario C") is: "An ex-employee has taken intellectual property to their new employer. Their iPhone need to be searched to see if it contains certain documents" (Table 4.7). Similar to Scenario B, Scenario C is focused on document extraction. In Scenario C the use of an iPhone is as a transport device. The fourth scenario ("Scenario D") is: "A kidnapping has been reported and the victim's iPhone has been recovered. Information that may help track down the victim needs to be extracted from the iPhone ASAP" (Table 4.7). Extraction tools vary significantly in the time required to perform the extraction. Time is essential in Scenario D. The final scenario ("Scenario E") is: "A stolen iPhone has been recovered and investigators are looking for evidence linking the stolen property to a known crime ring" (Table 4.7). Extraction data for analysis is important for Scenario E.

Scenario	Description
A	An iPhone needs to be imaged for archiving.
B	A fraudster used their iPhone for email when away from the office. Their iPhone has been seized and needs to be searched for email not on their PC or the server.
C	An ex-employee has taken intellectual property to their new employer. Their iPhone need to be searched to see if it contains certain documents.
D	A kidnapping has been reported and the victim's iPhone has been recovered. Information that may help track down the victim needs to be extracted from the iPhone ASAP.
E	A stolen iPhone has been recovered and investigators are looking for evidence linking the stolen property to a known crime ring.

Table 4.7: Scenarios

17 requirements were identified for scenario analysis (Table 4.9). The same 17 requirements were used in all five scenarios. The differing factor was a weighted rating from 0 to 3. A weighted rating of ‘0’ means the requirement is unimportant for that scenario. Weighting ‘1’ means the requirement is useful but not important. Weighting ‘2’ means somewhat important but not essential and weighting ‘3’ means the requirement is essential for that scenario. The 17 requirements are outlined in Table 4.8.

Scenario Requirements	
Physical image	Extracts of all files
Logical image	Extracts email messages
Non-jailbroken iPhones	Can extract rating '2'
Jailbroken iPhones	Can extract rating '1'
Software writeblocking	Can extract rating '0'
Export files	File names are retained
Extraction took less than 12 hours	Logging
Extraction took less than 1 hour	MD5 hashing
Extraction took less than 10 minutes	

Table 4.8 Scenario Requirements

Rating	Requirement Rating	Tool Criteria
0	Unimportant	Unable to meet requirement
1	Useful but not important	Sometimes meets requirement
2	Somewhat important requirement can be met	Meets requirement half the time or with 50% success
3	Essential requirement can be met	Can meet requirement all the time

Table 4.9: Ratings

All evaluated extraction tools were included in the scenario analysis. For full results see Appendix D. The maximum score possible in Scenario A is 31. The range of results for Scenario A are 18 (58%) to 6 (19%) (Table 4.10). Oxygen Forensics Suite 2010 received the highest score and MobileSyncBrowser and iPhone Explorer received the lowest score equal. For Scenario B the maximum score possible is 33 and the range of results is 26 (89%) to 11 (34%) (Table 4.10). Oxygen Forensics Suite 2010 received the highest result and MobileSyncBrowser the lowest. For Scenario C the maximum score is 34 and the range is from 24 (77%) to 9 (29%) (Table 4.10). Oxygen Forensics Suite 2010 scored the highest and MobileSyncBrowser the lowest. For Scenario D the maximum score is 37 and the range is 28 (90%) to 11 (35%) (Table 4.10). Oxygen Forensics Suite 2010 scored the highest and MobileSyncBrowser the lowest. For the final scenario, Scenario E, the maximum score is 25 and range 20 (65%) to 14 (45%) (Table 4.10). Oxygen Forensics Suite 2010 and Mobilyze scored the highest equal and Paraben Device Seizure and MobileSyncBrowser scored the lowest equal.

Scenario	Max	Highest		Lowest		Average
A	31	18	Oxygen Forensics	6	MobileSyncBrowser	11.33
B	33	26	Oxygen Forensics	11	iPhone Explorer	18.33
C	34	24	Oxygen Forensics	9	MobileSyncBrowser	16.5
D	37	28	Oxygen Forensics	11	MobileSyncBrowser	19.17
E	25	20	Oxygen Forensics Mobilyze	14	MobileSyncBrowser	18

Table 4.10: Scenario Analysis Summary Results

4.3 RESEARCH ANALYSIS

The intended audience for this research is the forensic professional that wants to establish and understanding of the capability of some of the more common software based extraction tools. For this research a descriptive methodology is an important component in bridging the technical and practical aspects of this research. An audit of the procedure followed was documented in the journal. As with any testing that involves breaking some of the common forensic practices there are associated issues. Section 4.3 discusses the descriptive methodology and issues with the forensic procedure reported in section 4.2. Descriptive aspects of section 4.2 are pulled out of section 4.2 and analysed in section 4.3.1. Section 4.3.1 provides an explanation for procedures described. An analysis of issues identified that differ from normal forensic procedure is performed in section 4.3.2. Issues came from collection of the catalog, security mechanisms, software restrictions, writeblocking and carving deleted data.

4.3.1 Descriptive Methodology

As discussed in section 3.3 a descriptive methodology has been selected for this research. In section 4.2 the methodology is put into practice with a descriptive approach taken in reporting the field findings. Section 4.2 consists of a combination of the raw results from the field research and a descriptive explanation of the findings.

In section 4.2.1 to 4.2.3 every process performed as part of the research has been explicitly reported as part of the results. A process that provides context for the results and a logical progression of findings. In sections 4.2.1 and 4.2.2 the steps followed to obtain the respective output are outlined. The steps ensure the best possible forensic procedure has been followed considering the circumstances. An example of a step outlined in section 4.2.1 and 4.2.2 that was followed to ensure procedure was the use of read-only DMG files to prevent changes made to extracted data. The MD5 hash value of the original data (catalog and extracted data) and the data stored in the read-only DMG file were calculated to ensure the process of creating the DMG didn't make changes to the data.

Another aspect of the descriptive approach followed in section 4.2 was a report of the system specification and configuration of the computer system used and iPhone used for testing, including software used. In order to be able to replicate the field findings the system configuration may be required. In section 4.2.1 the operating system of the test computer system, iPhone firmware and iTunes version details are reported.

As part of the jailbreaking process software needed to be installed onto the iPhone in order for a dd disk image to be created and tranferred over the wireless network to a destination computer. The software installed on the iPhone is reported in section 4.2.1 so further research can be performed on the effect installing the specified software has on the evidential value of an iPhone. An analysis of the files changed as part of all the steps followed would allow these files to be ignored from forensic analysis. Another change reported in section 4.2.1 was the use of the networking capability on the iPhone to transfer the dd disk image and installed the required software. The dd disk image was transferred over a local wireless network with no Internet connectivity. The software was installed over a wireless network with Internet connectivity. The connection on the iPhone to the Internet was temporary (enough time to download and install the software). In section 4.3.2 the potential risks with this procedure are outlined.

As part of the data processing activities the information collected in the extraction log was classified based on likelyhood of relevance. In section 4.2.2.2 the three classifications are defined. The three classifications provide the ability to filter out data that is highly likely to be irrelevant including files created as part of the jailbreaking process. Files were classified based on full path. A more indepth analysis of all the common files on an iPhone could produce more thorough classifications.

Scenario findings are reported in section 4.2.3. The purpose of the five scenarios is defined. Scenarios focus on different areas of extraction. For example, Scenario C focuses on document recovery whereas Scenario A focuses on the capability of archiving.

4.3.2 Forensic Procedure

Ref	Issue	Action Taken
1	Catalog accuracy	Both an iTunes backup and dd image was collected
2	PIN code	Test phone set up with no PIN code
3	Encryption	Only an issue for hardware extraction
4	Firmware downgrading	Performed evaluation only on current stable
5	Firmware version	n/a
6	iTunes version	Confirmed required iTunes version
7	Writeblocking	No writeblocking was used
8	Data carving	File Salvage auto detect tool was used

Table 4.11: Issues with Forensic Procedure

Reference 1 (Table 4.11) refers to the accuracy of the catalog data. As discussed in section 4.1 the catalog could only be obtained while the test iPhone was in a jailbroken state. The process of jailbreaking an iPhone makes changes to the data on the device. Normal forensic procedure dictates that changes shouldn't be made to an exhibit as the process could cause the evidence to be not admissible in court. However, in cases where changes are unavoidable the next best alternative is to thoroughly document the process that could make changes to the data on the device. The latter approach is what was used in collecting the catalog. Therefore, the accuracy of the catalog must be tested to ensure accurate results.

References 2 and 3 (Table 4.11) refer to security mechanisms implemented at the software layer on the iPhone. Encryption can be a barrier for forensic professionals to overcome when examining a computer system. The PIN code used on an iPhone is a security mechanism that professionals need to be aware of and be able to bypass if required. A PIN code was not set on the test iPhone during the field research as the added complication would hinder the ability to evaluate the tool extraction capability. However, the way that Apple has implemented the PIN code on the iPhone causes the feature to provide weak security. The PIN code relies on software to enforce access restrictions. If the software can be bypassed, the PIN code becomes irrelevant. Plugging an iPhone into Ubuntu allows limited access to the iPhone disk and bypasses any PIN requirement.

References 4, 5 and 6 (Table 4.11) refer to the issues in regards to firmware and software versions. For the software extraction tools evaluated as part of this research iTunes proved to be a critical prerequisite for any of the tools to detect and extract the data from the iPhone. The iTunes application provides two things: the USB diskr required for the iPhone to communicate with the computer (Linux port *USBMUXD*) and a front-end that provides the ability to initiate a backup of a limited portion of the iPhone files.

Reference 7 (Table 4.11) refers to the lack of write-blocking capability either at the hardware or software layers. This change to procedure was deemed acceptable as other procedures were followed to minimise changes to the data on the disk.

Reference 8 (Table 4.11) refers to the issue of carving data from the HFS/X file system. SQLite and PLIST (Property List) files were carved from the dd disk image with File Salvage.

4.4 VISUAL PRESENTATION OF FINDINGS

A summary of the field findings from section 4.2 are presented with visual summaries. The three importance rating levels are graphed in section 4.4.2 comparing number of hash values claculated and number of files extracted. These graphs represent the total number of items extracted compared with the number collected in the catalog. The number extracted is much lower than the number in the catalog. The final section, section 4.4.3, presents the findings from the scenario analysis. The seven evaluated tools are graphed to display the level of capability.

4.4.1 Phase One: Test iPhone Capability

The catalog consists of a dd disk image of a jailbroken iPhone and extracted iTunes backup. The dd disk image includes 12,963 active files, totaling 15.33GB in size and the iTunes backup includes 343 files, totaling 7.4MB. The files stored in the catalog were classified into 16 classifications that were rated on importance from 0 to 2. Figure 4.1 shows the total number of files classified in both sources of the catalog.

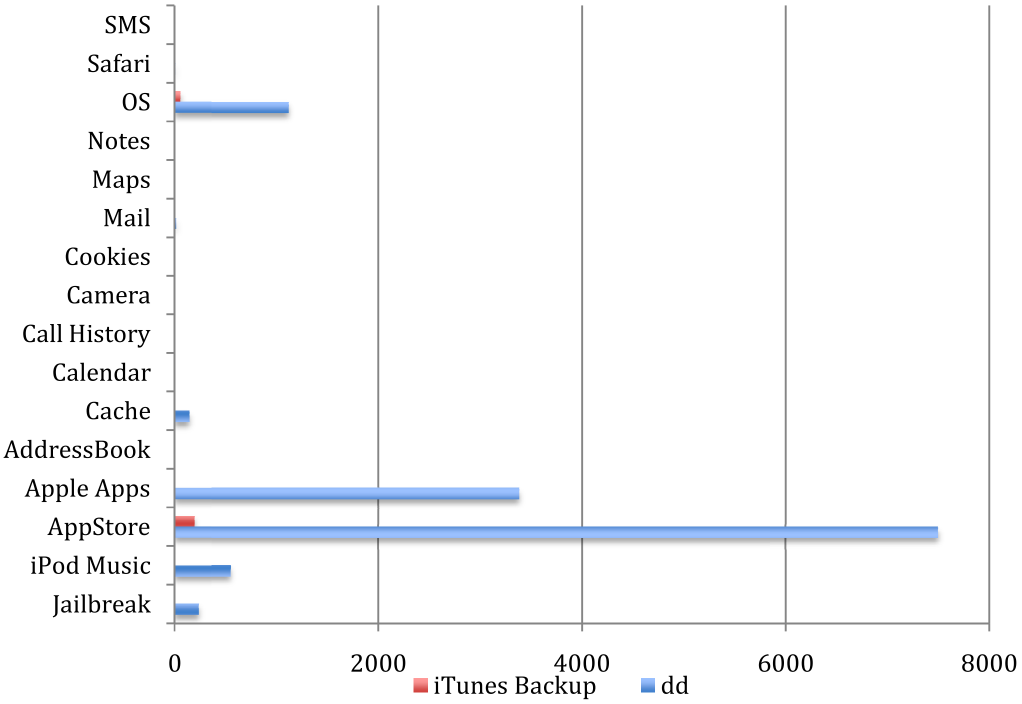

Figure 4.1: Number of Classified Catalog Files

4.4.2 Phase Two: Evaluate Extraction Tools

Two metrics were taken from the extraction log to generate the results for phase two: hash values and file names. Matching based on hash value identifies files that match exactly. Matching on file name identifies files that match on name but the contents might not necessarily match. Three bar-chart graphs have been generated to plot the results of the evaluation. The first graph displays the total results from matching on both hash and file name with the catalog and the five extraction tools that could extract the files in raw format (Figure 4.2).

Figures 4.2 to 4.5 compare the number of files extracted by each extraction tool with the information stored in the catalog. The two coloured bars: blue and red indicate the number of files counted and number of hashes. Blue bars are the number of hashes and red bars are the number of files. For the dd disk image source of the catalog the two bars should match but for the remaining sets of data it's expected there be variations in the two bars.

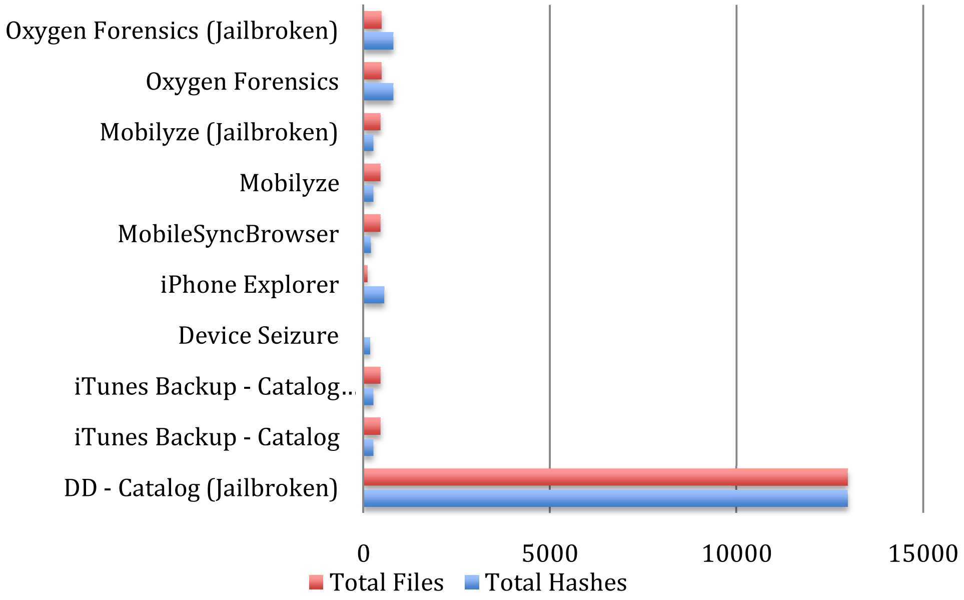

Figure 4.2: Extraction Log Results

The results from Figure 4.2 indicate that none of the extraction tools can extract close to 100% of the catalog data. Figure 4.2 also shows variances in the number of hashes and the number of files that matched. No common trend indicates which is higher as the results differ with the five tools.

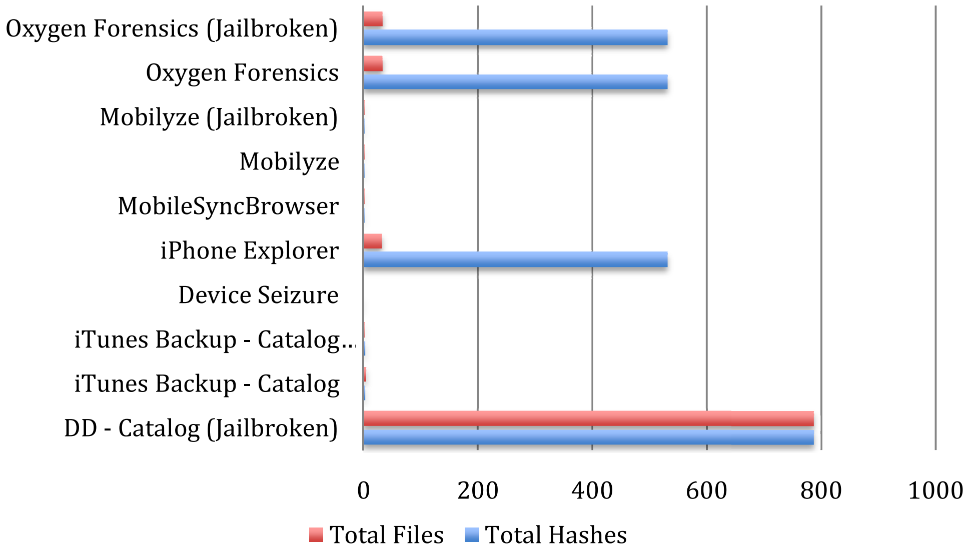

Figure 4.3: Rating '0' Results

Figure 4.3 looks only at files classified as rating '0'. Two tools stand out of the five in total; Oxygen Forensics Suite 2010 and iPhone Explorer. These two tools score highly at rating '0' because the tools are able to extract the MP3 files stored on the iPhone disk.

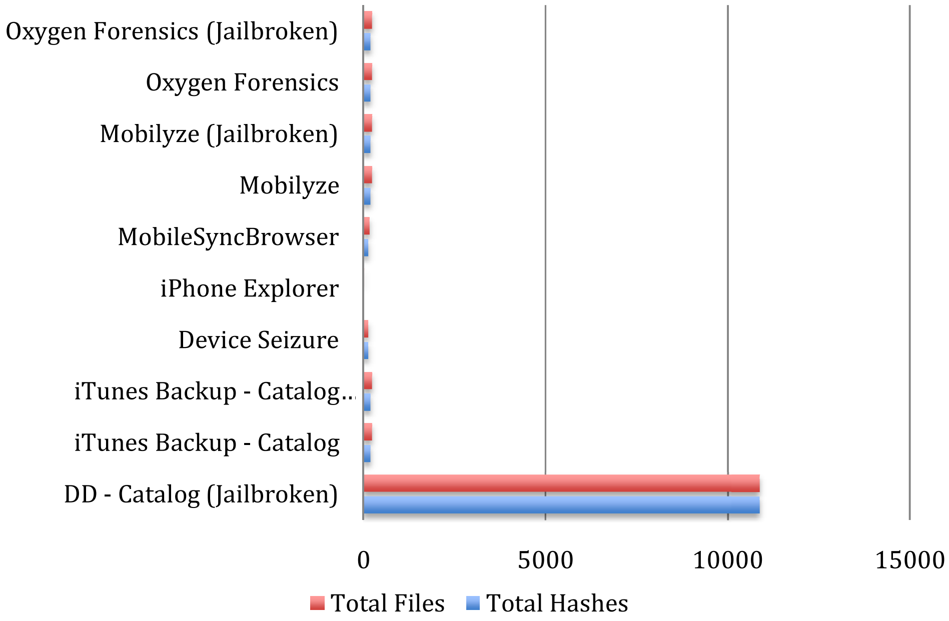

Figure 4.4: Rating '1' Results

Up a level at rating '1' Figure 4.3 looks similar to Figure 4.2. None of the extraction tools are able to extract any significant number of files classified as rating '1'. File classified as rating '1' typically are files that would not require backing up as the files are unlikely to contain personal information and would result in a slow backup.

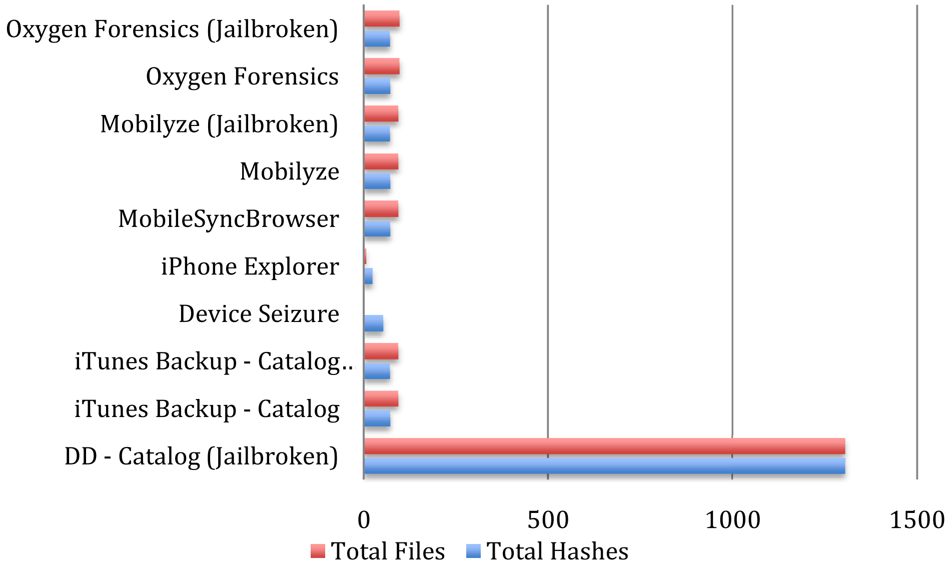

Figure 4.5: Rating '2' Results

The final classification, rating '2', is again a similar shape to the previous bar-chart graphs. However, the extraction tools are able to extract a portion of the data at rating '3'. The results among the extraction tools are generally consistent with the exclusion of Device Seizure and iPhone Explorer. Device Seizure didn't retain any file names during extract which is why matching has only occurred on hash value. Figure 4.4 displays the plotted results from rating '2'.

4.4.3 Phase Three: Compare Extraction Tools

Five scenarios were selected to compare the seven extraction tools evaluated in this research. The results for all scenarios have been plotted on a line-chart graph (Figure 4.6). The range of maximum scores for the five scenarios is 37 to 25 and the range of actual scores received is 28 to 18. Several trends have been identified based on the scenario results. For instance Oxygen Forensics Suite 2010 consistently scored the highest among all five scenarios. MobileSyncBrowser and iPhone Explorer (both non-forensic tools) scored consistently low. MOBILedit! and Device Seizure scored similarity in all scenarios. Mobilyze typically scored just below Oxygen Forensics but above MOBILedit! and Device Seizure.

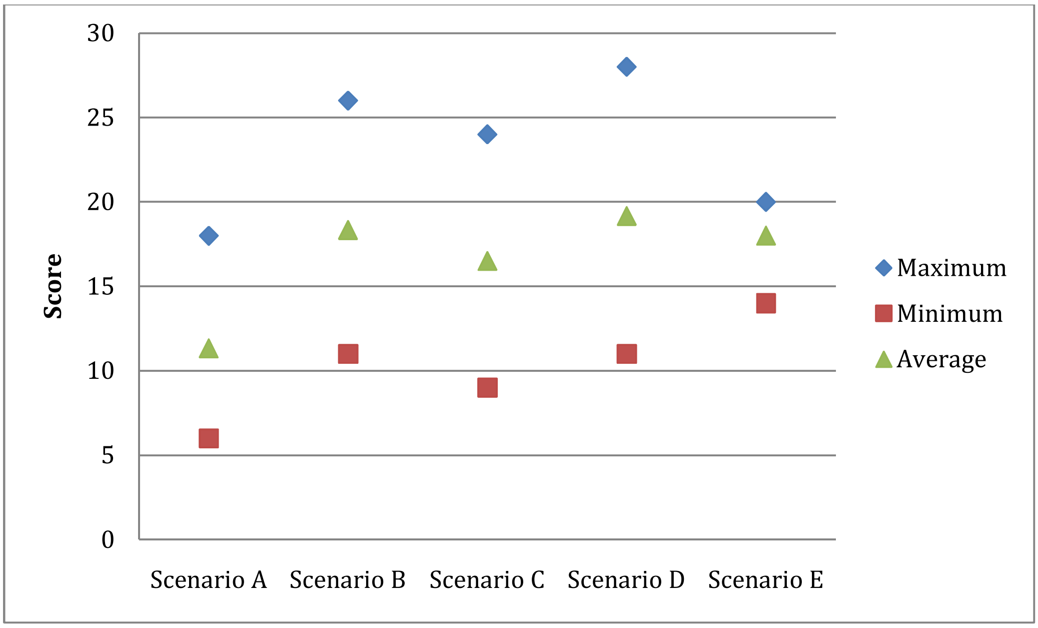

Figure 4.6: Scenario Results

4.5 CONCLUSION

Understanding the capability of the extraction tools that support the iPhone helps a forensic examiner determine the accuracy and completeness they can expect when deciding to use a particular tool. The integrity of the data that is extracted by a tool is an important factor to understand before being used as evidence in court proceeding. Field findings have shown that based on the seven tools evaluated that similar methods of extraction are utilised and the major difference is merely the additional features the tool supply, the storage medium and the user interface. Similarities in extraction method are most likely due to operating system restrictions that lock down the iPhone file system. Jailbreaking was used to open full access to the file system but there are limitations with jailbreaking. Without proper testing and documentation jailbreaking can destroy evidential data.

Changes in specified methodology from that discussed in Chapter 3 have been outlined in 4.1. Issues with unforeseen software restrictions implemented by Apple meant that some changes needed to be made to the data on the test iPhone in order for a full catalog to be collected. The process followed was fully documented and outlined in section 4.2.2.1. The results of the field work have been outlined in section 4.2 in a descriptive way. Section 4.2 outlined data collected as part of the catalog, extraction log, journal and weighted scenarios. The procedure and raw results have been outlined in section 4.2. Section 4.3 discussed the descriptive approach and issues with the forensic procedure. The benefit of a descriptive reporting approach is discussed with references to section 4.2. The eight identified issues with the forensic procedure are discussed in section 4.3. Section 4.4 provided a summary and visual presentation of the findings outlined in section 4.2.

The next chapter, Chapter 5, will use the findings reported in chapter four as a basis for discussion. Chapter 5 will go into discussion and analysis of findings with comparisons made with chapter two.

Chapter Five

DISCUSSION OF FINDINGS

5.0 INTRODUCTION

Chapter five is a discussion of the research findings key points reported in chapter four. Findings provide the most value with comprehensive discussion on the strengths, weaknesses and limitations of the results. Discussion in chapter five is intended to assist in the interpretation and scope of results. The research question and sub-questions can be answered based on the research findings in chapter four. Hypotheses first discussed in section 3.2.4 can be tested and validated. Chapter five is where the relevant and importance of the findings from chapter four are analysed and discussed.

Chapter four reported the field findings in a descriptive manner following the methodology discussed in chapter three. Field findings in chapter four begin to answer some of the underlying questions of this research. Chapter five will go into in-depth discussion of those findings and refer back to relevant previous sections.

Chapter five is split into seven main sections. Section 5.1 answers the research question and sub-questions outlined in section 3.2.3. Results reported in section 4.2 form the basis for answering the research question. The three hypotheses outlined in section 3.2.4 are tested with the assistance of a weighting to find if the hypothesis is correct or not, based on the research findings. Section 5.2 discusses the iPhone software and the importance of understanding the access restrictions that limit a tool's ability to expand capability. The third section, section 5.3, discusses jailbreaking and the affect the process has on forensic procedure. Jailbreaking is identified as a viable method of bypassing access restrictions on the iPhone software as long as procedure is fully documented and tested. Literature indicates an acceptance for the extraction capability when limited to a logical extraction. Section 5.3 discusses that capability is not definite and tools can improve. Section 5.4 discusses maintaining evidential integrity of the data extracted from an iPhone. Although all the evaluated tools extracted while the device was in a live state, steps can still be taken to maintain the integrity of the copied data. Steps were taken during the field work to ensure integrity but more thorough procedure testing would identify any inaccuracies in the data. Section 5.5 discusses the data collected in section 4.2. Section 5.5 explains what areas of capability have been evaluated and where there is room for improvement. Section 5.6 discusses capability in the context of case environments. A scenario analysis was performed and the results reported in section 4.2.3. The extent of guidance scenario results provide is discussed in section 5.6. The final section, section 5.7, discusses possible areas for further research.

5.1 RESEARCH QUESTION AND HYPOTHESE

In section 3.2.3 the research question and sub-questions were derived based on the literature review in chapter two. The research question defines the scope of this research and sub-questions help ensure all components of the main question are answered thoroughly. The sub-questions relate to the data collection objectives discussed in section 3.3.1 and mapped in the data map (Figure 3.3). The research question and sub-questions are answered in section 5.1.1 and 5.1.2. Hypotheses were discussed in section 3.2.4 and are tested in section 5.1.3. Results of testing the three hypotheses indicate H1 (Extraction tools obtain a full physical copy) is incorrect, H2 (Extraction is complete, accurate and repeatable) correct and H3 (Jailbreaking doesn’t modify user data) also correct. Hypothesis testing is based on field findings.

5.1.1 Research Question

The main question for this research is derived in section 3.2.3. The research question research is: What is the capability of extraction tools for the extraction of information stored on an iPhone? Test data has been extracted from the seven selected extraction tools and a scenario analysis has been performed to assist in answering the research question. Two components of capability were measured in this research: what logical files can be extracted and what is a tool’s capability in different scenarios.

The first component of capability was measured by processing data into the extraction log. Results in section 4.2.2.2 indicate that the highest percentage of extraction the evaluated tools can extract when compared with the catalog is 6.17%.

The second component of capability was measured by a weighted scenario analysis. Oxygen Forensics Suite 2010 scored consistently high in the scenario analysis, section 4.2.3. However, the average result is low and no tool scored 100% in any sample scenario.

Challenges are discussed in section 2.1.2. Dankner (2009) states that maintaining integrity is difficult because components cannot be easily removed. Limited physical accessibility means extraction tools are forced to use alternative extraction methods. If a tool is required to access the iPhone through software and not hardware the tool can only access as much as the iPhone OS will allow. Hacking the device (jailbreaking) bypasses the access controls but there are inherent risks with this approach and stored data may be modified. These risks are discussed in section 5.3. In section 2.1.1 the file types of expected evidence is discussed by Punja & Mislan (2008). The evidence types include: contacts, call history, SMS and data typical of a PDA. Findings in section 4.2.1 indicate all the data types described in section 2.1 could be extracted by the evaluated tools.

5.1.2 Sub-Questions

Sub-questions are outlined in section 3.2.3 and are used to thoroughly answer the research question. The first sub-question is: What information is stored on an iPhone? The first sub-question is asking what type data can be extracted from an iPhone if a full physical copy is obtained. The first sub-question can be answered by looking at the data extracted as part of the catalog. A dd disk image of the iPhone disk was taken containing 12,963 active files and 15.33GB in size. Those files were classified into 16 classifications.

The second sub-question is: What information is input by the user? Five forensic tools were evaluated and two non-forensic tools. As discussed in section 4.2.2 the two main differences between forensic tools and non-forensic tools is the method of storing the extracted data and the user interface of the tool. Forensic tools typically store the extracted data in a database that can be validated for integrity. Forensic tools also provide the ability to extract all accessible data off the device by “acquiring” the device.

The third sub-question is: What information is system generated? Two common formats identified in the active files extracted were SQLite and PLIST files. Both file types store information that is potentially relevant in an investigation. The file types common on an iPhone are similar to those on a Mac OS X system, as discussed in section 2.5. Mac forensic analysis tools can be used to analyse data extracted from an iPhone.

The fourth sub-question is: What information can be extracted? The fourth sub-question can be answered by positioning an extraction tool on Brothers (2009) five layers of extraction, discussed in section 2.4.1. As discussed in section 4.2.1, six out of seven of the extraction tools evaluated work at the logical extraction level. The remaining extraction tool fits better into manual extraction as no original files are extracted but information is copied out of the original files. As discussed in section 2.4.1 logical extraction doesn't require a high level of technical expertise to perform. Following sound forensic procedure is separate to the expertise required to use a tool.

Research shows that previous thoughts that extraction tools are limited to logical extraction are correct. The software access restrictions implemented at the OS limit extraction tools to a portion of the logical (active) files. Only data that is given explicit rights to be copied off the iPhone for the purposes of a backup can be copied by the evaluated extraction tools. Jailbreaking is a viable method of bypassing access restrictions if the scope of an examination requires a larger portion of the data to be extracted.

5.1.3 Hypotheses

As discussed in section 3.2.4 three hypotheses have been developed to test the validity of the research findings. The three hypotheses are: H1: Extraction tools obtain a full physical copy, H2: Extraction is complete, accurate and repeatable and H3: Jailbreaking doesn't modify user data. Each hypothesis has been tested with a corresponding weighting 'for' and 'against' to help identify the validity of each hypothesis. The scale of weighting is from 1 to 3. A weighting of 1 indicates that the comment should only have a limited sway in the testing of the hypothesis, weighting 2 indicates an important but not critical comment and 3 indicates the comment is critical to the validation of that hypothesis.

H1: Extraction tools obtain a full physical copy.

W	For	W	Against
1	Software could be expanded to allow more access	3	Tools rely on iTunes that is designed for backing up
3	Chip removal would bypass software restrictions	3	Software restrictions limit file system access
2	Jailbreaking could be used to open access	3	Requires jailbreaking
2	Full physical copy may not be required		
Total: 8		**Total: 9**	

H2: Extraction is complete, accurate and repeatable.

W	For	W	Against
3	Write-blocker solution could be updated to support iPhone	3	No software write-blocking in evaluated extraction tools
3	Forensic procedure followed ensures accuracy	1	Limited hash checks
3	Documentation makes process repeatable	1	Limited logical extraction
		2	Live acquisition, data is constantly changing
Total: 9		**Total: 7**	

H3: Jailbreaking doesn’t modify user data.

W	For	W	Against
2	Classifications show limited change in rating ‘1’ and ‘2’ files	1	User data can be stored anywhere on the disk
2	Doesn’t change files accessible by iTunes	1	Likely to notice files jailbreak files only from full physical copy
3	Hash set could be made of jailbreak files and removed from review	2	Jailbreaking may overwrite unallocated data
2	Prior testing can identify bugs with jailbreak tool	2	Jailbreak tool may contain bugs and delete data
Total: 9		**Total: 6**	

Three hypotheses have been tested at as part of this research. Results indicate that based on weighting H1 is not correct, H2 is correct and H3 is also correct. H1 may indicate that a full physical copy is more unlikely based on the research findings, rather than impossible. None of the evaluated tools were able to obtain a full physical copy. However, another tool may utilise jailbreaking or another innovative method to bypass software access restrictions. H2 indicates that although there are issues with integrity with the evaluated tools, testing shows that the tools are trustworthy. H3 argues that although jailbreaking changes data, user data isn't affected. Results indicate that a limited amount of files of the logical data extracted by the tools was changed by jailbreaking. However, jailbreaking may overwrite unallocated areas of the disk or user data that is not extracted by the tools.

5.2 IPHONE SOFTWARE

In section 2.2.1 three environments the iPhone runs at are discussed: physical, information systems and end user. The statement is made in section 2.2.1 that the iPhone OS bridges the gap between hardware and information systems so the device can be used by the end user. Chip extraction would involve extraction at the physical layer and wouldn't be effected by the limitations of logical extraction.

Section 2.6 states that Apple has designed the iPhone OS to strip the user and software developers of access to most of the logical data. These limitations become apparent when looking to extract files outside the rights of the *mobile* user. Software limitations made the collection of the catalog more difficult than first anticipated. The factory locked state that iOS (iPhone OS) is in when an iPhone is not jailbroken provides limited data access. The limitations shouldn't be apparent to the typical iPhone user as all preinstalled software and software downloaded off the official AppStore is designed to adhere to the access limitations. However, once a user wants to act outside the sandboxed environment the limitations become clear. As forensic professionals a high level of access is required to obtain a full physical copy of an exhibit in a forensically sound way. As discussed in section 4.2.1 in order to get around the OS user access limitations the iPhone used for testing was jailbroken using the "Spirit" jailbreak tool. The process of jailbreaking was fully documented in the journal, section 4.2.2. Software restriction isn't only an iPhone only issue. As discussed in section 3.1.2 Me & Rossi (2008) had difficulty accessing some critical system files, such as the SMS database, on the Symbian OS. Me & Rossi (2008) believed the restriction was due to the database being open and potentially written to. However, as discovered with the iPhone, software restrictions have been explicitly implemented into the iPhone OS to restrict user and developer access to the data.

Another software limitation described in section 4.2.2.1 that was not anticipated was firmware signing. Firmware signing is a control feature implemented at the hardware layer of the iPhone 3GS and iPhone 4 that allows Apple to accept or reject the restoration of a firmware package. Apple currently only allows restoration of the current stable release and developer beta releases. Apple rejects older firmware versions or modified firmware packages. The signing process requires that the computer performing the restore with iTunes be connected to the Internet so the restoration request can be sent to Apple. If the computer can't connect to Apple, the restore will not proceed. As discussed in section 4.2.2.1 the only way to install firmware that is no longer signed by Apple is to save the unique ECID SHSH generated while the firmware version is still signed. Even if Apple stops signing that firmware a local signing server can be set up and the saved ECID SHSH used for restoration authentication can be utilised. For everyday jailbreakers the method of manually saving the ECID SHSH after every firmware version is feasible as control of their iPhone is completely up to them. However, forensic professionals typically only receive an iPhone as an exhibit and have never had access to the device before, so will never have had the chance to save the ECID SHSH. The argument can be made that the implementation of this feature by Apple is in direct retaliation to the jailbreaking community as up until the iPhone 3GS the most popular method of jailbreaking was the restoration of a modified (hacked) firmware package file. Now, jailbreaking methods (such as the Spirit jailbreak used in this research) are run after the iPhone has the officially signed firmware installed.

A consideration when acquiring an iPhone is the constant network connectivity that an iPhone has. A risk involved with the network connectivity is the remote wipe feature can be activated at any time, as long as there is Internet connectivity. As discussed in section 2.3.2 the remote wipe command can be sent from a remote location and potentially destroy the data stored on the device. The remote wipe command can be sent either from the MobileMe website or an iPhone application on another iPhone. If the iPhone is set up with Exchange server, the remote wipe can be sent from the Exchange Management Console. As a Faraday bag wasn't available for testing, airplane mode was used to simulate the blocking of remote wipe. The advantage of using a Faraday bag is that the device doesn't need to be interfaced with in order to block communication. Following forensic procedure a Faraday bag should be put around an iPhone as part of a first responder's process. The potential of remote wipe being activated on the device used for evaluation is not existent as it was acquired in a controlled environment but remote wipe is a consideration for real world cases.

In section 2.2.1.2 the seamless interaction between physical hardware and information system is discussed. In terms of security this interaction is critical as the iPhone relies on software to implement some security features. However, some features require hardware to work. Data is encrypted on the flash hard disk at the hardware layer and firmware signing is also implemented at the hardware layer. Security mechanisms are an important aspect to be aware of when acquiring an iPhone. There are three main security components integrated in the iPhone 3GS and iPhone 4, these are: remote wipe, PIN codes and hardware encryption. PIN codes are a way to limiting access to the user interface at the software level. For example, if an iPhone is set to require a PIN code then the device still functions normally, background processes continue to run and phone calls can still be received. However, without the PIN code, changes can't be made to the configuration of the device and new applications can't be launched. As described in section 4.3.2 no PIN code was configured on the iPhone used for data extraction. A tool's ability to bypass or crack the software PIN code was not a requirement of evaluating capability. There are additional tools that claim to recover iPhone PIN codes. Jonathan Zdziarski outlines that the PIN code is a trivial security measure to bypass due to the mechanism running at the software (operating system) level and not the hardware level. Utilising a method of extraction that is loaded from RAM means that the OS is loaded but the software that performs the PIN code checking is not, so full access can be obtained without entering the PIN code. Hardware encryption has been added to the iPhone since the iPhone 3GS.

The current implementation of hardware encryption means that data stored on the iPhone is encrypted. Fortunately, the data is only encrypted on the chip and not during transmission. The forensic tools evaluated got around encryption because the tools would copy the logical files off the iPhone while the OS is fully booted and all data is decrypted. Jonathan Zdziarski's method relies on that same flaw in implementation. The operating system is loaded into RAM to a point and then the decrypted data is sent over SSH to a dd disk image.

5.3 JAILBREAKING

The process of jailbreaking removes software restrictions in the iPhone and allows full access to the OS. The iPhone can still be used in the same way but the ability to access the file system at the root level and install third-party applications that haven't been specifically allowed by Apple is possible. In section 2.2 jailbreaking is described as coming out of the hacker community. The community has been around since the first iPhone was released and continues to grow and evolve to hack the latest firmware releases. The number of jailbreak tools available now is much greater than with previous versions of the iPhone OS firmware. A sample of the available jailbreaking tools include: Spirit, PwnageTool, purplera1n, blackra1n, redsn0w, sn0wbreeze and JailBreakMe.

The process of jailbreaking an iPhone for forensics is not without risks. The process involves making changes to the data stored on the device and could potentially render the device unusable. Not using devices, such as write-blockers to prevent changes to the data can be considered difficult to accept. However, with complicated devices like smartphones that only run in a sandboxed environment the best method of acquisition may be use a jailbreak tool as long as the process is fully documented. As well as documentation the procedure should be a tested on a setup that mirrors the exhibit as closely as possible in hardware revision, firmware version and cellular carrier. An example of why pre-extraction testing is important is an early version of the Spirit jailbreak removed all active photos when run. The bug was fixed in a later version but the bug still highlights that all procedures should be thoroughly tested before being deployed on a real exhibit.

Jonathan Zdziarski's method described in his book "iPhone Forensics" relies on using the jailbreak tool called PwnageTool to restore an old firmware version to RAM on the iPhone. Due the Apple's signing feature Jonathan Zdziarski's method is no longer valid for the iPhone 3GS or iPhone 4. Jonathan Zdziarski's method has since been updated to support newer devices but is available only to law enforcement. The book describes the forensic procedure for iPhones running firmware versions 1.0.2 to 1.1.4 and all revisions of version 2. The method for version 1.0.2 to 1.1.4 uses a jailbreak tool "iLiberty+" to install a modified payload. The payload is used to boot the iPhone into a forensically sound environment in which a dd disk disk image can be obtained. The process does have bugs, as described in section 3.1.5.3 of the book. The methods described in Jonathan Zdziarski's book leverage popular jailbreak tools for each major firmware release. If Jonathan Zdziarski has continued to follow a similar methodology then recent jailbreak techniques have been adopted to create a similar forensic environment for firmware versions 3.x and 4.x.

As described in section 4.2.3 one of the sources of the catalog was a dd disk image that was captured of the test iPhone while in a jailbroken state. The same process as described in Jonathan Zdziarski's book was followed to obtain the image. The major difference being that the image was not collected in a forensically sound way. However, the process and configuration was fully documented. As described in section 4.2.1 one step did not work as expected as outlined by Zdziarski (2008). MD5 hashing of the acquired partition and acquired image. Despite mounting the partition in read-only mode and multiple transfer attempts, the MD5 hash of the source partition and copied file never matched.

As part of setting up the iPhone to obtain a dd disk image several software packages had to be installed onto the device. As described in section 4.2.1 the package manager Cydia was used to download and install the required packages, OpenSSH and netcat. The process of downloading the two packages required that the iPhone be connected to the Internet. Like jailbreaking the device, the process of connecting to the Internet does not follow sound forensic practice. The methodology of using Cydia was selected because it was the most simplistic method. As there was no risk of a remote wipe command being sent to the phone while it was connected to the Internet as the process was performed on a known device. However, the process of installing the required packages should involve the least amount of changes being made to the device. Further research may have identified methods for installation of the packages without the use of the Cydia package manager or a connection to the Internet. The device was put back into airplane mode as soon as the download of the packages was complete.

To confirm that jailbreaking an iPhone only makes changes to some irrelevant files stored on the iPhone, results of extraction were performed with the tools while the device was both in a non-jailbroken and jailbroken state. The results outlined in section 4.2.1 indicate that based on the limited set of logical files extracted by extraction tools only a small number of files mismatch in MD5 hash. Whether the mismatch in MD5 is because of the jailbreaking process or normal use of the device is unknown. The device was booted into the OS and running live.

5.4 MAINTAINING EVIDENTIAL INTEGRITY

In section 2.1 Punja & Mislan (2008, p.1) describe a smartphone as a hybrid between a cellphone and PDA. The form factor of the iPhone and diversity of the data stored on an iPhone made maintaining integrity a difficult task. Components to maintaining integrity are to confirm the state of a file that has been copied, confirm that state is unchanged in the extracted copy and to store the extracted files so no changes can be made. However, as discussed in section 2.1.2.2 calculating hash values is only a valid approach to maintaining integrity if the procedure isn't going to make changes to the data. Findings indicate that all of the evaluated tools allow changes to be made to the data as the iPhone is acquired in a live state.

As discussed in section 2.3 one of the reasons for continued data change is constant network connectivity. However, risks involved with network connectivity were mitigated because the during field work the iPhone was not connected to a local wireless network or a cellular provider. In a real case a similar process should be followed which would mitigate any risk of changes by network connectivity. Any changes made to the data were the result of processes running on the live system. The iPhone does have a remote wipe feature that can be used to restrict user access to data. Field work indicates that as discussed in section 2.3.2 the methods of remote wipe are correct and that the command to wipe can be executed remotely or on the local device. The command can be blocked as long as there is no network connectivity.

In section 4.3.2 the inability to use standard write-blocking techniques is discussed. Further research could identify why the iPhone requires a two-way connection for data to be copied off. Acquiring an iPhone using the evaluated extraction tools is similar to acquiring a live computer system with a tool such as FTK Imager. Normal forensic procedure of a computer dictates that acquisition is performed while the computer is in an off state if possible, in order to minimise the risk of changes being made to active files on the computer. All extraction tools evaluated in this research require that the iPhone be in a fully booted state. The Jonathan Zdziarski method works around this issue by stopping the operating system boot process before all services are started and only the services required to perform the acquisition have started. Although the Jonathan Zdziarski method runs off RAM because the hard disk isn’t write-blocked there could be changes made to the disk if improper procedure is followed. The Jonathan Zdziarski method describes mounting the main partition in read-only mode, an effective workaround for the lack of hardware or software write-blocker. Chip extraction although highly complicated would not be affected by the need rely on software to prevent changes to the data. However, chip extraction is complex, requires physically opening the device and the encryption key must be retrieved.

As described in section 4.2.2 the independent tool selected for calculating hash values for the extraction log was md5deep. The md5deep tool is a more feature-rich implementation of md5sum, a popular command line tool for calculating MD5 hash values. Validation of the result from md5deep was not confirmed. As the hash value is the most important component of the extraction log for evaluation of extraction tools the integrity of the hash values calculated should be confirmed with as great a certainty as possible. Validation of the hash values was not performed due to the limitation of time to collect all the data for analysis and because of the heavy development into md5sum. The md5sum tool is a stable tool that has been included in Linux and Mac OS X systems for many years.

Section 4.3 discusses the importance of thoroughly testing forensic tools prior to use. Use of the evaluated tools shows that testing and full documentation of procedure is critical. In some instances software bugs meant test extractions didn't complete as expected. Several extracts need to be obtained in order to mitigate some software bugs before a final extract can be taken. As discussed in section 3.2.2, testing is important because it ensures the trustworthiness of a tool. However, testing will only ensure a level of comfort on the areas tested. There is always the potential areas are missed from testing. This research has tested a small portion of extraction capability.

5.5 RESEARCH DATA

As described in section 4.2.1 the method of obtaining the iTunes backup was much simpler than the dd disk image. No changes needed to be made to the data on the iPhone and the process was completed on the computer the iPhone was connected to via a USB cable. Unlike obtaining a dd disk image the iPhone didn't need to be jailbroken to collect the data. An iTunes backup was obtained both while the iPhone was in a jailbroken and non-jailbroken state. As outlined in Table 4.1 only one file changed by jailbreaking the device in the iTunes backup. The data that is backed up as part of the iTunes backup is completely controlled by Apple. An iTunes backup is not designed for forensic acquisition but to provide an iPhone user the ability to backup some of the critical files stored on their iPhone in case their data is lost. The backup process is performed by iTunes every time an iPhone is connected to synchronise. Therefore, the backup process needs to be quick or the user may become frustrated with slow operation. For the backup to be quick Apple has only selected a limited portion of the active files stored on the iPhone to be backed up (Table 4.1). As outlined in section 4.2.2 all forensic tools evaluated utilise iTunes backups to extract the data off a exhibit iPhone.

As part of the catalog creation every file contained in both sources of the catalog were classified as described in section 4.2.1. The 16 classifications are a guideline of what a file could potentially be used for. Classifications were selected based on the file path and file name. For example, any file under the directory "/apt/cydia/" was classified as "Jailbreak". The goal of classifying catalog files was to help identify the importance of the files that were actually extracted.

Rating	Classification	Full Path
0	Jailbreak	/lib/dpkg/info/cydia-sources.list
0	iPod Music	/mobile/Media/iTunes_Control/Music/F01/ZRBK.mp3
1	AppStore	/mobile/Applications/C3A935D4-E8AC-4A1A-8735-C14425BFB7FA/TrivialPursuit.app/gamelib.rlb
1	Apple Apps	/stash/Applications.wdCcKQ/MobileAddressBook.app/MobileAddressBook
2	OS	/Keychains/TrustStore.sqlite3
2	AddressBook	/mobile/Library/AddressBook/AddressBook.sqlitedb
2	Cache	/mobile/Library/Caches/SBShutdownCookie
2	Calendar	/mobile/Library/Calendar/Calendar.sqlitedb
2	Call History	/mobile/Library/CallHistory/call_history.db
2	Cookies	/mobile/Library/Cookies/Cookies.plist
2	Mail	/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/26.2.emlxpart
2	Notes	/mobile/Library/Notes/notes.db
2	SMS	/mobile/Library/SMS/sms.db
2	Safari	/mobile/Library/Safari/Bookmarks.plist
2	Camera	/mobile/Media/DCIM/.MISC/Info.plist

Table 5.2: Classification File Locations

As part of the journal data collection 11 findings were identified (Table 4.2). The journal was collected over phases one and two (Figure 3.3). Six of the journals findings are discussed in section 5.1 as the findings were identified during phase one. The renaming five findings were identified during phase two. As described in section 4.2.2.1 a process called "iTunes Helper" runs on a computer with iTunes installed and opens iTunes whenever an iPhone is connected to the computer. The process of opening iTunes can initiate the synchronisation process, potentially changing the data on the iPhone. If a method of write-blocking the iPhone could be identified that confirms no changes are made then the iTunes Helper process would not need to be disabled. However, because the connection between the iPhone and computer requires write access, procedures need to be followed to ensure the risk of changes to the data are minimised. Disabling the screen lock function in the settings of the phone stops the iPhone from going to sleep. If the device goes into sleep-mode then the extraction process may fail because the connection to the device may be lost. The link failing is more likely to occur when transmitting over wireless on a iPhone 3GS as the wireless connection is broken only minutes after an iPhone locked to save battery life. The iPhone 4 maintains a constant wireless connection.

A simple procedure was followed in processing of the original data for analysis. The output from the md5deep tool was imported into Microsoft Excel as a CSV (Comma-Separated Values). A simple approach was selected, as the requirements of analysis were not complex. An important factor of processing the results was that the results of each tool were output in a similar way so analysis could be performed on the hash values extracted. Using the hash values as a basis an Excel function was used to identify which hash values match between the extraction tools and catalog. Several factors can be observed by comparing hash values (Table 5.2).

Based on the extraction tools evaluated as part of this research there are two common storage medium options: storage of original files or within a database. Most of the forensic tools use a proprietary database format for storage. Databases are an effective storage medium because the risk of information about the extracted files is less likely to be affected by the host OS. By storing the extracted files in original format there is the potential for file property or metadata information to be modified. For example, the file creation date could be changed to indicate when the file was created on the destination computer, not on the iPhone. Maintaining the integrity of extracted file isn’t limited to the contents of the file but the file as a whole. A process of calculating the MD5 hash values of the files, as they’re stored on the iPhone with the extracted file could identify files that have changed during transmission. The issue with the procedure of calculating individual file hashes is that only logical files can be validated as all extraction tools required the iPhone be booted to the OS. Files continue to be created, deleted and modified on a live system.

5.6 CASE ENVIRONMENTS

Five scenarios were used to compare extraction tools as part of this research (Table 4.7). Each scenario was developed based on a “main component” and selected to provide a range of common case scenarios where an iPhone could be an exhibit. The main component for Scenario A is that the data stored on the iPhone needs to be archived. Not all cases require evidence is extracted as quickly as possible. If the data only needs to be archived and potentially used at a later date then the completeness and restoration capabilities of the process are more important than the time it takes to extract the data. Extraction tools obtained high scores in Scenario A if the volume of data extracted by the tool was high.

The main component for Scenario B is the fact that the evidence of high value is email. That’s not to say other data couldn’t potentially be relevant and should be collected if possible. As described in section 4.2.2.2, none of the evaluated extraction tools were able to obtain a copy of the email stored locally on the iPhone. The average score for Scenario B is lower than averages across other scenarios. Email is not backed up as part of the iTunes backup process but is stored on the email server. If an iPhone is lost, damaged or stolen the user can reconnect to their email server and restore all the lost data. Another consideration for a forensic examiner looking at email stored on an iPhone is the format in which the email is stored. The iPhone works in a similar way to the Mail client on Mac OS X and supports MBOX format. MBOX files are stored in plain-text and can be parsed by many forensic analysis tools.

Searching the extracted data is the main component of Scenario C. Scenario C has a broader scope than previous scenarios so the most complete extracted data set is more likely to provide the best results. As long as the files extracted by the tool are readable and retain integrity (including file and metadata property information) searching should not be an issue. Keyword searching could be used to identify the documents provided. The portability of the extracted data is important because the tool that performed the extraction may not be the tool a forensic examiner chooses to perform analysis with. The keyword searching capability of a tool that supports the iPhone may not be as rigorously tested as an industry standard tool, such as EnCase or FTK. However, the advantage of using the same tool for extraction and analysis is that the likelihood the tool can read all the file types is higher. For example, the iPhone heavily uses SQLite, PLISTS and MBOX files. Some tools may not support all required file types and that would cause review of the original documents to be more complex.

Time is the main component in Scenario D. The methods of extraction are highly relevant in Scenario D. The amount of time it takes to extract the information stored on an iPhone in a format ready for review is essential. Figure 2.3 states that the less complex an extraction method the less forensically sound. In time-preasure situations, such as a kidnapping, the robustness of the approach is less important than the time required executing the extraction. Another aspect of Scenario D that needs to be considered is whether the situation requires a forensic tool or if manual extraction (manual browsing of the user interface) is the most suitable option.

The final scenario, Scenario E, involves a major focus on analysis. As like Scenario C where analysis is also important, Scenario E requires that the extracted data be portable so it can be reviewed in another tool if required.

17 requirements are outlined in section 4.2.3. The requirements are not an exhaustive list but were selected as the requirements range through all five scenarios. In section 4.2.2.2 three levels of rating are outlined. The three levels provide a weighted measure of the seven extraction tools in regards to the five scenarios. A “Requirement Rating” as described in section 4.2.3 is a measure of how important to the specific scenario each requirement is. For example, in a scenario where time is critical the completeness of the data extracted may not be as important as the time it takes the tool to complete the extraction.

5.7 RECOMMENDATIONS FOR FURTHER RESEARCH

In section 3.5 an expected outcome of this research is that all evaluated extraction tools are limited in the amount of data that the tools can extract. After collecting and analysing the results it can be stated that this outcome is indeed correct. The sample of extraction tools evaluated in this research is small compared to all available tools. There is the potential that another tool provides more complete results, especially a tool that does not utilise iTunes backup and is able to extract the iPhone data in a more complete way. A similar evaluation of capability of the other tools that support the iPhone would provide an interesting comparison of results with this research. As described in section 5.5 all the extraction tools evaluated use the same method of extraction. However, some tools are able to extract more data because the tool utilises the access granted by the iPhone OS to extract the logical files available to the *mobile* user. The Jonathan Zdziarski method requires *root* user access. Another limitation that isn't directly related to extraction but is still important is the portability of the extracted data. Most of the forensic tools use different storage formats but none use common forensic formats such as: DMG, dd, E01 or L01. Further research could be done into the storage mediums utilised by extraction tools for the storage of evidential data.

What has been described as the "holy grail" (Zdziarski, 2008) of iPhone data extraction is the ability to obtain a full physical copy of the iPhone disk. However, as discussed in section 5.5 the requirements of a case are always different and the simple extraction of the logical files that are included as part of the iTunes backup and therefore accessible by forensic tools is often all that is required. Extraction of a full physical copy is often unnecessary and complex. An analysis of the feasibility of using jailbreaking techniques in forensic tools could be an area for further research. Documentation of procedure is essential in all cases. However, the documentation regarding the jailbreaking process could be quite high and add unnecessary time to the time spent on the case.

As discussed in section 3.5 an expected outcome is that the evaluated extraction tools will be limited to logical files only. During field research this expectation is confirmed correct and that only a limited portion of the logical files can be extracted with the evaluated tools. The reason the evaluated tools do not support unallocated disk space is because the iTunes backup and *mobile* user only have access to a limited portion of the logical files. However, as described in section 4.2.2 some deleted data can be restored because of the way SQLite databases function. A SQLite database is not compacted every time a row is deleted so even if information is deleted by the user and is no longer accessible through the user interface, the deleted data may still be accessible by reviewing the source database file.

The Jonathan Zdziarski method could not be adopted with the available resource for the iPhone 3GS. Section 3.5 states that the Jonathan Zdziarski method would be time consuming. This expectation could not be tested but time was spent attempting to adopt the method for the iPhone 3GS. The process is complicated and requires a high level of expertise. As the method relies on unofficial methods of access there is no clear documentation to work from, only a trial-and-error approach that relies on hacking the iPhone OS. Although possible performance improvements could not be tested on the Jonathan Zdziarski method, improvements were tested with the catalog collection. The Jonathan Zdziarski method requires sending the dd image over a wireless connection with OpenSSH and netcat. There are software tools available that can set up a SSH tunnel over USB and not wireless. Transfer of 15.33GB is much faster over USB than wireless.

In section 3.5 the statement is made that software restrictions would limit the capability of being able to collect the catalog information. As described in section 5.2, software restrictions did contribute to difficulty with catalog collection but workarounds were established. The extent of which the software restrictions would limit the catalog is unknown and based on the research findings the only way to open the iPhone access up is by jailbreaking or using a modified variation of the jailbreaking process. A possible alternative to jailbreaking an iPhone for catalog collection could be to perform chip extraction of the iPhone and use the data extracted from as catalog data. The advantage of using chip removal is that there is no chance the data will be changed as no modifications have had to be made to allow full file system access. However, chip removal is still complex and expensive.

An expected outcome stated in section 3.5 is that none of the evaluated extraction tools would match the data collected as part of the catalog directly. As described in section 5.5 the low result is due to the method of extraction used to by the evaluated tools only allowing access to a limited portion of the file system. A dd image is an entire physical image and therefore access permissions are not an issue. Similarly an expected outcome is that the Jonathan Zdziarski method would match the catalog directly. As discussed, the Jonathan Zdziarski method could not be tested so a comparison can't be made.

Results from the extraction log analysis and scenario analysis weren't as expected. A variation that differs from the expected outcome of the scenario analysis is that the same tool scored consistently high in the scenarios and same tools scored consistently low. The expectation was that certain tools would score well in some scenarios and not as well in others. The expectation was based on the thought that tools would have strengths and weaknesses. However, results indicate that Oxygen Forensics Suite 2010 would work suitability well in all scenarios based on the limited set of requirements. Further scenario analysis based on expert opinion could expand on understanding the capability of the evaluated tools in different case scenarios.

The complexity of setup for extraction did not vary between the evaluated tools. Extraction method similarity discussed in section 5.5 is the main reason for the commonality of complexity. The evaluated tools were selected for evaluation because the tools can be easily purchased off-the-shelf and aren't limited to law enforcement use. Although the interfaces are different and the way in which the tool stores in the data varies, the method of extraction is almost identical with all evaluated tools. Variances in results can be contributed to the source and processing of data.

5.8 CONCLUSION

A thorough understanding of the research findings reported in chapter four has been established and discussed in chapter five. Discussion on field findings has identified strengths and weaknesses with results as well as limitations with the approach that could be improved on and provide areas for further research. The scope of the results has been discussed in chapter five and put into the context of real world forensic scenarios. Chapter five has provided information about tool capability for forensic professionals looking to begin testing of extraction tools to retrieve data from an iPhone. Results indicate that although the amount of data that can be extracted is limited, the tool may still effectively meet the requirements of a particular case. Forensic extraction tools also provide benefit in forensic cases as forensic tools often provide better storage of evidential data and accuracy checks.

The research question and sub-questions have been answered based on research findings in section 5.1.1 and 5.1.2. In section 5.1.3 the three hypotheses are tested on a weighting scale. Testing hypotheses shows that H1 is not correct while H2 and H3 are correct. The five main areas of findings are discussed in sections 5.2 to 5.6. Access restrictions and limitations of the iPhone software that affect data extraction are discussed in section 5.2. Bypassing software restrictions is discussed in section 5.3. Findings on the accuracy and integrity of the evidential data are discussed in section 5.4. Classification of file formats is discussed in section 5.5 and case environments and iPhone may be involved are discussed in section 5.6. Areas of potential further research in and around the topic area are outlined in section 5.7.

Chapter six will summarise and conclude the research. Research findings reported in chapter four will be summarised. Possible areas of further research will be outlined creating a link to continued research.

Chapter Six

CONCLUSION

6.0 INTRODUCTION

The research has evaluated the capability of a set of extraction tools that can extract data from an iPhone. Understanding the capability of tools forensic professionals use ensures the result of extraction meets expectations. The data needs to be accurate and the procedure repeatable or the information may not be admissible in court. Capability can only be obtained if the result can be compared with a known set of data. Hashing has been used to identify files that match in content exactly, even if the file names have been removed or changed. Another component of capability researched is a tool's ability to work in common forensic case scenarios. The requirements of a case differ so a robust tool should work well in most situations.

Chapter six will conclude the thesis and summarise the research findings reported in chapter four. Findings report on the two components of capability evaluated: file based and scenario based. This main objective for this research is concluded while discussing areas of further research, creating a flow on to further work in the topic area.

Section 6.1 is a summary of findings, previously reported in chapter four and discussed in chapter five. The maximum and minimum results of the extraction log are discussed. Findings indicate that forensic tools extract more files than non-forensic tools. The answer to the research question is summarised and concluded in section 6.2. Section 6.2 concludes the answer of this research, based on research findings. Section 6.3 summarises the areas of further research discussed in section 5.7. Section 6.3 is the final section of the thesis and links this research to subsequent further research in the same topic area.

6.1 SUMMARY OF FINDINGS

As part of testing iPhone capability a catalog was collected containing hash information from an iTunes backup and dd disk image. From the iTunes backup 343 hash values were calculated and from the dd disk image 12,963 were calculated. The iTunes backup grew to a size of 7.4MB containing logical active files and the dd disk image grew to a size of 15.33GB containing all logical files and unallocated disk space. Catalog files were classified in 16 classifications with three corresponding ratings (0 to 2). A rating of 0 indicates low relevance (jailbreak and iPod music files) and 2 indicates a highly relevant file (SMS, Safari, OS, notes, maps, mail, cookies, camera, call history, calendar, cache and address book).

Five forensic extraction tools and two non-forensic extraction tools have been evaluated as part of the field work. Extracts from the same iPhone were taken with all seven tools while fully documenting the procedure in a journal. MD5 hash values and file names were collected for the extracted files from the seven tools. Oxygen Forensics Suite 2010 extracted the highest number of files, 903, of which 781 (86.49%) match the dd disk image and 346 (38.32%) match the iTunes backup. MobileSyncBrowser extracted the least number of files, 336. Of the files extracted, 174 (51.79%) match the dd disk image and 254 (75.60%) match the iTunes backup.

During tool evaluation a journal was kept to fully document the procedure followed. The journal contains information on every event: date, action and result. 11 findings were identified in the journal (Table 4.2). The journal findings include issues, lessons learnt and best practices. Issues include the inability to downgrade the firmware version due to hash signing, write-blocking, radio blocking and security mechanisms. Software restrictions implemented on the iPhone OS limit the firmware versions that can be restored on an iPhone and the access the user has to the iPhone file system. The method described by Zdziarski (2008) in his book “iPhone Forensics” describes using a superseded jailbreaking tool called PwnageTool to restore a modified firmware file onto an iPhone to run a forensically sound environment for full physical data extraction. Due to the hash signing implemented by Apple the described method no longer works on the iPhone 3GS or iPhone 4.

Once the restoration process begins the iPhone phones home and detects the modified firmware.

A scenario analysis was performed as part of the field work to identify what tools work well in a set of sample scenarios. Five scenarios were developed for analysis. Each scenario has a corresponding main component. The five main components are: archiving, email recovery, document recovery, speed of recovery and tracking. Findings show that Oxygen Forensics Suite 2010 scored consistently high in all of the five scenarios. MobileSyncBrowser and iPhone Explorer (both non-forensic tools) scored consistently low. Full results are in Table 4.10. Tools were scored against 17 weighted requirements. A requirement weighting was based on the importance of a tool's ability to perform a requirement in that particular scenario. Requirements were developed around the completeness of extraction, hardware support, write-blocking, speed of extraction, hashing and export functionality. Forensic tools typically scored higher in the scenario analysis as forensic tools support additional features required for an investigation, including hashing and evidence storage.

6.2 RESEARCH QUESTION

As part of this research a research question and five sub-questions have been derived. The research question is: What is the capability of extraction tools for the extraction of information stored on an iPhone? The research question is derived from the literature review in chapter two and answered in section 5.1.1. Two measurements of capability have been used in this research, the number of files extracted and an analysis of a sample set of scenarios. The extraction log presented in section 4.2.2.2 is a complete list of both calculated MD5 hash values and file names extracted by both catalog sources and the seven extraction tools. Analysis has been performed on the extraction log data to compare the results of all the extractions. Analysis of the extraction log indicates that the highest level of extraction the seven tools can perform is 6.17% of the known data stored on an iPhone.

Although initial thought was that some tools would work well in particular scenarios and no tool would work well in all scenarios, Oxygen Forensic Suite 2010 scored the highest result in all five scenarios. The scenario analysis result is unexpected. However, research into the extraction method indicates that because all the tools use the same approach to logical extraction (with the exception of MacLockPick) so a consistent result is expected.

The first sub-question is: What information is stored on an iPhone? The first sub-question is answered by the research findings in phase one. Although there are limitations to the data collection approach in phase one, a near complete disk image was collected to provide a robust baseline for iPhone capability. The second sub-question is: What information is input by the user? Results in phases two and three both indicate improved success in extraction with forensic tools. All tools use the same extraction method but findings indicate that forensic tools are designed to ensure evidential data integrity is maintained by storing the data in a database and not the original logical files.

The results of this research are limited to the seven extraction tools available for evaluation. Conclusions have been made on the basis of these tools. However, research into other tools that support the iPhone may yield different results. A common trend identified among most of the evaluated tools is that the method for extraction is the same. A tool's differentiation is in the analysis features the tool supplies and what the tool does with the data the tool extracts. There may be another tool that isn't constrained by the same limitations as the tools evaluated in this research that may be able to provide more complete and accurate results.

The third sub-question is: What information is system generated? The classification of files provides an overview look at what the files on an iPhone are used for. The last sub-question is: What information can be extracted? All the evaluated tools extract at the logical level and even if the iPhone is jailbroken none of the tools were able to extract a complete physical copy. The method used to extract the data limits extraction to a logical extraction. The technical expertise required to use the evaluated tools is low. However, the process must still be fully documented and validated for accuracy before use.

6.3 FURTHER RESEARCH

Areas of further research are discussed in section 5.7. An area for additional research to be performed is in the number of extraction tools tested. Seven software based extraction tools were evaluated as part of this research. Further research could look at more extraction tools, including newly available and hardware based extraction tools. Evaluated tools don't necessarily have to be forensic tools that can be bought off-the-shelf. The Jonathan Zdziarski method is a case-in-point that a developed procedure and set of scripts may offer a better result. Further research could go into looking at the capability of alternative evidence extraction methods. The Jonathan Zdziarski method is a popular technique for law enforcement extracting data from an iPhone. However, other non-software based methods may prove viable in forensic cases.

A part of extraction tool capability that has only been discussed at a limited level is the storage medium for storing evidential data. In section 4.2.2.1 the difference between forensic and non-forensic tools is discussed. Findings indicate that forensic tools typically utilise a database for data storage whereas non-forensic tools store the original files. None of the forensic tools utilise the same storage formats and none use the dd or E01 formats.

The relevance of PLIST and SQLite files is discussed in section 4.3.2. There are other file formats stored on the iPhone that could contain relevant information for an investigation. Basic classification of files has been performed on the files extracted in the catalog. Further research could go into a more thorough analysis and classification of the file formats identified. Files could be further prioritised so as to assist forensic professionals in quickly identifing the files most likely to provide relevance information for their case. Further research could also go into expanding the scenario analysis into more scenarios that are critiqued with the use of a survey of industry experts.

6.4 CONCLUSION

This research has focused on software tools (both forensic and non-forensic) that advertise support for extracting information stored on an iPhone. The volume of the known data that is stored on an iPhone has been evaluated. The iPhone capability has been identified and compared with the result of the seven extraction tools.

Chapter six has concluded this research into iPhone extraction tool capability by reviewing the findings, research question and areas for further research. Research findings have been discussed, including the most complete, and incomplete results obtained from the seven extraction tools. Scenario analysis data has been summarised and limitations of findings also discussed. This research has been concluded by completing the discussion of the research question and sub-questions by summarising the answers discussed in section 5.1.1. The research question encapsulates evaluating the capability of the iPhone, capability of extraction tools and the technical expertise required to perform an extraction. Chapter six links onto further research and summarises the potential areas that research could continue in the topic area.

Complete data extraction from an iPhone is complex due to the hardware and software restrictions. Data extraction is possible due to features that open access to a limited portion of the logical files.

Publications

Cusack, B. & Knight, B. (2010, August 1). iPhorensics – No Pain, No Gain! *Digital Forensics Magazine*, Issue 04, 50-54.

References

New cellphone network set to launch. (2009, May 11). *3 News.* Retrieved from www.3news.co.nz/New-cellphone-network-set-to-launch/tabid/421/articleID/103647/Default.aspx

2 Degrees. (2009) *What does the 2degrees 3G rollout mean for me?* Retrieved from http://blog.2degreesmobile.co.nz/media/what-does-the-2degrees-3g-rollout-mean-for-me/

Apple Inc. (n.d.) *iPhone 2G: Technical Specifications.* Retrieved March 24, 2010, from http://web.archive.org/web/20101106083452/http://www.apple.com/i

Apple Inc. (n.d.). *iPhone 3G: Technical Specifications.* Retrieved March 24, 2010, from http://www.apple.com/iphone/specs-3g.html

Apple. (n.d.). *iPhone 3GS: Technical Specifications.* Retrieved March 24, 2010, from http://www.apple.com/iphone/specs.html

Apple Inc. (2009). *iPhone OS Overview.* Retrieved April 6, 2010, from http://developer.apple.com/technologies/ios/

Apple Inc. (2009). *iPhone in Business: Security Overview.* Retrieved April 11, 2010, from http://www.apple.com/iphone/business/docs/iPhone_Security_Overview.pdf

Ayers, D. (2009). A second generation computer forensic analysis system. *Digital Investigation, 6*, 34-42. doi: 10.1016/j.diin.2009.06.013

Ayers, R., Jansen, W., Cilleros, N., & Daniellou, R. (2005). *Cell Phone Forensic Tools: An Overview and Analysis.* Gaithersburg, USA: National Institute of Standards and Technology.

Ayers, R., Jansen, W., Moenner, L., & Delaitre, A. (2007). *Cell Phone Forensic Tools: An Overview and Analysis Update*. Gaithersburg, USA: National Institute of Standards and Technology.

Ayers, R. (2008). Mobile Device Forensics – Tool Testing [PowerPoint slides]. USA: National Institute of Standards and Technology. Retrieved April 11, 2010 from www.cftt.nist.gov/documents/MobileDeviceForensics-MFW08.pdf

AL-Hajri, H. & Sansurooah, K. (2008). *iPhone Forensics Methodology and Tools*. Paper presented at the 6th Australian Digital Forensics Conference. doi: 10.1.1.149.5015

Baggili, I. M., Mislan, R., & Rogers, M. (2007). Mobile Phone Forensics Tool Testing: A Database Diskn Approach. *International Journal of Digital Evidence, 6*(2). Retrieved April 11, 2010 from www.utica.edu/academic/institutes/ecii/publications/articles/1C33DF76-D8D3-EFF5-47AE3681FD948D68.pdf

Biggs, S., & Vidalis, S. (2009). *Cloud Computing: The Impact on Digital Forensic Investigations*. Paper presented at the International Conference for Internet Technology and Secured Transactions. Retrieved from http://ieeexplore.ieee.org.ezproxy.aut.ac.nz/stamp/stamp.jsp?tp=&arnumber=5402561&isnumber=5402499

Breeuwsma, M., De Jongh, M., Klaver, C., Van der Knijff, R., & Roeloffs, M. (2007). Forensic Data Recovery from Flash Memory. *Small Scale Digital Device Forensics Journal, 1*(1), 1-17. Retrieved April 09, 2010from www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

Brothers, S. (2008). *How Cell Phone "Forensic" Tools Actually Work (Proposed Leveling)* [PowerPoint slides]. Presented at Mobile Forensics World 2008. Retrieved April 15, 2010 from www.mobileforensicsworld.org/2008/.../MFW2008_Brothers_HowCellPhoneForensicToolsWork.pdf

Brothers, S. (2009). *Cell Phone and GPS Forensic Tool Classification System: 2009 Update* [PowerPoint slides]. Presented at Mobile Forensics World 2009. Retrieved April 01, 2010 from www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhoneandGPSForensicToolClassificationSystem.pdf

Brothers, S. (2009). *Image Ballistics* [PowerPoint slides]. Presented at Mobile Forensics World 2009. Retrieved April 20, 2010 from www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_ImageBallistics.pdf

Burghardt,A. & Feldman, A. (2008). Using the HFSD journal for deleted file recovery, *Digital Investigations*, 5, 76-82. doi:10.1016/j.diin.2008.05.013

Byers, D., & Shahmehri, N. (2009). A systematic evaluation of disk imaging in EnCase 6.8 and LinEn 6.1. *Digital Investigation, 6*, 61-70. doi: 10.1016/j.diin.2009.05.004

Carlton, G. H. (2008). An Evaluation of Windows-Based Computer Forensics Application Software Running on a Macintosh. *Journal of Digital Forensics, Security and Law, 3*(3). doi: 10.1.1.169.638

Casadei, F., Savoldi, A., & Gubian, P. (2006). Forensics and SIM cards: An Overview. *International Journal of Digital Evidence, 5*(1). Retrieved March 11, 2010 from http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE3EDD5-0AD1-6086-28804D3C49D798A0.pdf

Casadei, F., Savoldi, A., & Gubian, P. (2005). *SIMbrush: an Open Source Tool for GSM and UMTS Forensics Analysis.* Paper presented at the First International Workshop on Systematic Approaches to Digital Forensic Engineering. doi: 10.1109/SADFE.2005.22

Casey, E. (2009). Digital forensics: Coming of age. *Digital Investigation, 6,* 1-2. doi: 10.1016/j.diin.2009.08.001

Casey, E. (2007). What does ''forensically sound'' really mean? *Digital Investigation, 4,* 49-50. doi: 10.1016/j.diin.2007.05.001

Casey, E. (2007). Attacks against forensic analysis. *Digital Investigation, 4*, 105-106. doi: 10.1016/j.diin.2008.01.001

Chennamma, H. R., Rangarajan, L., & Rao, M. S. (2009). Robust Near Duplicate Image Matching for Digital Image Forensics. *International Journal of Digital Crime and Forensics, 1*(3), 62-79. doi: 10.4018/jdcf.2009070104

Cohen, K. (2007). Digital Still Camera Forensics. *Small Scale Digital Device Forensics Journal, 1*(1), 1-8. Retrieved April 11, 2010 from www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf

Danker, S. (2009). *Viability of Using Hash Values in Mobile Phone Forensics* [PowerPoint slides]. Presented at Mobile World Forensics 2009. Retrieved April 16, 2010 from www.mobileforensicsworld.org/2009/presentations/MFW2009_DANKNER_HashingIntegrityandMobilePhones.pdf

Danker, S., Ayers, R., & Mislan, R. P. (2009). Hashing Techniques for Mobile Device Forensics. *Small Scale Digital Device Forensics Journal, 3*(1), 1-6. Retrieved April 01, 2010 from www.ssddfj.org/.../SSDDFJ_V3_1_Dankner_Ayers_Mislan.pdf

Duvinage, N. (2008). *Advanced GSM Forensics* [PowerPoint slides]. Presented at Mobile Forensics World 2008. Retrieved April 02, 2010 from www.mobileforensicsworld.org/2008/presentations/MFW2008_Duvinage_AdvancedGSMForensics.pdf

Federal Bureau of Investigation. (2009). *Mobile Forensics: A Path Forward* [PowerPoint slides]. Presented at Mobile Forensics World 2009. Retrieved April 05, 2010 from www.mobileforensicsworld.org/2009/presentations/MFW2009_VOSS_MobileForensicsAPathForward.pdf

Frakes, D. (2009). *Inside iPhone 3.0's Remote Wipe feature: How long a wipe takes—and how secure it is— depends on which device you use.* Retrieved April 11, 2010, from www.macworld.com/article/141605/2009/07/remotewipe.html

Gratzer, V., & Naccache, D. (2006). Cryptography, Law Enforcement, and Mobile Communications. *Security & Privacy, IEEE, 6*(4), 67-70. doi: 10.1109/MSP.2006.148

Gratzer, V., Naccache, D., & Znaty, D. (2006). *Law enforcement, forensics and mobile communications.* Paper presented at the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops. doi: 10.1109/PERCOMW.2006.73

Grossman, L. (2007). *Invention Of the Year: The iPhone.* Retrieved from www.time.com/time/specials/2007/article/0,28804,1677329_1678542,00.html

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic software tools - Searching Function. *Digital Investigation, 6,* 12-22. doi: 10.1016/j.diin.2009.06.015

Hadjidj, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A., & Benredjem, D. (2009). Towards an integrated e-mail forensic analysis framework. *Digital Investigation, 5,* 124-137. doi: 10.1016/j.diin.2009.01.004

Harrill, D. C., & Mislan, R. P. (2007). A Small Scale Digital Device Forensics Ontology. *Small Scale Digital Device Forensics Journal, 1*(1), 1-7. Retrieved April 11, 2010 from www.ssddfj.org/papers/SSDDFJ_V1_1_Harrill_Mislan.pdf

Heusser, M. (2005). *Methodology Design: The Way We Do Things Around Here.* Retrieved October 1, 2009, from http://www.informit.com/articles/article.aspx?p=434641&seqNum=2

Hoog, A. (2009). *Android Forensics* [PowerPoint slides]. Presented at Mobile Forensics World 2009. Retrieved April 08, 2010 from www.mobileforensicsworld.org/2009/.../MFW2009_HOOG_ AndroidForensics.pdf

Hoog, A., & Gaffaney, K. (2009). *iPhone Forensics* [White Paper]. Retrieved February 20, 2010 from http://viaforensics.com/wpinstall/wp-content/uploads/2009/03/iPhone-Forensics-2009.pdf

Honan, M. (2007). *Apple unveils iPhone.* Retrieved from www.macworld.com/article/54769/2007/01/iphone.html

Induruwa, A. (2009). Mobile phone forensics: an overview of technical and legal aspects. *International Journal of Electronic Security and Digital Forensics, 2*(2), 169-181. doi: 10.1504/IJESDF.2009.024901

Iqbal, F., Hadjidj, R., Fung, B. C. M., & Debbabi, M. (2008). A novel approach of mining write-prints for authorship attribution in e-mail forensics. *Digital Investigation, 5,* 42-51. doi: 10.1016/j.diin.2008.05.001

Jahankhani, H. (2009). Criminal investigation and forensic tools for smartphones. *International Journal of Electronic Security and Digital Forensics, 2*(4), 387 – 406. doi: 10.1504/IJESDF.2009.027671

Joyce, R., Powers, J. & Adelstein, F. (2008). MEGA: A tool for Mac OS X operating system and application forensics. *Digital Investigation*, 5, 83-90. doi:10.1016/j.diin.2008.05.011

Kiley, M., Shinbara, T., & Rogers, M. (2007). iPod Forensics Update. *International Journal of Digital Evidence, 6*(1). Retrieved April 11, 2010 from http://www.utica.edu/academic/institutes/ecii/publications/articles/B40DD0EA-D340-962F-F98B868F3C69129F.pdf

Koennecke, K. (2008). *Forensic Analysis of Cell Phones and SIM Cards* [PowerPoint slides]. Presented at Mobile Forensics World 2008. Retrieved May 05, 2010 from www.mobileforensicsworld.org/2008/presentations/MFW2008_Mansell_EssentialToolsforPhoneExaminers_SLIDES.pdf

Kubasiak, R. R. (2007). *Macintosh Forensics: A Guide for the Forensically Sound Examination of a Macintosh Computer* [White Paper]. Retrieved from http://www.macforensicslab.com/ProductsAndServices/index.php?main_page=index&cPath=11&zenid=c0b18ef733395ce4284df183e5777c9c

Levine, B. & Liberatore, M. (2009). MEGA DEX: Digital evidence provenance supporting reproducibility and comparison. *Digital Investigation*, 6(2009), S48-S56. doi:10.1016/j.diin.2009.06.011

Losavio, M., Wilson, D., & Elmaghraby, A. (2006). Prevalence, Use, and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small-Scale Digital Devices. *Journal of Digital Forensic Practice, 1*(4), 291-296. doi: 10.1080/15567280701418080

Luck, J., & Stokes, M. (2008). An Integrated Approach to Recovering Deleted Files from NAND Flash Data. *Small Scale Digital Device Forensics Journal, 2*(1), 1-13. Retrieved April 25, 2010 from http://www.ssddfj.org/papers/SSDDFJ_V2_1_Luck_Stokes.pdf

Lurie, D. (2007). *iPhone Announced: The Unofficial Apple Weblog.* Retrieved from www.tuaw.com/2007/01/09/iphone-announced/

Malinowski, C., & Noble, R. (2007). Hashing and data integrity: Reliability of hashing and granularity size reduction. *Digital Investigation, 4,* 98-104. doi: 10.1016/j.diin.2007.03.001

Mansell, K. (2008). Essential Online Tools for Phone Examiners [PowerPoint slides]. Presented at Mobile Forensics World 2008. Retrieved April 25, 2010 from www.mobileforensicsworld.org/2008/presentations/MFW2008_Mansell_EssentialToolsforPhoneExaminers_SLIDES.pdf

Mansell, K. (2008). Digging Deeper: Finding Gold [PowerPoint slides]. Presented at Mobile Forensics World 2008. Retrieved April 25, 2010 from www.mobileforensicsworld.org/2008/presentations/MFW2008_Mansell_DiggingDeeperFindingGold.pdf

McDonald, K. (2005). To image a Macintosh. *Digital Investigation, 2,* 175-79. doi: 10.1016/j.diin.2005.07.004

Me, G., & Rossi, M. (2008). *Internal forensic acquisition for mobile equipments.* Paper presented at the IEEE International Symposium on Parallel and Distributed Processing. doi: 10.1109/IPDPS.2008.4536557

Microsoft Corporation. (2010). *Glossary.* Retrieved April 11, 2010, from http://msdn.microsoft.com/en-us/library/ee394786(v=PROT.13).aspx

Murphy, C. A. (2009). The Fraternal Clone Method for CDMA Cell Phones. *Small Scale Digital Device Forensics Journal, 3*(1), 1-8. Retrieved March 11, 2010 from www.ssddfj.org/papers/SSDDFJ_V3_1_Murphy.pdf

Narayanaswami, C. (2005). *Form factors for mobile computing and device symbiosis.* Paper presented at the Eight International Conference on Document Analysis and Recognition. doi: 10.1109/ICDAR.2005.114

Nutter, B. (2008). Pinpointing TomTom location records: A forensic analysis. *Digital Forensics, 5,* 10-18. doi: 10.1016/j.diin.2008.06.003

Oberheide, J., & Jahanian, F. (2010). *When mobile is harder than fixed (and vice versa): Demystifying security challenges in mobile environments*. Paper presented at the Eleventh Workshop on Mobile Computing Systems & Applications. Retrieved from http://doi.acm.org/10.1145/1734583.1734595

O’Connor, T. P. (2009). Provider Side Cell Phone Forensics. *Small Scale Digital Device Forensics Journal, 3*(1), 1-4. Retrieved March 15, 2010 from www.ssddfj.org/papers/SSDDFJ_V3_1_OConnor.pdf

Olsson, J. & Boldt, M. (2009). Computer forensic timeline visualization tool. *Digital Investigation*, 6(2009), S78-S87. doi: 10.1016/j.diin.2009.06.008

Palmer, P. (2008). *iPhone 3G Announced: The Unofficial Apple Weblog.* Retrieved from www.tuaw.com/2008/06/09/iphone-3g-announced/

Pan, L., & Batten, L. M. (2009). Robust performance testing for digital forensic tools. *Digital Investigation, 6,* 71-81. doi: 10.1016/j.diin.2009.02.003

Punja, S. G., & Mislan, R. P. (2008). Mobile Device Analysis. *Small Scale Digital Device Forensics Journal, 2*(1), 1-16. Retrieved April 11, 2010 from www.ssddfj.org/papers/SSDDFJ_V2_1_Punja_Mislan.pdf

Punja, S. (2009). *BlackBerry Forensics* [PowerPoint slides]. Presented at Mobile Forensics World 2009. Retrieved April 09, 2010 from www.mobileforensicsworld.org/2009/presentations/MFW2009_PUNJA_BlackberryForensics.pdf

Pereira, M. T. (2009). Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records. *Digital Forensics, 5,* 93-103. doi: 10.1016/j.diin.2009.01.003

Ridder, C. K. (2009). Evidentiary Implications of Potential Security Weaknesses in Forensic Software. *International Journal of Digital Crime and Forensics,1*(3), 80-91. doi: 10.4018/jdcf.2009070105

Sande, S. (2009). *WWDC 2009 Keynote meta-liveblog: The Unofficial Apple Weblog.* Retrieved from www.tuaw.com/2009/06/08/wwdc-2009-keynote-meta-liveblog/

Sencar, H. T., & Memon, N. (2009). Identification and recovery of JPEG files with missing fragments. *Digital Investigation*, *6,* 88-98. doi: 10.1016/j.diin.2009.06.007

Seriot, N. (2009). iPhone Privacy [PowerPoint slides]. Geneva, Switzerland. Retrieved April 18, 2010 from http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf

Slay, J., & Przibilla. (2007). *iPod Forensics: Forensically Sound Examination of an Apple iPod.* Paper presented at the 40th Annual Hawaii International Conference on System Sciences. doi: 10.1109/HICSS.2007.300

Slivka, E. (2010). *Gartner: iPhone Sales Double in 2009 as Apple Claims Third Place in Smartphone Sales.* Retrieved from http://www.macrumors.com/2010/02/23/gartner-iphone-sales-double-in-2009-as-apple-claims-third-place-in-smartphone-sales/

Souvignet, T. (2009). *Using Bootloaders to Dump the Internal Flash Memory of Mobile Phones* [PowerPoint slides]. Presented at Mobile Forensics World 2009. Retrieved April 30, 2010 from www.mobileforensicsworld.org/2009/presentations/MFW2009_SOUVIGNET_BootloadersDumpInternalFlashMemory.pps

Strawn, C. (2009). Expanding the Potential for GPS Evidence Acquisition. *Small Scale Digital Device Forensics Journal, 3*(1), 1-12. Retrieved April 13, 2010 from www.ssddfj.org/papers/SSDDFJ_V3_1_Strawn.pdf

Tsai, M. J., Lai, C. L., & Liu, J. (2007). *Camera/ Mobile Phone Source Identification For Digital Forensics*. Paper presented at the IEEE International Conference on Acoustics, Speech and Signal Processing. doi: 10.1109/ICASSP.2007.366212

University of Pennsylvania: Information Systems & Computing. (2010). *Approximate Desktop, Notebook, & Netbook Power Usage.* Retrieved from www.upenn.edu/computing/provider/docs/hardware/powerusage.html

U.S. Department of Justice. (2007). *Investigative Uses of Technology: Devices, Tools, and Techniques.* Washington, USA: Keisler, P. D., Daley, C. K., & Hagy, D. W.

Vodafone Group. (2008). *Vodafone and Apple to bring iPhone 3G to Australia, Italy, New Zealand & Portugal on July 11*. Retrieved from www.vodafone.co.nz/about/media-centre/2008-media-releases/apple-iphone-3G.jsp

Westman, M. (2009). *Complete Mobile Phones Forensic Examination: Why we need both Logical & Physical Extractions* [PowerPoint slides]. Presented at Mobile Forensics World 2009. Retrieved April 12, 2010 from www.mobileforensicsworld.org/2009/presentations/MFW2009_Westman_LogicalandPhysicalExtractions.pdf

Zdziarski, J. (2008). *iPhone Forensics* (1st edition). Sebastopol, USA: O'Reilly Media, Inc.

Zhu, G., Huang, J., Kwong, S., & Yang, J. (2009). A Study on the Randomness Measure of Image Hashing. *IEEE Transactions on Information Forensics and Security, 4*(4), 928-932. doi: 10.1109/TIFS.2009.2033737

Appendix A - Catalog

Column Key
iTunes Backup - A
iTunes Backup (Jailbroken) - B
Device Seizure - C
iPhone Explorer - D
MobileSyncBrowser - E
Mobilyze - F
Mobilyze (Jailbroken) - G
Oxygen Forensics - H
Oxygen Forensics (Jailbroken) - I

The full electronic copy of Appendix A in PDF format can be downloaded from:
http://goo.gl/K5ujI

Rating	Classification	MD5 Hash	File Name	Full Path	A	B	C	D	E	F	G	H	I
2	OS	04b33c204ea83d7b46868d02c56ee4ab	TrustStore.sqlite3	/Volumes/Data/Keychains/TrustStore.sqlite3	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	f476e68db9407a3418964a7e6e34b14d	keychain-2.db	/Volumes/Data/Keychains/keychain-2.db									
2	OS	7158502a1cf9a8fa3f49c4146ee4f3b3	ocspcache.sqlite3	/Volumes/Data/Keychains/ocspcache.sqlite3									
2	OS	2de6a04cdba79ed13580c47dfd70cc5f	com.apple.springboard.plist	/Volumes/Data/Managed Preferences/mobile/com.apple.springboard.plist	Y	Y		Y	Y	Y	Y	Y	Y
2	OS	2fb87af12a45b051218cde908e1339bb	ABE3CCC2-FF22-429F-9C87-AFDB9DE6C719	/Volumes/Data/MobileDevice/ProvisioningProfiles/ABE3CCC2-FF22-429F-9C87-AFDB9DE6C719	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	17204bbe354101fc86e77bbef614c5e1	C4A5B07E-5FCD-4A60-A43F-B6B0583A94CD	/Volumes/Data/MobileDevice/ProvisioningProfiles/C4A5B07E-5FCD-4A60-A43F-B6B0583A94CD	Y	Y			Y	Y	Y	Y	Y
2	OS	d41d8cd98f00b204e9800998ecf8427e	lock	/Volumes/Data/cache/apt/archives/lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	6473f811cbafca3ee85d81cddc227b0d	pkgcache.bin	/Volumes/Data/cache/apt/pkgcache.bin									
2	OS	d47a4b5c6a145ae9d1705f0b36cf8dc2	srcpkgcache.bin	/Volumes/Data/cache/apt/srcpkgcache.bin									
2	OS	d41d8cd98f00b204e9800998ecf8427e	.launchd_use_gmalloc	/Volumes/Data/db/.launchd_use_gmalloc	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	c797d66886ea93620e3ef4656f8a2467	en0-1,0:26:4a:c4:22:ee	/Volumes/Data/db/dhcpclient/leases/en0-1,0:26:4a:c4:22:ee									
2	OS	d41d8cd98f00b204e9800998ecf8427e	overrides.plist	/Volumes/Data/db/launchd.db/com.apple.launchd/overrides.plist	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	28e3497aa0acae03edee06ed4d7dc72b	localtime	/Volumes/Data/db/timezone/localtime									
2	OS	d41d8cd98f00b204e9800998ecf8427e	lock	/Volumes/Data/lib/apt/lists/lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	c76a853b7fbfeffa655a5c53f57677c4	available	/Volumes/Data/lib/dpkg/available									
2	OS	c76a853b7fbfeffa655a5c53f57677c4	available-old	/Volumes/Data/lib/dpkg/available-old									
2	OS	ef879736bb11c74e67471ec99d35d866	apr-lib.list	/Volumes/Data/lib/dpkg/info/apr-lib.list									
2	OS	32a4ea3d08eed72ede08a225cb1c10b0	apt7-key.list	/Volumes/Data/lib/dpkg/info/apt7-key.list									
2	OS	92efc2dee870b92ed0e0abcd35b15731	apt7-lib.list	/Volumes/Data/lib/dpkg/info/apt7-lib.list									
2	OS	4105cc31a20baaa0a2850cbe0d0a3de8	base.list	/Volumes/Data/lib/dpkg/info/base.list									
2	OS	5b584bb1da554532a6b0762c537777c8	bash.list	/Volumes/Data/lib/dpkg/info/bash.list									
2	OS	c2c4acc84776bc4df29588e6bf8db008	bigboss.list	/Volumes/Data/lib/dpkg/info/bigboss.list									
2	OS	09700673f1856adf5f98b0c1433c8563	bzip2.list	/Volumes/Data/lib/dpkg/info/bzip2.list									
2	OS	ba0d4d8be7d72da1fde74774ad17a1c9	coreutils-bin.list	/Volumes/Data/lib/dpkg/info/coreutils-bin.list									
2	OS	f530de65b768baab30da1355d5f0909a	darwintools.list	/Volumes/Data/lib/dpkg/info/darwintools.list									
2	OS	380c7aa9b8b377f15a5c7d21fd460953	diffutils.list	/Volumes/Data/lib/dpkg/info/diffutils.list									
2	OS	8868ed822537563f8eee4b7a4b63df04	diskdev-cmds.list	/Volumes/Data/lib/dpkg/info/diskdev-cmds.list									
2	OS	7ebd04789730b28f5903707058e4277e	dpkg.list	/Volumes/Data/lib/dpkg/info/dpkg.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	essential.list	/Volumes/Data/lib/dpkg/info/essential.list									
2	OS	b92bc18d01e7f5dcad7a3c65fe910ff1	findutils.list	/Volumes/Data/lib/dpkg/info/findutils.list									
2	OS	802931c44137312e8ec9531dc015878c	firmware-sbin.list	/Volumes/Data/lib/dpkg/info/firmware-sbin.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	firmware.list	/Volumes/Data/lib/dpkg/info/firmware.list									
2	OS	1303065d5d7e41c6bd53a835e08a4987	gnupg.list	/Volumes/Data/lib/dpkg/info/gnupg.list									
2	OS	49c25080293aab9ea95528b8cb7bb5c2	grep.list	/Volumes/Data/lib/dpkg/info/grep.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.accelerometer.list	/Volumes/Data/lib/dpkg/info/gsc.accelerometer.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.accessibility.list	/Volumes/Data/lib/dpkg/info/gsc.accessibility.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.all-features.list	/Volumes/Data/lib/dpkg/info/gsc.all-features.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.app-store.list	/Volumes/Data/lib/dpkg/info/gsc.app-store.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.application-installation.list	/Volumes/Data/lib/dpkg/info/gsc.application-installation.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.armv6.list	/Volumes/Data/lib/dpkg/info/gsc.armv6.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.armv7.list	/Volumes/Data/lib/dpkg/info/gsc.armv7.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.auto-focus-camera.list	/Volumes/Data/lib/dpkg/info/gsc.auto-focus-camera.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.bluetooth.list	/Volumes/Data/lib/dpkg/info/gsc.bluetooth.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.encode-aac.list	/Volumes/Data/lib/dpkg/info/gsc.encode-aac.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.encrypted-data-partition.list	/Volumes/Data/lib/dpkg/info/gsc.encrypted-data-partition.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.fcc-logos-via-software.list	/Volumes/Data/lib/dpkg/info/gsc.fcc-logos-via-software.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.gas-gauge-battery.list	/Volumes/Data/lib/dpkg/info/gsc.gas-gauge-battery.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.gps.list	/Volumes/Data/lib/dpkg/info/gsc.gps.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.hiccough-interval.list	/Volumes/Data/lib/dpkg/info/gsc.hiccough-interval.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.international-settings.list	/Volumes/Data/lib/dpkg/info/gsc.international-settings.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.launch-applications-while-animating.list	/Volumes/Data/lib/dpkg/info/gsc.launch-applications-while-animating.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.load-thumbnails-while-scrolling.list	/Volumes/Data/lib/dpkg/info/gsc.load-thumbnails-while-scrolling.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.location-services.list	/Volumes/Data/lib/dpkg/info/gsc.location-services.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.magnetometer.list	/Volumes/Data/lib/dpkg/info/gsc.magnetometer.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.microphone.list	/Volumes/Data/lib/dpkg/info/gsc.microphone.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.mms.list	/Volumes/Data/lib/dpkg/info/gsc.mms.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.music-store.list	/Volumes/Data/lib/dpkg/info/gsc.music-store.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.nike-ipod.list	/Volumes/Data/lib/dpkg/info/gsc.nike-ipod.list									

2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.not-green-tea.list	/Volumes/Data/lib/dpkg/info/gsc.not-green-tea.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.opengles-1.list	/Volumes/Data/lib/dpkg/info/gsc.opengles-1.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.opengles-2.list	/Volumes/Data/lib/dpkg/info/gsc.opengles-2.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.peer-peer.list	/Volumes/Data/lib/dpkg/info/gsc.peer-peer.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.proximity-sensor.list	/Volumes/Data/lib/dpkg/info/gsc.proximity-sensor.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.ringer-switch.list	/Volumes/Data/lib/dpkg/info/gsc.ringer-switch.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.sms.list	/Volumes/Data/lib/dpkg/info/gsc.sms.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.stand-alone-contacts.list	/Volumes/Data/lib/dpkg/info/gsc.stand-alone-contacts.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.still-camera.list	/Volumes/Data/lib/dpkg/info/gsc.still-camera.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.telephony-maximum-generation.list	/Volumes/Data/lib/dpkg/info/gsc.telephony-maximum-generation.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.telephony.list	/Volumes/Data/lib/dpkg/info/gsc.telephony.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.unified-ipod.list	/Volumes/Data/lib/dpkg/info/gsc.unified-ipod.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.video-camera.list	/Volumes/Data/lib/dpkg/info/gsc.video-camera.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.voice-control.list	/Volumes/Data/lib/dpkg/info/gsc.voice-control.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.volume-buttons.list	/Volumes/Data/lib/dpkg/info/gsc.volume-buttons.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.wifi.list	/Volumes/Data/lib/dpkg/info/gsc.wifi.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.youtube-plugin.list	/Volumes/Data/lib/dpkg/info/gsc.youtube-plugin.list									
2	OS	b8f46d6de6571b94ae7ced49112f88f0	gsc.youtube.list	/Volumes/Data/lib/dpkg/info/gsc.youtube.list									
2	OS	46da0719a4cbc1932751ad802b767b4b	gzip.list	/Volumes/Data/lib/dpkg/info/gzip.list									
2	OS	1680d2308e92ed65c5cdddbeb1c69c83	ispazio.net.list	/Volumes/Data/lib/dpkg/info/ispazio.net.list									
2	OS	935bba34ef3551f471fbd829312e41a2	lzma.list	/Volumes/Data/lib/dpkg/info/lzma.list									
2	OS	7e34c221c7a75074af3f3cf9f9471c3a	modmyifone.list	/Volumes/Data/lib/dpkg/info/modmyifone.list									
2	OS	53151eaa31e706124dca3b2124efb62d	ncurses.list	/Volumes/Data/lib/dpkg/info/ncurses.list									
2	OS	f21b47ffdff21d6f4aae69892cc15eda	netcat.list	/Volumes/Data/lib/dpkg/info/netcat.list									
2	OS	a96996669a5dbb3049465fb7e68c6c10	openssh.extrainst_	/Volumes/Data/lib/dpkg/info/openssh.extrainst_									
2	OS	c90b494b3bacce1c9a6fd595ececac8c	openssh.list	/Volumes/Data/lib/dpkg/info/openssh.list									
2	OS	934cdca561bff41198a611af062af751	openssh.prerm	/Volumes/Data/lib/dpkg/info/openssh.prerm									
2	OS	9eddced85d9f748c329f7abce638cb33	openssl.list	/Volumes/Data/lib/dpkg/info/openssl.list									
2	OS	8dde7c41a0c013c19a4f5e736a3887e9	pam-modules.list	/Volumes/Data/lib/dpkg/info/pam-modules.list									
2	OS	f3a2bcd32144e57a064694ae4cb48423	pam.list	/Volumes/Data/lib/dpkg/info/pam.list									
2	OS	2626939f43f7f7c13f6808525a6ff5d9	pcre.list	/Volumes/Data/lib/dpkg/info/pcre.list									
2	OS	db59e29039411e0c6f22948bf52b783a	profile.d.list	/Volumes/Data/lib/dpkg/info/profile.d.list									
2	OS	c291b38b7a463f808195d3284dc2f126	readline.list	/Volumes/Data/lib/dpkg/info/readline.list									
2	OS	ada5b3a6f602623b0f4eb6f90bf7385f	saurik.list	/Volumes/Data/lib/dpkg/info/saurik.list									
2	OS	577f68dadfd0d3eb845a97ec3210fc40	sed.list	/Volumes/Data/lib/dpkg/info/sed.list									
2	OS	7cc20d618f230316a0b7ce0ff6e7064d	shell-cmds.list	/Volumes/Data/lib/dpkg/info/shell-cmds.list									
2	OS	c804d1e46d9e59579a673385af68916e	system-cmds.list	/Volumes/Data/lib/dpkg/info/system-cmds.list									
2	OS	873ff574cd9343982490a6746054f1d5	tar.list	/Volumes/Data/lib/dpkg/info/tar.list									
2	OS	d5c866069c881578feb17af4f757fff2	uikittools.list	/Volumes/Data/lib/dpkg/info/uikittools.list									
2	OS	0ddd7940d126aaedd63dacca59a56210	yellowsn0w.com.list	/Volumes/Data/lib/dpkg/info/yellowsn0w.com.list									
2	OS	729a563858ebee41c657761c6a57ed65	zodttd.list	/Volumes/Data/lib/dpkg/info/zodttd.list									
2	OS	d41d8cd98f00b204e9800998ecf8427e	lock	/Volumes/Data/lib/dpkg/lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	54d598ffeb29a8ebbac873e1919662b0	status	/Volumes/Data/lib/dpkg/status									
2	OS	cb8a8bd83b72789355e772efa5bd16ab	status-old	/Volumes/Data/lib/dpkg/status-old									
2	OS	d41d8cd98f00b204e9800998ecf8427e	Lock	/Volumes/Data/lib/dpkg/triggers/Lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	d41d8cd98f00b204e9800998ecf8427e	Unincorp	/Volumes/Data/lib/dpkg/triggers/Unincorp	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	62197f2f39077aaecbf7c5ff6329e613	term.log	/Volumes/Data/log/apt/term.log									
2	OS	a4dff740a122fa842dc57a2a90bbcc66	general.log	/Volumes/Data/logs/AppleSupport/general.log									
2	OS	ab54419a4a4fe9c49611bb09972c7890	9LS1142UY2	/Volumes/Data/logs/IQAgent/9LS1142UY2									
2	OS	4763799a9e00ae63df8634039bc6047a	9LS1O12Z	/Volumes/Data/logs/IQAgent/9LS1O12Z									
2	OS	3961f7f3d7605698eca3495b18acd7c4	COV48Y3W	/Volumes/Data/logs/IQAgent/COV48Y3W									
2	OS	d41d8cd98f00b204e9800998ecf8427e	fairplayd.log	/Volumes/Data/logs/fairplayd.log	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	8bbda6b6a944a8688465e30d787e1ab0	lockdownd.log	/Volumes/Data/logs/lockdownd.log									
2	OS	2bd0117aff80164969e94f5d15ec4c79	log-bb-live-stats.txt	/Volumes/Data/logs/log-bb-live-stats.txt									
2	OS	341ffd9e59f9271ad9507e646dfff6f9	.forward	/Volumes/Data/mobile/.forward									
2	OS	d41d8cd98f00b204e9800998ecf8427e	.localized	/Volumes/Data/mobile/Library/.localized	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	AddressBook	eca2ffb1050f10c242dfaf347b2dbd6c	AddressBook.sqlitedb	/Volumes/Data/mobile/Library/AddressBook/AddressBook.sqlitedb									
2	AddressBook	dcc8f9bacbd229a81fc3d1134c7280d3	AddressBookImages.sqlitedb	/Volumes/Data/mobile/Library/AddressBook/AddressBookImages.sqlitedb									
2	Cache	d41d8cd98f00b204e9800998ecf8427e	AccessToMigrationLock	/Volumes/Data/mobile/Library/Caches/AccessToMigrationLock	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	Cache	d41d8cd98f00b204e9800998ecf8427e	AccountMigrationInProgress	/Volumes/Data/mobile/Library/Caches/AccountMigrationInProgress	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	Cache	d41d8cd98f00b204e9800998ecf8427e	SBShutdownCookie	/Volumes/Data/mobile/Library/Caches/SBShutdownCookie	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	Cache	3a8808c155346cfb28e267814773d8d6	4920F09CE9374925AD3A20B570B34D96	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/4920F09CE9374925AD3A20B570B34D96									
2	Cache	d4b1280cf17aba6172538f44457899f5	HT2B7EP525.com.gravitini.george	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/HT2B7EP525.com.gravitini.george									
2	Cache	e3cdcc74259c68815041033dd8321b9e	MZCZ5SMF8U.iCacher	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/MZCZ5SMF8U.iCacher									
2	Cache	1cbf8c00ef2bbc10b5d3308f92e74692	NetNewsWire	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/NetNewsWire									
2	Cache	fae5e1ff4f7c52235c90a6aae78598d7	UBI-018-WW	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/UBI-018-WW									
2	Cache	e0f3acd2e46fa8ed581789e010412fc4	ca.ianpage.Mactracker	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/ca.ianpage.Mactracker									
2	Cache	85d869d357376a93c0479fc2dae3ac8a	com.adobe.PSMobile	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.adobe.PSMobile									
2	Cache	a3332cb1f5b3c1623e0a356f581419da	com.allrecipes.dinnerspinner	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.allrecipes.dinnerspinner									
2	Cache	424c33449b5727576f9243d3972fa9a9	com.apple.AppStore	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.AppStore									
2	Cache	f57f1d256b046f57175791a95a86fb69	com.apple.DemoApp	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.DemoApp									
2	Cache	78e5d19cb7404796f6a7d1866b351905	com.apple.Maps	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.Maps									
2	Cache	97f15966a010edbe94a21a5e9a73fa2b	com.apple.MobileAddressBook	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.MobileAddressBook									

2	Cache	8133239354b765a48732201b2f94294a	com.apple.MobileSMS	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.MobileSMS									
2	Cache	fe9d15ffc26ea8f860a9421dea6a1c01	com.apple.MobileStore	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.MobileStore									
2	Cache	d6063ffab74a4f7f75df9a6e0e483f0b	com.apple.Preferences	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.Preferences									
2	Cache	4b0d7777a7f9fd2a22008d01b18471f0	com.apple.Remote	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.Remote									
2	Cache	04e096cffede0d26de766a7b20d39770	com.apple.VoiceMemos	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.VoiceMemos									
2	Cache	f57f1d256b046f57175791a95a86fb69	com.apple.WebSheet	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.WebSheet									
2	Cache	97814b5bd083bcf0a35986e0759e9f94	com.apple.calculator	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.calculator									
2	Cache	0800ca258aaf128d3880038ddcaac002	com.apple.compass	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.compass									
2	Cache	f57f1d256b046f57175791a95a86fb69	com.apple.fieldtest	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.fieldtest									
2	Cache	120014891ad46cebdc4c8b836f1cfe16	com.apple.iwork.KeynoteRemote	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.iwork.KeynoteRemote									
2	Cache	54e56ff51bd0746f5a95b12fdc1fa588	com.apple.me.Gallery	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.me.Gallery									
2	Cache	2b8e73bc258f9b611b708f98bdc77dd9	com.apple.mobilecal	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobilecal									
2	Cache	87181a3bd9bbb4561b88de453e1ffcf1	com.apple.mobileipod-MediaPlayer	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobileipod-MediaPlayer									
2	Cache	3c449b5f597f53d1b0e540815c7f5631	com.apple.mobilemail	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobilemail									
2	Cache	d07c671d22c5fb86134776c891988bf4	com.apple.mobilenotes	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobilenotes									
2	Cache	031c61dad5456ac94180379d3ed1dc7e	com.apple.mobilephone	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobilephone									
2	Cache	0214e25cb00ef8a14f5e958f8bbcb258	com.apple.mobilesafari	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobilesafari									
2	Cache	8e44fadb70077cad1e7d61825d88d43f	com.apple.mobileslideshow-Camera	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobileslideshow-Camera									
2	Cache	364ba84d876f4a92eca8630b083e7aea	com.apple.mobileslideshow-Photos	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobileslideshow-Photos									
2	Cache	fd47dab49d1c5d278cca08fccfed5267	com.apple.mobiletimer	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.mobiletimer									
2	Cache	2397ed0081bfcbbe04d6226f90e634be	com.apple.nike	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.nike									
2	Cache	f57f1d256b046f57175791a95a86fb69	com.apple.springboard	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.springboard									
2	Cache	2edc9dd59156a2346f724de1a215ea80	com.apple.stocks	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.stocks									
2	Cache	6351461d7bc1f048e8b6706762406ad0	com.apple.weather	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.weather									
2	Cache	33ef961c21b52dcd222c19c02f6ac902	com.apple.youtube	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.apple.youtube									
2	Cache	66cf0dd3cdab8c108ba07508c0cb7dc1	com.atebits.Tweetie2	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.atebits.Tweetie2									
2	Cache	8e6e33d82dbe8e68cd64a393ced72f9c	com.barlow.TRWC	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.barlow.TRWC									
2	Cache	0b04187bd92ae6e17dd479354592cd49	com.ea.simcitybv	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.ea.simcitybv									
2	Cache	c61eb57c23a0bbe97c3b6c8999641535	com.ea.trivialpursuit.bv	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.ea.trivialpursuit.bv									
2	Cache	18eaf4ee2a7f02df792ff965ec689f86	com.facebook.Facebook	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.facebook.Facebook									
2	Cache	1161b371347a9b65c20f2835eb77d4ca	com.firemint.flightcontrol	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.firemint.flightcontrol									
2	Cache	f104d962e864ed26d5543f2ab147ca0e	com.gameloft.AVATAR	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.gameloft.AVATAR									
2	Cache	bf8abca0cac137a1fc45bd100a54ab13	com.gameloft.uno	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.gameloft.uno									
2	Cache	72babaf344f22466a3d84f0782f8d7bc	com.gamerizon.chopchopninjalite	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.gamerizon.chopchopninjalite									
2	Cache	ff018d86bfa641eb49dedffaf162265a	com.gamerizon.chopchoprunner	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.gamerizon.chopchoprunner									
2	Cache	ce1a2b6db9f23ae5b36d8b5ef6766f72	com.getdropbox.Dropbox	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.getdropbox.Dropbox									
2	Cache	74ff26b12f938f0b462e9877c927d1f6	com.gravitymobile.MusicIDWorld	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.gravitymobile.MusicIDWorld									
2	Cache	cd34375dee300dac09e991246140544d	com.imdb.imdb	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.imdb.imdb									
2	Cache	7ba56252b0981b23d28fdeab557582c0	com.labpixies.lineup2.free	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.labpixies.lineup2.free									
2	Cache	ce5495484b17ff76c54abe4d1b093544	com.lastpass.ilastpass	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.lastpass.ilastpass									
2	Cache	aa657bf4eea79309c7db9626d8132a75	com.lesscode.AucklandAirport	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.lesscode.AucklandAirport									
2	Cache	99ebf8f23b5f518b5284a6160035169b	com.ookla.speedtest	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.ookla.speedtest									
2	Cache	282630a82221841ab3ceab2d5e99fcd3	com.pangea.cromag	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.pangea.cromag									
2	Cache	fc65022531ceef5fe5382a5df8908a3a	com.pressokentertainment.fingerphysics	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.pressokentertainment.fingerphysics									
2	Cache	1c062704ca620addf7e29c2f6390e39a	com.shazam.Shazam	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.shazam.Shazam									
2	Cache	8ae946d5990b8ea6b5b86e6c71e5d107	com.skype.skype	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.skype.skype									
2	Cache	4d05de378a3bef103f2ea91b681fcfe5	com.tapulous.taptaprevengeIII	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.tapulous.taptaprevengeIII									
2	Cache	e586d1b60a5d846660c251d8687e5328	com.vgmobile.cnk2	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.vgmobile.cnk2									
2	Cache	26295038bc34c22058e7413c43947f2e	com.yourcompany.ZenbuSearch	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/com.yourcompany.ZenbuSearch									
2	Cache	c91f26ec077614760fbffdc0e704ce93	nz.co.airnz.mPassiPhone	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/nz.co.airnz.mPassiPhone									
2	Cache	9436060cc4459c87cb15da77099b14a9	nz.co.orsome.guide	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/nz.co.orsome.guide									
2	Cache	2d36c4fec63a234e0044a8c6472cf181	nz.co.tvnz.news	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/nz.co.tvnz.news									
2	Cache	9f72ae3038999b03667a1e4def1c39fd	se.illusionlabs.sway	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache/se.illusionlabs.sway									
2	Cache	fb62234dfeccb34016597fc26cd5158c	4920F09CE9374925AD3A20B570B34D96	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/4920F09CE9374925AD3A20B570B34D96									
2	Cache	6aae9e0f12d81ab52867f9bd1c60e3c7	HT2B7EP525.com.gravitini.george	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/HT2B7EP525.com.gravitini.george									
2	Cache	1f8ac77103762552c97693891efa302a	MZCZ5SMF8U.iCacher	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/MZCZ5SMF8U.iCacher									
2	Cache	bc53b81ed3e15caa00b83d211eeb829a	NetNewsWire	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/NetNewsWire									
2	Cache	5fa0aa1149d39741072f9637cb5b2b53	UBI-018-WW	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/UBI-018-WW									
2	Cache	075f293422bc31675bcdfdd18bf835a8	ca.ianpage.Mactracker	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/ca.ianpage.Mactracker									
2	Cache	f32f1c38bb45ecd5dc932c84b34c286a	com.adobe.PSMobile	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.adobe.PSMobile									
2	Cache	5d2baca93f221932610843d11fc9c719	com.allrecipes.dinnerspinner	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.allrecipes.dinnerspinner									
2	Cache	2169d2624c14a3e45d528da09fc9ba36	com.apple.AppStore	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.AppStore									
2	Cache	ed7fc30bbcd8bc0037ff41ffcb130925	com.apple.DemoApp	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.DemoApp									
2	Cache	ea05c25147b99babca30df062c091fd8	com.apple.Maps	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.Maps									
2	Cache	6b1437f48763feaf631b60059e9bdfd8	com.apple.MobileAddressBook	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.MobileAddressBook									
2	Cache	b7ed262bd56b5ade412dd7bae488537e	com.apple.MobileSMS	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.MobileSMS									
2	Cache	77e61117fc60c036a0d412dad22e0cb6	com.apple.MobileStore	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.MobileStore									
2	Cache	e171153b32dfc3f4cf66ea5315060f3e	com.apple.Preferences	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.Preferences									
2	Cache	95d045f2c2e4c9b099bf333736d0247b	com.apple.Remote	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.Remote									
2	Cache	e249a90b8bb65b0647a06b1d47a9d829	com.apple.VoiceMemos	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.VoiceMemos									
2	Cache	ed7fc30bbcd8bc0037ff41ffcb130925	com.apple.WebSheet	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.WebSheet									
2	Cache	407296faafaa46314e9b4829a03b1ee7	com.apple.calculator	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.calculator									
2	Cache	e5bfb94572ce3534f551da5ad9077ca7	com.apple.compass	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.compass									

2	Cache	ed7fc30bbcd8bc0037ff41ffcb130925	com.apple.fieldtest	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.fieldtest									
2	Cache	3144dd148e025cab241b079db45e6ce8	com.apple.iwork.KeynoteRemote	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.iwork.KeynoteRemote									
2	Cache	9667f4291175d78c5dc09b0d98cfc15b	com.apple.me.Gallery	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.me.Gallery									
2	Cache	242062c967e9f3e5f23fb74903595af8	com.apple.mobilecal	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobilecal									
2	Cache	76cfecad950022f64326e87379fe089f	com.apple.mobileipod-MediaPlayer	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobileipod-MediaPlayer									
2	Cache	98d8674679129355ba117f0a4a06d220	com.apple.mobilemail	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobilemail									
2	Cache	e3607bc6c06bdf8ab07747b41c4c6c8c	com.apple.mobilenotes	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobilenotes									
2	Cache	04d0b12489850554a7cc139782f9f46f	com.apple.mobilephone	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobilephone									
2	Cache	24f14934aaf8e1ecd03e677a923ddcf1	com.apple.mobilesafari	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobilesafari									
2	Cache	819363d33b3bfab230ca71dd65bf14be	com.apple.mobileslideshow-Camera	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobileslideshow-Camera									
2	Cache	f2dc181fccc92be225bd50be8000eabd	com.apple.mobileslideshow-Photos	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobileslideshow-Photos									
2	Cache	12b9e62b640e1bd8ff3c7ab36ed629ce	com.apple.mobiletimer	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.mobiletimer									
2	Cache	ad12a4ba6265b165ed38951df175e75f	com.apple.nike	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.nike									
2	Cache	ed7fc30bbcd8bc0037ff41ffcb130925	com.apple.springboard	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.springboard									
2	Cache	c1c25039acdb3fb459a03fe006044bf6	com.apple.stocks	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.stocks									
2	Cache	d9742116b8bda725374dd4b5d5a4dc0f	com.apple.weather	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.weather									
2	Cache	05d8f33de50a08f4a4e81e6f8837b135	com.apple.youtube	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.apple.youtube									
2	Cache	b072eb6d97b407ca114cb519d37d3373	com.atebits.Tweetie2	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.atebits.Tweetie2									
2	Cache	14997d63df5fe4ebef81067154c5957b	com.barlow.TRWC	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.barlow.TRWC									
2	Cache	37ea067d10223c6a662e19db973dce6a	com.ea.simcitybv	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.ea.simcitybv									
2	Cache	50cf3828415c766332c460782f9ed720	com.ea.trivialpursuit.bv	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.ea.trivialpursuit.bv									
2	Cache	b9d7cfa28e601dfe7797546054f4706e	com.facebook.Facebook	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.facebook.Facebook									
2	Cache	74c066c332d9ea00d9c01e33a529b92a	com.firemint.flightcontrol	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.firemint.flightcontrol									
2	Cache	3c37e6266e49ad9f60d692e47ae44571	com.gameloft.AVATAR	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.gameloft.AVATAR									
2	Cache	1a59e08c0ed2f0523e099bcb31b66e94	com.gameloft.uno	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.gameloft.uno									
2	Cache	a276d4f1284ae2c84da01452f8f91148	com.gamerizon.chopchopninjalite	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.gamerizon.chopchopninjalite									
2	Cache	86100e4297935117b26d3c14cf88c44c	com.gamerizon.chopchoprunner	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.gamerizon.chopchoprunner									
2	Cache	6c39153d418017e6fa9cf1413a6a214c	com.getdropbox.Dropbox	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.getdropbox.Dropbox									
2	Cache	3c9c3d3cd5b4154cc3d10277b8c85cb2	com.gravitymobile.MusicIDWorld	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.gravitymobile.MusicIDWorld									
2	Cache	72264f79aa087e4c2b2608d27f9b1751	com.imdb.imdb	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.imdb.imdb									
2	Cache	ae4e730ffa4a538b03993eb9d8790102	com.labpixies.lineup2.free	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.labpixies.lineup2.free									
2	Cache	e51d49dd9160c7175b7d40ba6950c0c6	com.lastpass.ilastpass	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.lastpass.ilastpass									
2	Cache	0141e1fef9c48eac994d58f9ba8ea273	com.lesscode.AucklandAirport	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.lesscode.AucklandAirport									
2	Cache	708d8768ebf6ae4819d112a9a22a9f8b	com.ookla.speedtest	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.ookla.speedtest									
2	Cache	da75cba8535a2c0056d75d56518c3e86	com.pangea.cromag	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.pangea.cromag									
2	Cache	3fe101df16ac27fa8e5c4f9a5c3cfa85	com.pressokentertainment.fingerphysics	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.pressokentertainment.fingerphysics									
2	Cache	83b069222d742eea3cec12afa5516685	com.shazam.Shazam	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.shazam.Shazam									
2	Cache	2d51f378cdf59bc9bbaec425e23e5da6	com.skype.skype	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.skype.skype									
2	Cache	9b6ee108e6054e4f725dcc672e9221ba	com.tapulous.taptaprevengeIII	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.tapulous.taptaprevengeIII									
2	Cache	03257223283a5f79c95f5773f1366ac1	com.vgmobile.cnk2	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.vgmobile.cnk2									
2	Cache	7670d65277bb04071b64f64de29e067c	com.yourcompany.ZenbuSearch	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/com.yourcompany.ZenbuSearch									
2	Cache	3810422dcdb403b755cca36b82f1f53b	nz.co.airnz.mPassiPhone	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/nz.co.airnz.mPassiPhone									
2	Cache	7f5605b5a46c3d476e18d8adcd692d26	nz.co.orsome.guide	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/nz.co.orsome.guide									
2	Cache	80b04a5fc4e65f6005a9acf1d373e78f	nz.co.tvnz.news	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/nz.co.tvnz.news									
2	Cache	13e382351bb58240564faa53fdd864b7	se.illusionlabs.sway	/Volumes/Data/mobile/Library/Caches/SpringBoardIconCache-small/se.illusionlabs.sway									
2	Cache	12de80ebdf235c71ff036eb394b365c5	Info.plist	/Volumes/Data/mobile/Library/Caches/VoiceServices/Express.vscache/Info.plist									
2	Cache	de59c2797a218739eafdabdf43d23601	KeywordIndex.plist	/Volumes/Data/mobile/Library/Caches/VoiceServices/Express.vscache/KeywordIndex.plist									
2	Cache	a76424381dd4975fd2ec6f34c637c35b	Manifest.sqlitedb	/Volumes/Data/mobile/Library/Caches/VoiceServices/Express.vscache/Manifest.sqlitedb									
2	Cache	5875001462b2882ab293568cc3f613c0	express.psa	/Volumes/Data/mobile/Library/Caches/VoiceServices/Express.vscache/express.psa									
2	Cache	1ca22aacbaa36a6d7986687697e664e6	PluginRegistry.plist	/Volumes/Data/mobile/Library/Caches/VoiceServices/PluginRegistry.plist									
2	Cache	141294c4909c0c1d0d1e6d1c2a5941e1	ApplicationCache.db	/Volumes/Data/mobile/Library/Caches/com.apple.WebAppCache/ApplicationCache.db	Y	Y	Y		Y	Y	Y	Y	Y
2	Cache	4d396eb68f110270aca85720e23272b6	updates-com.apple.itunesstored.updateQueue.plist	/Volumes/Data/mobile/Library/Caches/com.apple.itunesstored/updates-com.apple.itunesstored.updateQueue.plist									
2	Cache	65356dbe519e1769d05e55edc8773b3f	url-resolution.plist	/Volumes/Data/mobile/Library/Caches/com.apple.itunesstored/url-resolution.plist									
2	Cache	678e606b1026ad17d4dd18ce51dde1ae	com.apple.mobile.installation.plist	/Volumes/Data/mobile/Library/Caches/com.apple.mobile.installation.plist									
2	Cache	e6bbfe8bf78161c62326d41f40da6ab7	com.apple.persistentconnection.cache.plist	/Volumes/Data/mobile/Library/Caches/com.apple.persistentconnection.cache.plist									
2	Cache	262711094c0e8fa7cf6fa3f9e8fe4d10	com.apple.springboard.displaystate.plist	/Volumes/Data/mobile/Library/Caches/com.apple.springboard.displaystate.plist									
2	Calendar	9eb7fe762f68bfeca307d086683b9bea	Calendar.sqlitedb	/Volumes/Data/mobile/Library/Calendar/Calendar.sqlitedb									
2	Call History	cbdfc64080edfc3dd4eb28698edd2cb6	call_history.db	/Volumes/Data/mobile/Library/CallHistory/call_history.db									
2	OS	0fbfc141cbf2162ad78e35db02b417bc	PasswordHistory.plist	/Volumes/Data/mobile/Library/ConfigurationProfiles/PasswordHistory.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	ed3b3357b48e1d2d19a40fdd7e06480d	PayloadManifest.plist	/Volumes/Data/mobile/Library/ConfigurationProfiles/PayloadManifest.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	Cookies	ab9673528a685d4588c2aff9b9db8b44	Cookies.plist	/Volumes/Data/mobile/Library/Cookies/Cookies.plist									
2	Cookies	786f4cfed8d5206d2e2aca393d1edce7	com.apple.itunesstored.plist	/Volumes/Data/mobile/Library/Cookies/com.apple.itunesstored.plist									
2	OS	22f8eaad38cd0af8d05c02ac5db38515	dynamic-text.dat	/Volumes/Data/mobile/Library/Keyboard/dynamic-text.dat									
2	OS	d6ff4dda2168bdcab6b1297cb127424b	LockBackground.jpg	/Volumes/Data/mobile/Library/LockBackground.jpg	Y	Y			Y	Y	Y	Y	Y
2	OS	12e58146da32a19271cc2c447c2660f7	ADDataStore.sqlitedb	/Volumes/Data/mobile/Library/Logs/ADDataStore.sqlitedb									
2	OS	218e50b3ac04e0420ae298b18e8a81f0	ADDataStore.sqlitedb-journal	/Volumes/Data/mobile/Library/Logs/ADDataStore.sqlitedb-journal									
2	OS	be22589c9bc96688f4b342c2db40863d	general.log	/Volumes/Data/mobile/Library/Logs/AppleSupport/general.log									
2	OS	3490d3c30b79d7a5528937b3df5fdae1	mobile_installation.log.0	/Volumes/Data/mobile/Library/Logs/MobileInstallation/mobile_installation.log.0									
2	Mail	634314bb920287b16957f17e4dc33a68	AutoFetchEnabled	/Volumes/Data/mobile/Library/Mail/AutoFetchEnabled	Y	Y	Y		Y	Y	Y	Y	Y
2	Mail	8aab3ba75aaada110b9ccbd1c68de3f5	Envelope Index	/Volumes/Data/mobile/Library/Mail/Envelope Index									
2	Mail	6c2c4a80418931d0041b771c1a762189	.mboxCache.plist	/Volumes/Data/mobile/Library/Mail/Mailboxes/.mboxCache.plist									
2	Mail	f4e9095262f23546c4a8644166b8f16f	.mboxCache.plist	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/.mboxCache.plist									
2	Mail	ab7a941ee732d20f01761eeb87b1a99d	26.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/26.2.emlxpart									

2	Mail	c127d1eee35f8b8553399d9246d39dba	27.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/27.2.emlxpart									
2	Mail	0e2ee22280f09a30452d791dd86f9bbf	28.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/28.2.emlxpart									
2	Mail	905a18306feb666c2b0dd7f60c098d44	29.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/29.2.emlxpart									
2	Mail	aa8554fa2390f62a278bf3e3ad44c1fa	32.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/32.2.emlxpart									
2	Mail	58ba7f8c26206d9afd5d32068976003c	36.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/36.2.emlxpart									
2	Mail	76901bfa921753fa99af5bf8c8c9233f	4.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/4.2.emlxpart									
2	Mail	4e4940dd52b9501b0d66cf8420826e86	41.1.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/41.1.emlxpart									
2	Mail	83a60abce20949816ca52385333cda4f	44.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/44.2.emlxpart									
2	Mail	726119e785d7fa65571be5531c8a08ae	5.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/5.2.emlxpart									
2	Mail	8cbd784ca4f24ce7b11416b3152665a5	6.2.emlxpart	/Volumes/Data/mobile/Library/Mail/MobileMe-ben.knight/INBOX.imapmbox/Messages/6.2.emlxpart									
2	Mail	3c392fdadb3acfc7fc8226aba82b6289	metadata.plist	/Volumes/Data/mobile/Library/Mail/metadata.plist									
2	Maps	108782fa662c9efa49f11724bc4eab93	Directions.plist	/Volumes/Data/mobile/Library/Maps/Directions.plist	Y	Y			Y	Y	Y	Y	Y
2	Maps	84e5978f01c23e94f14fe92f2702628b	History.plist	/Volumes/Data/mobile/Library/Maps/History.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	5a50cc6ab8277f5f4a02116c1cda770e	ApplicationAttributes.plist	/Volumes/Data/mobile/Library/MobileInstallation/ApplicationAttributes.plist									
2	OS	ce7f5b3d4bfc7b4b0da6a06dccc515f2	SafeHarbor.plist	/Volumes/Data/mobile/Library/MobileInstallation/SafeHarbor.plist									
2	Notes	72cbe1f2f171e5b183e23a0dc777524a	notes.db	/Volumes/Data/mobile/Library/Notes/notes.db									
2	Notes	35944408bd0d142210cbe39147bf63fc	notes.idx	/Volumes/Data/mobile/Library/Notes/notes.idx	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	99a2c0a5a194eebd50df8b3cd39a84c9	.GlobalPreferences.plist	/Volumes/Data/mobile/Library/Preferences/.GlobalPreferences.plist	Y				Y	Y		Y	
2	OS	d41d8cd98f00b204e9800998ecf8427e	com.apple.AOSNotification.launchd	/Volumes/Data/mobile/Library/Preferences/com.apple.AOSNotification.launchd	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	7166546d81590ac5aa1292a20ceba821	com.apple.AOSNotification.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.AOSNotification.plist									
2	OS	b885e1ecdfed27a0e4f13172fdaf6b26	com.apple.AppStore.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.AppStore.plist									
2	OS	b05ef315c7458840f6f7b68c28fab969	com.apple.AppSupport.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.AppSupport.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	ba130c824f6de4dd66df9f79d621198d	com.apple.BTServer.airplane.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.BTServer.airplane.plist									
2	OS	f0a31dab9cd81074797e92dab98775c1	com.apple.BTServer.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.BTServer.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	79e982d176f73210620761969765b476	com.apple.GMM.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.GMM.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	7474d4792df6238d0a04192b66bdc83b	com.apple.Maps.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.Maps.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	2d3164ef587538dfb27fc59bdb6dba90	com.apple.MobileBluetooth.services.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.MobileBluetooth.services.plist									
2	OS	b5fcbb6f8451476232166cfadbbfb0d4	com.apple.MobileInternetSharing.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.MobileInternetSharing.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	e4dae28f6e4dade63cdca11de1774c25	com.apple.MobileSMS.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.MobileSMS.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	a8757b57fcc71f4b1a886ba6cb3698c0	com.apple.MobileStore.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.MobileStore.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	1ee46c14edfd757b6425594a35f1019e	com.apple.OTASyncAgent.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.OTASyncAgent.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	09677b25b0f1636e9225fc89ba7e76fa	com.apple.OTASyncState.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.OTASyncState.plist									
2	OS	e31353df2ed8a4f69a48617814ccae0a	com.apple.PeoplePicker.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.PeoplePicker.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	4927fcdaa98e038e81212f79287c6da1	com.apple.Preferences.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.Preferences.plist									
2	OS	724bdfe48e204cdb5465d45605e28f3e	com.apple.VoiceMemos.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.VoiceMemos.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	8a00e0acf7a00d7a73d1c7dd528c65bf	com.apple.WebFoundation.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.WebFoundation.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	d196ca2c2233fd766fa7a68be4a19af2	com.apple.accountsettings.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.accountsettings.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	5b0232aeb996f59ca1f9c15d6e4dc758	com.apple.aggregated.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.aggregated.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	c70f06c1e65bd6aeaf10ae2764785ab9	com.apple.apsd.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.apsd.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	1121dc196083fd296525231f26be1c8f	com.apple.calculator.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.calculator.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	ddbcbed1a106c3bd11bd5d715bf6c62a	com.apple.celestial.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.celestial.plist									
2	OS	8300dd8ea7489aa1fada2a8ed8278f4c	com.apple.commcenter.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.commcenter.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	1b5e0ba9fbe0ca9996216638a7ff5b23	com.apple.iqagent.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.iqagent.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	32e4d401e6fa074d87b0c3bbbfde0221	com.apple.itunesstored.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.itunesstored.plist									
2	OS	4f62f8aaab5a6aa1d346c4ba013c482e	com.apple.locationd.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.locationd.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	cdbebb6b3e2aa6bfceef5a47fb85a9c0	com.apple.mms_override.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mms_override.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	88f4591f1a9ec093b7737e39ed99c47b	com.apple.mobile.SyncMigrator.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobile.SyncMigrator.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	f7d6c77c58d47639def52021a6edeb6d	com.apple.mobilecal.alarmengine.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobilecal.alarmengine.plist									
2	OS	e39c62df0feecac6bb3be4eb8ce14f13	com.apple.mobilecal.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobilecal.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	a40031b68bd1e31ad3deb2da75cda487	com.apple.mobileipod.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobileipod.plist									
2	OS	ddee55ec31b591b536a8f1b5e096197b	com.apple.mobilemail.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobilemail.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	e8c4d87cbad87b9e417db50b9bad9734	com.apple.mobilenotes.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobilenotes.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	4b2789d5ad9e95eebaac68ce4ece916b	com.apple.mobilephone.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobilephone.plist									
2	OS	1be0c246d70ffef9fedfa19514593b17	com.apple.mobilesafari.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobilesafari.plist									
2	OS	0698134c20595eb02bf1ae0f85f428f3	com.apple.mobileslideshow.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobileslideshow.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	69139f962fd79185373f0792637c7af7	com.apple.mobiletimer.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.mobiletimer.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	2e56f70f277faa543ae5421796cc1b38	com.apple.nike.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.nike.plist									
2	OS	ef72daf82c166792ec2dc2b341c975d2	com.apple.persistentconnection-mcc.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.persistentconnection-mcc.plist	Y	Y			Y	Y	Y	Y	Y
2	OS	51f44f81755c89a0e10e4f9be0aff3d9	com.apple.preferences.datetime.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.preferences.datetime.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	3dd3b11c89827ba808c4eccd4928e144	com.apple.preferences.network.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.preferences.network.plist									
2	OS	02725990299d884493104857d19ac5f2	com.apple.preferences.sounds.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.preferences.sounds.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	OS	c798b3214c3fb93e7ac841a8c4682df8	com.apple.springboard.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.springboard.plist									
2	OS	240a6e41139e36f4af0966bfc5575c9e	com.apple.youtube.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.youtube.plist									
2	OS	a90147e2069d9bfa2b04f0759a3d5444	com.apple.youtubeframework.plist	/Volumes/Data/mobile/Library/Preferences/com.apple.youtubeframework.plist									
2	OS	c84e8f6b44eafd7e096059c555ff09e1	Clients.plist	/Volumes/Data/mobile/Library/RemoteNotification/Clients.plist	Y	Y	Y		Y	Y	Y	Y	Y
2	SMS	22f44c8a6f6571cf2a8107d67526a8bb	message.plist	/Volumes/Data/mobile/Library/SMS/Drafts/PENDING.draft/message.plist	Y	Y			Y	Y	Y	Y	Y
2	SMS	21e5d6d59aa85e0157c2b7941ea3cf59	sms.db	/Volumes/Data/mobile/Library/SMS/sms.db									
2	Safari	16142f0f7dd161f7f0cb3a2fc6f8cd40	Bookmarks.plist	/Volumes/Data/mobile/Library/Safari/Bookmarks.plist									
2	Safari	6429185997f776ae6e423cfcf08316a6	Bookmarks.plist.anchor.plist	/Volumes/Data/mobile/Library/Safari/Bookmarks.plist.anchor.plist									
2	Safari	887e293bb1acc54210bcfb1edff3356a	History.plist	/Volumes/Data/mobile/Library/Safari/History.plist									
2	Safari	13a3871a0c0de916a588bc446a467d25	SuspendState.plist	/Volumes/Data/mobile/Library/Safari/SuspendState.plist									
2	Safari	5c0ad37ccfcb2f8a48bdf6cc97f6e95e	voicemail.db	/Volumes/Data/mobile/Library/Voicemail/voicemail.db	Y	Y			Y	Y	Y	Y	Y
2	Safari	5e75766cbe877ebc86adb202aaa202f8	Info.plist	/Volumes/Data/mobile/Library/WebClips/4920F09CE9374925AD3A20B570B34D96.webclip/Info.plist	Y	Y	Y		Y	Y	Y	Y	Y

2	Safari	d991c4eabf5f5d1bf013f23c949ca601	icon.png	/Volumes/Data/mobile/Library/WebClips/4920F09CE9374925AD3A20B570B34D96.webclip/icon.png	Y	Y	Y		Y	Y	Y	Y	Y
2	Safari	b140b1b16ffa5ae5dc246b82a73f6db8	Databases.db	/Volumes/Data/mobile/Library/WebKit/Databases/Databases.db	Y	Y	Y		Y	Y	Y	Y	Y
2	Safari	0b52bf1ddcc632a5f08418a2848a4d6c	0000000000000001.db	/Volumes/Data/mobile/Library/WebKit/Databases/https_mail.google.com_0/0000000000000001.db	Y	Y	Y		Y	Y	Y	Y	Y
2	Safari	8c2aa56c25394642723d41aef978631a	itunesstored2.sqlitedb	/Volumes/Data/mobile/Library/com.apple.itunesstored/itunesstored2.sqlitedb									
2	Camera	4b56fd7c12ddc65f2148da230334d43e	Info.plist	/Volumes/Data/mobile/Media/DCIM/.MISC/Info.plist	Y	Y		Y	Y	Y	Y	Y	Y
2	OS	92c40c615b2a5f809bb50559934ad6c5	Recordings.db	/Volumes/Data/mobile/Media/Recordings/Recordings.db	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	Safari	ca2b7464f853322124d5cd0b80229404	goog-phish-shavar.dat	/Volumes/Data/mobile/Media/Safari/goog-phish-shavar.dat									
2	OS	d41d8cd98f00b204e9800998ecf8427e	com.apple.itdbprep.postprocess.lock	/Volumes/Data/mobile/Media/com.apple.itdbprep.postprocess.lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	d41d8cd98f00b204e9800998ecf8427e	com.apple.itunes.lock_sync	/Volumes/Data/mobile/Media/com.apple.itunes.lock_sync	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	d41d8cd98f00b204e9800998ecf8427e	bounds	/Volumes/Data/msgs/bounds	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	9ceff0b06e4c0f39d1a08d32168ad4e6	AeneasCustomFlags.plist	/Volumes/Data/preferences/AeneasCustomFlags.plist									
2	OS	e0b020dc294c03411082311e27061106	NetworkInterfaces.plist	/Volumes/Data/preferences/SystemConfiguration/NetworkInterfaces.plist									
2	OS	93f0d9323b98ad9039548375b7887d8d	com.apple.AutoWake.plist	/Volumes/Data/preferences/SystemConfiguration/com.apple.AutoWake.plist									
2	OS	770490b00ed2ce427eaa1a95ab7c3b50	com.apple.network.identification.plist	/Volumes/Data/preferences/SystemConfiguration/com.apple.network.identification.plist									
2	OS	2daae880de22bf1ee7df1a1008f31179	com.apple.wifi.plist	/Volumes/Data/preferences/SystemConfiguration/com.apple.wifi.plist									
2	OS	09963f443128e1d9829c3b3238f8b49c	preferences.plist	/Volumes/Data/preferences/SystemConfiguration/preferences.plist									
2	OS	88836f935e1a1b7a62fc6f99f39c5156	csidata	/Volumes/Data/preferences/csidata									
2	AddressBook	9421a3b0670502c1e2349dc58e67dd13	AddressBook.sqlitedb	/Volumes/Data/root/Library/AddressBook/AddressBook.sqlitedb									
2	Cookies	21594d7332fc5238a49a3351e3ec7a41	Cookies.plist	/Volumes/Data/root/Library/Cookies/Cookies.plist									
2	OS	5f713f5ba34cbf95289fc790b7d0b13c	wildcard_record.plist	/Volumes/Data/root/Library/Lockdown/activation_records/wildcard_record.plist									
2	OS	d717a51ef098f234fc0f1962a3ff755a	data_ark.plist	/Volumes/Data/root/Library/Lockdown/data_ark.plist									
2	OS	0f1b860f0c2a0d18882bbe8b5618c591	device_private_key.pem	/Volumes/Data/root/Library/Lockdown/device_private_key.pem									
2	OS	ce48a49ade7d41acceb4c9684dfb322b	device_public_key.pem	/Volumes/Data/root/Library/Lockdown/device_public_key.pem									
2	OS	49e75fcba797545dce2624b624478eba	47F8B545-B384-4D43-ABCC-7CD818C3FF12.plist	/Volumes/Data/root/Library/Lockdown/pair_records/47F8B545-B384-4D43-ABCC-7CD818C3FF12.plist									
2	OS	80df8f36885de8f51b151dc774f337d5	.GlobalPreferences.plist	/Volumes/Data/root/Library/Preferences/.GlobalPreferences.plist									
2	OS	3150e5ae680a23fdc084f9697187d353	com.apple.Preferences.plist	/Volumes/Data/root/Library/Preferences/com.apple.Preferences.plist									
2	OS	4cc29172b8d6abd8f2e9a7dc0cdbbe9e	com.apple.stackshot.plist	/Volumes/Data/root/Library/Preferences/com.apple.stackshot.plist									
2	OS	2a53da1a6fbfc0bafdd96b0a2ea29515	configd.pid	/Volumes/Data/run/configd.pid									
2	OS	8c9eb686bf3eb5bd83d9373eadf6504b	syslog.pid	/Volumes/Data/run/syslog.pid									
2	OS	d41d8cd98f00b204e9800998ecf8427e	utmp	/Volumes/Data/run/utmp	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	d1524c1b01c728f2c53a0d24675fcaaa	utmpx	/Volumes/Data/run/utmpx									
2	OS	d0cac0977484b5e461e023643057c8ba	Alarm.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Alarm.m4r									
2	OS	02a1ad7966f731e34154a695e7a8efd2	Ascending.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Ascending.m4r									
2	OS	038094ecfe5d566eeb2b85b8df468f2d	Bark.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Bark.m4r									
2	OS	d38e4d8d045f736e5848d8954b321661	Bell Tower.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Bell Tower.m4r									
2	OS	d489fd781d899787f747d490df7bf916	Blues.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Blues.m4r									
2	OS	bdf2dc2ef722e53fb3540708892d6c5c	Boing.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Boing.m4r									
2	OS	ea1ad55fba0217712f6bce89cac4c714	Crickets.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Crickets.m4r									
2	OS	528d6b9e6a3be10fac8b4b49eea89177	Digital.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Digital.m4r									
2	OS	4327d2e4b50f46ed8c82869674eea0a7	Doorbell.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Doorbell.m4r									
2	OS	fac947617f3b6fafb0cb2669bdcaf24e	Duck.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Duck.m4r									
2	OS	4b415fd52261265bc40df1beec71a479	Harp.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Harp.m4r									
2	OS	2dc9508d4ee115bfa168b0626545f524	Motorcycle.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Motorcycle.m4r									
2	OS	97e5749ee4f326f8bcbe02f7582dbcd4	Old Car Horn.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Old Car Horn.m4r									
2	OS	06550674882bf53de695982ae71fff1c	Old Phone.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Old Phone.m4r									
2	OS	c1bac8f257153c6a00b1f6401544d913	Piano Riff.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Piano Riff.m4r									
2	OS	ef33c5ecf306c27add38b3d1f612c094	Pinball.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Pinball.m4r									
2	OS	d0ed05d91976700dbc57d5b9c6a08b23	Robot.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Robot.m4r									
2	OS	420271a6ca05dfa6c2a92888d9fc9f1e	Sci-Fi.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Sci-Fi.m4r									
2	OS	5f87e839893897598f3b516637ec7195	Sonar.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Sonar.m4r									
2	OS	2c5b25700a66a8beb2ee3ba301629291	Strum.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Strum.m4r									
2	OS	85e0af1e967996f8a11d07cd03402a0c	Timba.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Timba.m4r									
2	OS	a7393d5507b75d534e92e4ead444d18a	Time Passing.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Time Passing.m4r									
2	OS	277f224d50f954de614ffeb8aa5bf357	Trill.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Trill.m4r									
2	OS	2512b799c1adacafc67d69a8ca9210d2	Xylophone.m4r	/Volumes/Data/stash/Ringtones.JVrbJZ/Xylophone.m4r									
2	OS	d92ff08217de75ce5630848dc0ff0ff8	100.png	/Volumes/Data/stash/Wallpaper.FJHfjF/100.png									
2	OS	840cbde47c27f57d906d5707edc4ccd2	100.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/100.thumbnail.png									
2	OS	3a2efb87061fda8a1fbdf65e6b608dc8	101.png	/Volumes/Data/stash/Wallpaper.FJHfjF/101.png									
2	OS	db735e9543a72d8b72e5bb9cfc4fbe90	101.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/101.thumbnail.png									
2	OS	f781c099d3bd699e942b55fc82f24d95	102.png	/Volumes/Data/stash/Wallpaper.FJHfjF/102.png									
2	OS	65740e243c0f6aa32a4b62b8f8f10f01	102.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/102.thumbnail.png									
2	OS	ae5ae36a7aa063998ae0f3275f1952f4	103.png	/Volumes/Data/stash/Wallpaper.FJHfjF/103.png									
2	OS	86163a5604377626145e843ff5009ef3	103.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/103.thumbnail.png									
2	OS	54a7f7142953e7b64df92b35c172c475	104.png	/Volumes/Data/stash/Wallpaper.FJHfjF/104.png									
2	OS	79df37daa8f74d4bcf1fef6753a2243b	104.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/104.thumbnail.png									
2	OS	2e6ba933cf9a0bebe0eb51b9e3b91b9a	105.png	/Volumes/Data/stash/Wallpaper.FJHfjF/105.png									
2	OS	8a3c6117ab39f658f3f27a1422f621de	105.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/105.thumbnail.png									
2	OS	6774494b16fb2e9b3c5488058e8ebd21	106.png	/Volumes/Data/stash/Wallpaper.FJHfjF/106.png									
2	OS	cce2b9306a2453a7b40aad8846bb7f28	106.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/106.thumbnail.png									
2	OS	8bbb4e2e8694220f8b830e917cdf71d9	107.png	/Volumes/Data/stash/Wallpaper.FJHfjF/107.png									
2	OS	c10aea0e555c582e7176fed9ebcba269	107.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/107.thumbnail.png									
2	OS	430898f2736cfe9b979432597d84b5e3	108.png	/Volumes/Data/stash/Wallpaper.FJHfjF/108.png									
2	OS	998b57a8c61fb753a74382b7915d416c	108.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/108.thumbnail.png									

2	OS	10e9c42d40ec2d712495a151ba16fc21	109.png	/Volumes/Data/stash/Wallpaper.FJHfjF/109.png									
2	OS	8fe7c2750ecd106ef767bb67bbea470f	109.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/109.thumbnail.png									
2	OS	7fe637a6ad3bbcead33b32d768353225	110.png	/Volumes/Data/stash/Wallpaper.FJHfjF/110.png									
2	OS	2d88dd128ac5939406d77be45aa0dda9	110.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/110.thumbnail.png									
2	OS	3e5118ee75cf0e1c93df436b5935da13	111.png	/Volumes/Data/stash/Wallpaper.FJHfjF/111.png									
2	OS	4ba102d9566cc21215d0ff7807a9d01c	111.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/111.thumbnail.png									
2	OS	1377f74d669837e9c7321072cdbe8770	112.png	/Volumes/Data/stash/Wallpaper.FJHfjF/112.png									
2	OS	e4681aa3b93ad626a8b0b893555a3f45	112.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/112.thumbnail.png									
2	OS	1f8a7a8112d79648f6fcf35441a82621	113.png	/Volumes/Data/stash/Wallpaper.FJHfjF/113.png									
2	OS	e102be5c3db17fd10b56202ac9327bc1	113.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/113.thumbnail.png									
2	OS	a0e7b2bdec29c1d12b1b1a67953883d4	114.png	/Volumes/Data/stash/Wallpaper.FJHfjF/114.png									
2	OS	c71c520db1da6597189c010383313b4e	114.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/114.thumbnail.png									
2	OS	fba96c685c4e4532ff08bc89705d1602	115.png	/Volumes/Data/stash/Wallpaper.FJHfjF/115.png									
2	OS	15678307368467633ff3ad0531c13870	115.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/115.thumbnail.png									
2	OS	ba4e887bd7ba475d5f5203879bdcba4d	116.png	/Volumes/Data/stash/Wallpaper.FJHfjF/116.png									
2	OS	3202a1f462a8ee2b1366407bb44703e5	116.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/116.thumbnail.png									
2	OS	b2327d0d4227c83bac2653813044dbb7	117.png	/Volumes/Data/stash/Wallpaper.FJHfjF/117.png									
2	OS	f4368cf638b27270d277da6ee5bd077c	117.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/117.thumbnail.png									
2	OS	9543574e52d079300289e9f4aa1a126f	118.png	/Volumes/Data/stash/Wallpaper.FJHfjF/118.png									
2	OS	ac3115117a8c35fb67432adfc313380e	118.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/118.thumbnail.png									
2	OS	8c14f945a10491fadf814d0c710f0a97	poster.thumbnail.png	/Volumes/Data/stash/Wallpaper.FJHfjF/poster.thumbnail.png									
2	OS	c5f94e7559cb76cca1ff2b5c57cfcab3	curses.h	/Volumes/Data/stash/include.fjRbht/curses.h									
2	OS	46619a92f07cdee2a510913bb900b83b	cursesapp.h	/Volumes/Data/stash/include.fjRbht/cursesapp.h									
2	OS	8fa9132dd401401122d0c8fe01d9e315	cursesf.h	/Volumes/Data/stash/include.fjRbht/cursesf.h									
2	OS	c4f8606b9f175836e0ca8cb860b1307c	cursesm.h	/Volumes/Data/stash/include.fjRbht/cursesm.h									
2	OS	7e89e643926ae71ae25f0803050999ef	cursesp.h	/Volumes/Data/stash/include.fjRbht/cursesp.h									
2	OS	7dd7ad2e30c19d6f092cbe769117c1a1	cursesw.h	/Volumes/Data/stash/include.fjRbht/cursesw.h									
2	OS	4807773a6b9d71d035a16d21470905e5	cursslk.h	/Volumes/Data/stash/include.fjRbht/cursslk.h									
2	OS	ba8df089929addc55abbd7be6679a701	eti.h	/Volumes/Data/stash/include.fjRbht/eti.h									
2	OS	b5c9af0ce9bf600113f03bd196097f51	etip.h	/Volumes/Data/stash/include.fjRbht/etip.h									
2	OS	51d661a2381ba3c0318f43bb2c1c397c	form.h	/Volumes/Data/stash/include.fjRbht/form.h									
2	OS	f39a27776093beaec260742df3ab1b4f	lzmadec.h	/Volumes/Data/stash/include.fjRbht/lzmadec.h									
2	OS	a61a87a788b805c181b844b0ddfe42ad	menu.h	/Volumes/Data/stash/include.fjRbht/menu.h									
2	OS	55816bbb71eaad6e47d973d5f6f66508	nc_tparm.h	/Volumes/Data/stash/include.fjRbht/nc_tparm.h									
2	OS	c5f94e7559cb76cca1ff2b5c57cfcab3	ncurses.h	/Volumes/Data/stash/include.fjRbht/ncurses.h									
2	OS	7a2e6b1806288eaa04e4c5c2ce9b228b	ncurses_dll.h	/Volumes/Data/stash/include.fjRbht/ncurses_dll.h									
2	OS	e7457f298b02db0f1a4cd36617658217	curses.h	/Volumes/Data/stash/include.fjRbht/ncursesw/curses.h									
2	OS	c962ac5b707189215c8f292f9c584327	cursesapp.h	/Volumes/Data/stash/include.fjRbht/ncursesw/cursesapp.h									
2	OS	79919c95cf8abfd9a170c6756cd4c27c	cursesf.h	/Volumes/Data/stash/include.fjRbht/ncursesw/cursesf.h									
2	OS	9048f82d023486cdccc97a33485df615	cursesm.h	/Volumes/Data/stash/include.fjRbht/ncursesw/cursesm.h									
2	OS	b84ed79c1d740b0bceb2fd4138f72a1a	cursesp.h	/Volumes/Data/stash/include.fjRbht/ncursesw/cursesp.h									
2	OS	28bb36180717f58df658b18d5ce7fb49	cursesw.h	/Volumes/Data/stash/include.fjRbht/ncursesw/cursesw.h									
2	OS	5bb1f802303964cf58f8095c1f225d09	cursslk.h	/Volumes/Data/stash/include.fjRbht/ncursesw/cursslk.h									
2	OS	ba8df089929addc55abbd7be6679a701	eti.h	/Volumes/Data/stash/include.fjRbht/ncursesw/eti.h									
2	OS	b2cf9e471a34c53ff9cc1690ce2ff200	etip.h	/Volumes/Data/stash/include.fjRbht/ncursesw/etip.h									
2	OS	ce3bf8f1fae4a67bae3cea6d2ee3ff58	form.h	/Volumes/Data/stash/include.fjRbht/ncursesw/form.h									
2	OS	bcce8253d14305ffa8b60c891a09ddd6	menu.h	/Volumes/Data/stash/include.fjRbht/ncursesw/menu.h									
2	OS	55816bbb71eaad6e47d973d5f6f66508	nc_tparm.h	/Volumes/Data/stash/include.fjRbht/ncursesw/nc_tparm.h									
2	OS	e7457f298b02db0f1a4cd36617658217	ncurses.h	/Volumes/Data/stash/include.fjRbht/ncursesw/ncurses.h									
2	OS	7a2e6b1806288eaa04e4c5c2ce9b228b	ncurses_dll.h	/Volumes/Data/stash/include.fjRbht/ncursesw/ncurses_dll.h									
2	OS	e1a047ca0817f364182e0734a4747ad6	panel.h	/Volumes/Data/stash/include.fjRbht/ncursesw/panel.h									
2	OS	43a720e1ad258fcfd5ed8f11251626bc	term.h	/Volumes/Data/stash/include.fjRbht/ncursesw/term.h									
2	OS	7ea0d163d0d2e1759aaaae5b64427ae1	term_entry.h	/Volumes/Data/stash/include.fjRbht/ncursesw/term_entry.h									
2	OS	2a4ce9f2d528beeb263c1f608dbbd710	termcap.h	/Volumes/Data/stash/include.fjRbht/ncursesw/termcap.h									
2	OS	9052a71a03a252c59a260a5bbe9fec93	tic.h	/Volumes/Data/stash/include.fjRbht/ncursesw/tic.h									
2	OS	e4205e9e6c7beb3f017bf3eee5255075	unctrl.h	/Volumes/Data/stash/include.fjRbht/ncursesw/unctrl.h									
2	OS	685f7f16a32214163ecdc8f090bc6d7b	_pam_aconf.h	/Volumes/Data/stash/include.fjRbht/pam/_pam_aconf.h									
2	OS	e0961fd2f2100ffa55ffeb0a2d0cc9b0	_pam_compat.h	/Volumes/Data/stash/include.fjRbht/pam/_pam_compat.h									
2	OS	3a036f545ee8e9b1a2e04c3a1f6ae0ce	_pam_macros.h	/Volumes/Data/stash/include.fjRbht/pam/_pam_macros.h									
2	OS	e073f044c124157c0af10f3f213fd719	_pam_types.h	/Volumes/Data/stash/include.fjRbht/pam/_pam_types.h									
2	OS	0e88f0a4eb61b839a13ceb75dca599b0	pam_appl.h	/Volumes/Data/stash/include.fjRbht/pam/pam_appl.h									
2	OS	9d511ae8e6e8a74bc8c01c91c2b69992	pam_mod_misc.h	/Volumes/Data/stash/include.fjRbht/pam/pam_mod_misc.h									
2	OS	bc6c648eeb634167fa0b2c9aa41086e8	pam_modules.h	/Volumes/Data/stash/include.fjRbht/pam/pam_modules.h									
2	OS	4a675ecb2e63e223b5f48c5f2febe8e4	panel.h	/Volumes/Data/stash/include.fjRbht/panel.h									
2	OS	c32dd562be879518ef33a557e313a6cb	pcre.h	/Volumes/Data/stash/include.fjRbht/pcre.h									
2	OS	524fc49143dd83fa94d12e0b180d6be6	pcre_scanner.h	/Volumes/Data/stash/include.fjRbht/pcre_scanner.h									
2	OS	6efbc935bbf8c1dc0fff89c61ac61516	pcre_stringpiece.h	/Volumes/Data/stash/include.fjRbht/pcre_stringpiece.h									
2	OS	46716c13d80f7b11e0082a26cf6deba7	pcrecpp.h	/Volumes/Data/stash/include.fjRbht/pcrecpp.h									
2	OS	f907364a60cda13f1916726a65c9bd6c	pcrecpparg.h	/Volumes/Data/stash/include.fjRbht/pcrecpparg.h									
2	OS	f4804cf575eec6e5d973e1f65fbd3d5a	pcreposix.h	/Volumes/Data/stash/include.fjRbht/pcreposix.h									
2	OS	f83ffd9b7c44cc50a2eb6035d3951186	chardefs.h	/Volumes/Data/stash/include.fjRbht/readline/chardefs.h									
2	OS	97a435e52d83605ccd95f74df73ff6d1	history.h	/Volumes/Data/stash/include.fjRbht/readline/history.h									
2	OS	0456b14771f3f7a96aa125576d3ac501	keymaps.h	/Volumes/Data/stash/include.fjRbht/readline/keymaps.h									

2	OS	5160d88aad657f575d4a8e1310636df3	readline.h	/Volumes/Data/stash/include.fjRbht/readline/readline.h									
2	OS	59e7f6278ac99051302afcfd3b86d7cb	rlconf.h	/Volumes/Data/stash/include.fjRbht/readline/rlconf.h									
2	OS	f594e8f53a51eab2435bbda614326896	rlstdc.h	/Volumes/Data/stash/include.fjRbht/readline/rlstdc.h									
2	OS	f076ab39ee4f3a84dd3cfec045048139	rltypedefs.h	/Volumes/Data/stash/include.fjRbht/readline/rltypedefs.h									
2	OS	4b810af2c83168d3cd86815a6bbeaaff	tilde.h	/Volumes/Data/stash/include.fjRbht/readline/tilde.h									
2	OS	2cc2d1f82ae80c567dd6b8952781e070	term.h	/Volumes/Data/stash/include.fjRbht/term.h									
2	OS	c6ccf5f7b3788a1a54f69d4fea6cc23b	term_entry.h	/Volumes/Data/stash/include.fjRbht/term_entry.h									
2	OS	fefe4bd11af4dff2acc68aacb098da88	termcap.h	/Volumes/Data/stash/include.fjRbht/termcap.h									
2	OS	9210983b306c6371e73ac19d134a3dc4	tic.h	/Volumes/Data/stash/include.fjRbht/tic.h									
2	OS	d3b9173e2a30d532aeca60845a3bfe25	unctrl.h	/Volumes/Data/stash/include.fjRbht/unctrl.h									
2	OS	949282bc11ce13bf426114a643a805b2	BackupAgent	/Volumes/Data/stash/libexec.3MJ3tz/BackupAgent									
2	OS	ac895b01906b39a051ba7077f0d02a7d	CrashHousekeeping	/Volumes/Data/stash/libexec.3MJ3tz/CrashHousekeeping									
2	OS	bcbb50d15538dd20f3ba7ad485f35ea0	CrashReportCopyAgent	/Volumes/Data/stash/libexec.3MJ3tz/CrashReportCopyAgent									
2	OS	dfb7de55c52ff7b02fc6e323bc56c7e1	SyncAgent	/Volumes/Data/stash/libexec.3MJ3tz/SyncAgent									
2	OS	50880dfa9b2136a068a14ee7e8021e26	afcd	/Volumes/Data/stash/libexec.3MJ3tz/afcd									
2	OS	e93bfc98c446759a0d3f0c703b8f59c9	amfid	/Volumes/Data/stash/libexec.3MJ3tz/amfid									
2	OS	06bf71d6d5d66769358fa17eafe25825	bigram	/Volumes/Data/stash/libexec.3MJ3tz/bigram									
2	OS	d68dc121cdb8f0dc23c9e5b85899155a	bootpd	/Volumes/Data/stash/libexec.3MJ3tz/bootpd									
2	OS	b5cae78c452ae34fc5036a56b37fd7c4	code	/Volumes/Data/stash/libexec.3MJ3tz/code									
2	OS	3540541a422ac1d0f9748c38da48cdae	configd	/Volumes/Data/stash/libexec.3MJ3tz/configd									
2	OS	0678e987af84e7ad1aef7cb2565aedc3	crash_mover	/Volumes/Data/stash/libexec.3MJ3tz/crash_mover									
2	OS	22f9a5bc42b6a3601b0ce25a8d99c553	debug_image_mount	/Volumes/Data/stash/libexec.3MJ3tz/debug_image_mount									
2	OS	f545f8f622caa8cab87e2abf5d4f6c22	frcode	/Volumes/Data/stash/libexec.3MJ3tz/frcode									
2	OS	476b3007a7bc9e6a0763f226f42563bb	gpgkeys_curl	/Volumes/Data/stash/libexec.3MJ3tz/gnupg/gpgkeys_curl									
2	OS	5912896a6211a5c9160eac70082f29ef	gpgkeys_finger	/Volumes/Data/stash/libexec.3MJ3tz/gnupg/gpgkeys_finger									
2	OS	f9b45c1a9d2a4af764cddeb7b6b30c15	gpgkeys_hkp	/Volumes/Data/stash/libexec.3MJ3tz/gnupg/gpgkeys_hkp									
2	OS	3236350248361e661355620888a21e17	installd	/Volumes/Data/stash/libexec.3MJ3tz/installd									
2	OS	bdeddd68d767458ee93ac54fe4d606c8	itdbprepserver	/Volumes/Data/stash/libexec.3MJ3tz/itdbprepserver									
2	OS	972c4ddb9be06f18b94e63ded58f9d16	launchproxy	/Volumes/Data/stash/libexec.3MJ3tz/launchproxy									
2	OS	69d88bedcb56797dc80e800fa229e6cb	locationd	/Volumes/Data/stash/libexec.3MJ3tz/locationd									
2	OS	b5a56bc9f8fcdb661291acadb6874043	lockbot	/Volumes/Data/stash/libexec.3MJ3tz/lockbot									
2	OS	2bc201bc9a01ccc55cce89ad6d076451	lockdownd	/Volumes/Data/stash/libexec.3MJ3tz/lockdownd									
2	OS	358181afa00b63ca44141bcb2046a718	mc_mobile_tunnel	/Volumes/Data/stash/libexec.3MJ3tz/mc_mobile_tunnel									
2	OS	219e194e68d5ea2523d1dba43e5cc359	misagent	/Volumes/Data/stash/libexec.3MJ3tz/misagent									
2	OS	045f746f892e5abdb12057732e55e436	misd	/Volumes/Data/stash/libexec.3MJ3tz/misd									
2	OS	07c783e0ce9cccb0ad3500a6fee21706	mobile_file_relay	/Volumes/Data/stash/libexec.3MJ3tz/mobile_file_relay									
2	OS	7a112169e1305c734463214416057ec2	mobile_house_arrest	/Volumes/Data/stash/libexec.3MJ3tz/mobile_house_arrest									
2	OS	9b57efcdedbfa6cec8d786199d1f6969	mobile_image_mounter	/Volumes/Data/stash/libexec.3MJ3tz/mobile_image_mounter									
2	OS	9792eea82158fa196915c235bbf53713	mobile_installation_proxy	/Volumes/Data/stash/libexec.3MJ3tz/mobile_installation_proxy									
2	OS	4a496a15f6a5641c3b62c4028c37f799	mobile_integrity_relay	/Volumes/Data/stash/libexec.3MJ3tz/mobile_integrity_relay									
2	OS	d20d741bd3729f253895b0b52e9aebf6	mobile_obliterator	/Volumes/Data/stash/libexec.3MJ3tz/mobile_obliterator									
2	OS	2e3e8ec39c93345ea67a1753057ba24a	mobile_profile_janitor	/Volumes/Data/stash/libexec.3MJ3tz/mobile_profile_janitor									
2	OS	5dc1513028ff9375db2ccb2f04a3aa87	mtmergeprops	/Volumes/Data/stash/libexec.3MJ3tz/mtmergeprops									
2	OS	dbb42a23f28e9a65af3f05ee69b9c55f	notification_proxy	/Volumes/Data/stash/libexec.3MJ3tz/notification_proxy									
2	OS	07a34438dbf035b3d4ad24225bcad734	ptpd	/Volumes/Data/stash/libexec.3MJ3tz/ptpd									
2	OS	3694bc4764f082356e6cc130338e1b69	rmt	/Volumes/Data/stash/libexec.3MJ3tz/rmt									
2	OS	7add9c54a56b94c39bde4018a05ec8b8	securityd	/Volumes/Data/stash/libexec.3MJ3tz/securityd									
2	OS	67bc461f4acdd7b39285a35927aa7604	sftp-server	/Volumes/Data/stash/libexec.3MJ3tz/sftp-server									
2	OS	78ef48519ca93d5269aff7ce3810e94b	springboardservicesrelay	/Volumes/Data/stash/libexec.3MJ3tz/springboardservicesrelay									
2	OS	5aabbd421624f0490c8d7c46651f4e97	ssh-keysign	/Volumes/Data/stash/libexec.3MJ3tz/ssh-keysign									
2	OS	d3d58138daf1ea424ef46511b6eced49	ssh-rand-helper	/Volumes/Data/stash/libexec.3MJ3tz/ssh-rand-helper									
2	OS	b0ccf6b96585c32f3b8b2c2beff311d9	sshd-keygen-wrapper	/Volumes/Data/stash/libexec.3MJ3tz/sshd-keygen-wrapper									
2	OS	325b4c24c7033ba3605f51ccd3375f0b	stackshot	/Volumes/Data/stash/libexec.3MJ3tz/stackshot									
2	OS	80c30929d86fd55ec884db49232ce574	stackshotserver	/Volumes/Data/stash/libexec.3MJ3tz/stackshotserver									
2	OS	3672000d85076f8cdc81be1125681a03	syslog_relay	/Volumes/Data/stash/libexec.3MJ3tz/syslog_relay									
2	OS	ab85c1f96d01f227348ad1c4080dd495	vndevice	/Volumes/Data/stash/libexec.3MJ3tz/vndevice									
2	OS	5b8c7e2978316ca6678cc758a305c657	wifiFirmwareLoader	/Volumes/Data/stash/libexec.3MJ3tz/wifiFirmwareLoader									
2	OS	5acf2cf2b04618ebd8c14e9f14718018	pam_deny.so	/Volumes/Data/stash/pam.5T0eS0/pam_deny.so									
2	OS	a30b4ce3fbca68fe16fb5e1b528cc033	pam_launchd.so	/Volumes/Data/stash/pam.5T0eS0/pam_launchd.so									
2	OS	f3b6c0355254ad4637937d4501a0f692	pam_nologin.so	/Volumes/Data/stash/pam.5T0eS0/pam_nologin.so									
2	OS	38f06fdc207ea69ea52742775095071f	pam_permit.so	/Volumes/Data/stash/pam.5T0eS0/pam_permit.so									
2	OS	2625a06b81df0d6296730ee45bde43d2	pam_rootok.so	/Volumes/Data/stash/pam.5T0eS0/pam_rootok.so									
2	OS	891edfb9c6cac454269d04ccf5013323	pam_securetty.so	/Volumes/Data/stash/pam.5T0eS0/pam_securetty.so									
2	OS	2d95cba6a52d5d5cb5c94d69ab9875f1	pam_unix.so	/Volumes/Data/stash/pam.5T0eS0/pam_unix.so									
2	OS	4736d3e6b9a6bd925ec28bb3909be765	pam_uwtmp.so	/Volumes/Data/stash/pam.5T0eS0/pam_uwtmp.so									
2	OS	c96d0981be6e389a080a436e5652ed06	pam_wheel.so	/Volumes/Data/stash/pam.5T0eS0/pam_wheel.so									
2	OS	5f0b31c45aea9e2606b31c1731cad66f	merger.pl	/Volumes/Data/stash/share.R9s6NA/CSI/merger.pl									
2	OS	9e2c8b8f47c1cd424e8fa886df57e4c7	tz_map.plist	/Volumes/Data/stash/share.R9s6NA/CSI/tz_map.plist									
2	OS	9770b444596be9ba496d21f1adbd45b7	Ssh.bin	/Volumes/Data/stash/share.R9s6NA/Ssh.bin									
2	OS	7db45b6af2bbf8376e626c1ed69090e9	all-wcprops	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/all-wcprops									
2	OS	4d2978d56cfe46fcba90c7842222aca6	entries	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/entries									
2	OS	7c5aba41f53293b712fd86d08ed5b36e	format	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/format									
2	OS	113136892f2137aa0116093a524ade0b	bigboss.png.svn-base	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/prop-base/bigboss.png.svn-base									

2	OS	113136892f2137aa0116093a524ade0b	planetiphones.png.svn-base	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/prop-base/planetiphones.png.svn-base									
2	OS	113136892f2137aa0116093a524ade0b	touchrev.png.svn-base	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/prop-base/touchrev.png.svn-base									
2	OS	2fe728042b0a2751a73bbed9974042a0	bigboss.png.svn-base	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/text-base/bigboss.png.svn-base									
2	OS	26b835b59c7f17aa163d6171ed62078b	planetiphones.png.svn-base	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/text-base/planetiphones.png.svn-base									
2	OS	35131e1cbc241e9be04b4b2821d10e57	touchrev.png.svn-base	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/.svn/text-base/touchrev.png.svn-base									
2	OS	2fe728042b0a2751a73bbed9974042a0	bigboss.png	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/bigboss.png									
2	OS	26b835b59c7f17aa163d6171ed62078b	planetiphones.png	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/planetiphones.png									
2	OS	35131e1cbc241e9be04b4b2821d10e57	touchrev.png	/Volumes/Data/stash/share.R9s6NA/bigboss/icons/touchrev.png									
2	OS	77958a836a21dd6653a3a7c1b467158b	cputable	/Volumes/Data/stash/share.R9s6NA/dpkg/cputable									
2	OS	52712e5e15ce3fcb94cbb2bbb603e16e	ostable	/Volumes/Data/stash/share.R9s6NA/dpkg/ostable									
2	OS	889b16a4d57a043b0b6065677a5711c0	triplettable	/Volumes/Data/stash/share.R9s6NA/dpkg/triplettable									
2	OS	e2964485ac530b3934c4908ce24a90c1	Common.mtprops	/Volumes/Data/stash/share.R9s6NA/firmware/multitouch/Common.mtprops									
2	OS	3c69e5abb7e2a08f140be2e7e94bd6c9	iPhone.mtprops	/Volumes/Data/stash/share.R9s6NA/firmware/multitouch/iPhone.mtprops									
2	OS	f2e8c6ce2a8531348ed6c177314744b7	options.skel	/Volumes/Data/stash/share.R9s6NA/gnupg/options.skel									
2	OS	d679e399a4e54e9fac9b34247ec09e2e	icudt40l.dat	/Volumes/Data/stash/share.R9s6NA/icu/icudt40l.dat									
2	OS	0d928ac3e3abb93a83cd16e32e8b9e5f	bigboss-keyring.gpg	/Volumes/Data/stash/share.R9s6NA/keyrings/bigboss-keyring.gpg									
2	OS	ba4cda977d6b253150de241af17e44fe	modmyi.com-keyring.gpg	/Volumes/Data/stash/share.R9s6NA/keyrings/modmyi.com-keyring.gpg									
2	OS	01dfcb35e246cc9c125420b7691e10ba	saurik-keyring.gpg	/Volumes/Data/stash/share.R9s6NA/keyrings/saurik-keyring.gpg									
2	OS	7368c90f29d29d3566022928184bcd94	zodttd-keyring.gpg	/Volumes/Data/stash/share.R9s6NA/keyrings/zodttd-keyring.gpg									
2	OS	47a85edd4e45b05fd17b870bf2e59f37	langid.inv	/Volumes/Data/stash/share.R9s6NA/langid/langid.inv									
2	OS	0633f2811ab9958deef70a4ceb124d2e	std	/Volumes/Data/stash/share.R9s6NA/tabset/std									
2	OS	75738443f4560dabbbb5781a43b6076f	stdcrt	/Volumes/Data/stash/share.R9s6NA/tabset/stdcrt									
2	OS	932387cdf8429aba6dd9c6567022829a	vt100	/Volumes/Data/stash/share.R9s6NA/tabset/vt100									
2	OS	fd329c87dc8cfd0191c9e9b4c891460b	vt300	/Volumes/Data/stash/share.R9s6NA/tabset/vt300									
2	OS	e423bd9bc2bd529f46a43f834bfe82a3	Eterm	/Volumes/Data/stash/share.R9s6NA/terminfo/E/Eterm									
2	OS	2e2fba96feeafdff8a8becf756b6a8ca	Eterm-256color	/Volumes/Data/stash/share.R9s6NA/terminfo/E/Eterm-256color									
2	OS	c0f4530998290ba7a891eb28c9977dd7	Eterm-88color	/Volumes/Data/stash/share.R9s6NA/terminfo/E/Eterm-88color									
2	OS	e423bd9bc2bd529f46a43f834bfe82a3	Eterm-color	/Volumes/Data/stash/share.R9s6NA/terminfo/E/Eterm-color									
2	OS	6b3a86ff2f1b95acfdd820fbf8750b01	ansi	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi									
2	OS	f18d72643477964bafbb499a518afab3	ansi-color-2-emx	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-color-2-emx									
2	OS	bd5a24c27f2aae15e7c8616478b35177	ansi-color-3-emx	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-color-3-emx									
2	OS	a811d944eb78b2a1f97aa6578dca08fa	ansi-emx	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-emx									
2	OS	30ef341210e5227e41eaff5b83fac717	ansi-generic	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-generic									
2	OS	0929a9ac82bd6cb0238dfb7577b8240f	ansi-m	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-m									
2	OS	c12e955efc5c4f813357a89fd90a84b3	ansi-mini	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-mini									
2	OS	0929a9ac82bd6cb0238dfb7577b8240f	ansi-mono	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-mono									
2	OS	d59ad3dfe0d905f83febae83bbb6490d	ansi-mr	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-mr									
2	OS	042f8da76683abcdace3439800571223	ansi-mtabs	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-mtabs									
2	OS	5b2a31e020e45acef8b3154423e36061	ansi-nt	/Volumes/Data/stash/share.R9s6NA/terminfo/a/ansi-nt									
2	OS	5eb691998583e67c1d1d66f6d1b065ba	cons25	/Volumes/Data/stash/share.R9s6NA/terminfo/c/cons25									
2	OS	5cc9c4e94f47197a1171e8841c0909a6	cons25-m	/Volumes/Data/stash/share.R9s6NA/terminfo/c/cons25-m									
2	OS	1e5d48c1d64c2b71712885a10e1144e1	cygwin	/Volumes/Data/stash/share.R9s6NA/terminfo/c/cygwin									
2	OS	ca3b114f0727da81a9b957b553a9915d	dumb	/Volumes/Data/stash/share.R9s6NA/terminfo/d/dumb									
2	OS	645999d4afb490d40ff6b55239ad8173	linux	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux									
2	OS	c908ab61179176e87feeffea61d48550	linux-basic	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-basic									
2	OS	d430677ee48aaa29b1ec07856fadf1b3	linux-c	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-c									
2	OS	3497148074bf923fb5947f332143b4dc	linux-c-nc	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-c-nc									
2	OS	1e2899cc9d0dbb7e97adc7c6117e296c	linux-koi8	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-koi8									
2	OS	0a3b98f41dbaa4ec10b6b33e1f7e5fb8	linux-koi8r	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-koi8r									
2	OS	6571655c5c8e2cdd82754860b0f12cf9	linux-lat	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-lat									
2	OS	859f454b42150769255dcb99d7715769	linux-m	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-m									
2	OS	ef9a25f74c562344cc9840830df27ce9	linux-nic	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-nic									
2	OS	53ab5f398fdf2fc9a04e3d443439c748	linux-vt	/Volumes/Data/stash/share.R9s6NA/terminfo/l/linux-vt									
2	OS	d982b12970acbb48d594ed799615f036	mach	/Volumes/Data/stash/share.R9s6NA/terminfo/m/mach									
2	OS	21465595967257ad4020192c005cb280	mach-bold	/Volumes/Data/stash/share.R9s6NA/terminfo/m/mach-bold									
2	OS	1bb86008400135036fea5773a9c819a1	mach-color	/Volumes/Data/stash/share.R9s6NA/terminfo/m/mach-color									
2	OS	59b6cdc31d1b042fbe93c693ad95fe28	pcansi	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi									
2	OS	1228baff2c0705bbd2384f949bc5c977	pcansi-25	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi-25									
2	OS	e3e5c30baba77f73d46a46ecfa7bd21d	pcansi-25-m	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi-25-m									
2	OS	4dafc07d86a10cd900bd6f1b8c53654c	pcansi-33	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi-33									
2	OS	7f059a2503c236bfa43f4be3ca4f5ff1	pcansi-33-m	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi-33-m									
2	OS	fcda11090c2ae5aaa236d4aa3b2b1b0c	pcansi-43	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi-43									
2	OS	6871af613871edf164a0656f20dc2c8c	pcansi-43-m	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi-43-m									
2	OS	dbcd0d12e10979f825a5ec0254dbfd54	pcansi-m	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi-m									
2	OS	dbcd0d12e10979f825a5ec0254dbfd54	pcansi-mono	/Volumes/Data/stash/share.R9s6NA/terminfo/p/pcansi-mono									
2	OS	71b1ed5d7c75fe9c959eb2fb8949fbd6	rxvt	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt									
2	OS	592c7a2a26f5641dfafa58d3b1bbdb91	rxvt-16color	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt-16color									
2	OS	f03948a7106681bc78bc2c411ef30d3a	rxvt-256color	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt-256color									
2	OS	033684ea08fcf1458a42809afb15858e	rxvt-88color	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt-88color									
2	OS	db474903470b8b12b4b06a6565023515	rxvt-basic	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt-basic									
2	OS	4f6052f8c49693e1ad79c765b419dbd8	rxvt-color	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt-color									
2	OS	910a311202ff5971c28822d15a3ca187	rxvt-cygwin	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt-cygwin									
2	OS	162b5a65c2c8091600ef7a662b657659	rxvt-cygwin-native	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt-cygwin-native									

2	OS	81f1b8a188ce986ef5e753cbce63b7ed	rxvt-xpm	/Volumes/Data/stash/share.R9s6NA/terminfo/r/rxvt-xpm									
2	OS	206907aeaa38189a8b2e74feae020f91	screen	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen									
2	OS	758da19fa1ad8fa0aa8872d2fa4fabc2	screen-16color	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-16color									
2	OS	bc62056fcb4a9609cb0ce74bbf3fa5e8	screen-16color-bce	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-16color-bce									
2	OS	6e536f3f0ca81e760cca30af42ef5ee5	screen-16color-bce-s	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-16color-bce-s									
2	OS	4209d2ad407722c4ee0d38679569633f	screen-16color-s	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-16color-s									
2	OS	ffb01624d78c3593c3a5c34624186a7d	screen-256color	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-256color									
2	OS	acdec11a201772f9868008c9b35370a4	screen-256color-bce	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-256color-bce									
2	OS	ac3ad0fb0869538166f5a12fbcfe0c21	screen-256color-bce-s	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-256color-bce-s									
2	OS	40e690ba777f5df6351949d569a0c419	screen-256color-s	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-256color-s									
2	OS	1e076f070f12f1039f827e518717c5e0	screen-bce	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-bce									
2	OS	6db29fffc6c61f7ce0052805f9d997d9	screen-s	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-s									
2	OS	2fdd2ae242a69fc6a6846adbad436bfb	screen-w	/Volumes/Data/stash/share.R9s6NA/terminfo/s/screen-w									
2	OS	d98cf6c328f0358c93389a38a95c0d6b	sun	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun									
2	OS	73d2274eebdcd0c6c883c8b45415c8d8	sun-1	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-1									
2	OS	42d36f1eb0a148b31abde05cd379b511	sun-12	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-12									
2	OS	35c4f494ab0a252601eb497853464232	sun-17	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-17									
2	OS	5b5a235a7e0c86199e1bd03edf9ae4a0	sun-24	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-24									
2	OS	6d2a29e9eef4f87fefa15ceb2f336a45	sun-34	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-34									
2	OS	2685c4a11a200f509ed57356a467e115	sun-48	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-48									
2	OS	17855d638fdbdc7b009b4cbd9647d62e	sun-c	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-c									
2	OS	9c33ac095fbd9b2861642d99c72feb39	sun-cgsix	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-cgsix									
2	OS	17855d638fdbdc7b009b4cbd9647d62e	sun-cmd	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-cmd									
2	OS	fd226fd5d226fd60695db8b319653bf6	sun-color	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-color									
2	OS	9eaddcb3877b7f2efeea9ef8e597f316	sun-e	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-e									
2	OS	03cb6c586712da3cbd518e9b788e0ebb	sun-e-s	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-e-s									
2	OS	cb0cb326eb8d3b7cc9ab728474c87c12	sun-il	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-il									
2	OS	9eaddcb3877b7f2efeea9ef8e597f316	sun-nic	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-nic									
2	OS	4d3d34c870f3f92739f38185fa50fe36	sun-s	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-s									
2	OS	03cb6c586712da3cbd518e9b788e0ebb	sun-s-e	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-s-e									
2	OS	9c33ac095fbd9b2861642d99c72feb39	sun-ss5	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-ss5									
2	OS	1b627e7c1467991817a4144cfc5ba2cf	sun-type4	/Volumes/Data/stash/share.R9s6NA/terminfo/s/sun-type4									
2	OS	96300e9c1b0dea5f61383f5d22342ef3	vt100	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100									
2	OS	96300e9c1b0dea5f61383f5d22342ef3	vt100-am	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-am									
2	OS	846029909338b3ee934e3cc1de3f3c0e	vt100-bot-s	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-bot-s									
2	OS	f99eba18048c6edefef69b2aa6cf9671	vt100-nam-w	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-nam-w									
2	OS	76baa3a9460d6112ac20dbf6f58725c2	vt100-nav	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-nav									
2	OS	5ab1f7397095f804dcb33dd95358ff71	vt100-nav-w	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-nav-w									
2	OS	a06a3fcbf8aebe420717a1933eb21572	vt100-putty	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-putty									
2	OS	4aaaf3867c2dd1faef92e6519d38e26e	vt100-s	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-s									
2	OS	846029909338b3ee934e3cc1de3f3c0e	vt100-s-bot	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-s-bot									
2	OS	4aaaf3867c2dd1faef92e6519d38e26e	vt100-s-top	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-s-top									
2	OS	4aaaf3867c2dd1faef92e6519d38e26e	vt100-top-s	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-top-s									
2	OS	5619ee07eba86463eb529b11fa45b7a5	vt100-vb	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-vb									
2	OS	25cbb52e83f147f21489d20addde7cd1	vt100-w	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-w									
2	OS	25cbb52e83f147f21489d20addde7cd1	vt100-w-am	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-w-am									
2	OS	f99eba18048c6edefef69b2aa6cf9671	vt100-w-nam	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-w-nam									
2	OS	5ab1f7397095f804dcb33dd95358ff71	vt100-w-nav	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt100-w-nav									
2	OS	5fe25a4370c02f4ddee6285eac2ab974	vt102	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt102									
2	OS	3289ee83b320e9b50f76efee3989016d	vt102-nsgr	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt102-nsgr									
2	OS	c5288bac8ef58eb512cc4e7b62ac79db	vt102-w	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt102-w									
2	OS	b2c90e2aaf7dc659c448d503a928bd05	vt220	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt220									
2	OS	593e91d4890a120e546532041555d4bd	vt220-8	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt220-8									
2	OS	593e91d4890a120e546532041555d4bd	vt220-8bit	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt220-8bit									
2	OS	1c798f9a26cc03551b3373f714097082	vt220-nam	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt220-nam									
2	OS	e7fbd0015ccc939df94a1970b9f9acca	vt220-old	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt220-old									
2	OS	80c39fca1a28fbaea5e41ea2d5a0735f	vt220-w	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt220-w									
2	OS	76df7c33a770fe4239c34c3dfb56ce1b	vt52	/Volumes/Data/stash/share.R9s6NA/terminfo/v/vt52									
2	OS	353443e47e0d0fe2d15535659e3b04af	xterm	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm									
2	OS	7e0ad52fc6dfe3e3b84e2a5a1c3004b8	xterm-1002	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-1002									
2	OS	11c965f11932634115646b5b237d5007	xterm-1003	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-1003									
2	OS	d94a6297e7ca3159c8ebb42e837b84ea	xterm-16color	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-16color									
2	OS	3cd412804c7a72ee56240cf422adaeca	xterm-24	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-24									
2	OS	0ba872cd880784a95b7af42a83c48949	xterm-256color	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-256color									
2	OS	a27d4fd9298162c7fe1086c7f16c4ecd	xterm-88color	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-88color									
2	OS	6067dd7e9549184fb9fbff4e974bc68f	xterm-8bit	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-8bit									
2	OS	9475482054b7cef735ff525dfa8e2432	xterm-basic	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-basic									
2	OS	b55edd6b80d3889b13cb568db626ccdc	xterm-bold	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-bold									
2	OS	d3be06075003387119121112f0cb3d690	xterm-color	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-color									
2	OS	c3c7c94ee7fba1f2b3988da5566822f0	xterm-hp	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-hp									
2	OS	8bee222d594313ae4fb74c75f90dca60	xterm-new	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-new									
2	OS	1c7acb51473c2dca2eeb0f84067db2a3	xterm-nic	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-nic									
2	OS	f9029cc45ee3e6b1ea30b0d3b1d845ea	xterm-noapp	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-noapp									

2	OS	eb03b6f5d4bb1266c4819b2f4df678bd	xterm-old	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-old									
2	OS	0082abb739267995f310520c01800b7a	xterm-pcolor	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-pcolor									
2	OS	39078c3627cceef6887d35d3e2dfa627	xterm-r5	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-r5									
2	OS	eb03b6f5d4bb1266c4819b2f4df678bd	xterm-r6	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-r6									
2	OS	66eb456a4c631191ca680bd8118df898	xterm-sco	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-sco									
2	OS	ae568e2b928093c308ce588c5f0aa8aa	xterm-sun	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-sun									
2	OS	e2b6b6e1a395e624668a994d5dbe6f92	xterm-vt220	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-vt220									
2	OS	bad6815dc79a0c7e0c9178f4c468d5c0	xterm-vt52	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-vt52									
2	OS	bec969d44d50acd8021054876d3aea8a	xterm-xf86-v32	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-xf86-v32									
2	OS	9eb87468c62a270b9a5ac8084078a33a	xterm-xf86-v33	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-xf86-v33									
2	OS	6d445e7a55cdedbb8b7f89b5b5148627	xterm-xf86-v333	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-xf86-v333									
2	OS	56995737bfe7f6c6fd93c670277924da	xterm-xf86-v40	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-xf86-v40									
2	OS	be0084efb2d8cc41175d9efa79b07b30	xterm-xf86-v43	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-xf86-v43									
2	OS	c66852864fa765e6ae9977f7c0f9c289	xterm-xf86-v44	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-xf86-v44									
2	OS	74a3ee0b701d7eaea58a06abbef1e639	xterm-xfree86	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-xfree86									
2	OS	a06055e5748916109b0352b00c8bffb1	xterm-xi	/Volumes/Data/stash/share.R9s6NA/terminfo/x/xterm-xi									
2	OS	464e2e1b18a93f9598593bd52fffb248	+VERSION	/Volumes/Data/stash/share.R9s6NA/zoneinfo/+VERSION									
2	OS	4bb3515a02f5789386360e076bbc80cf	Abidjan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Abidjan									
2	OS	193348a135d6e073652bd6a976f21058	Accra	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Accra									
2	OS	667eaf22c7998d054df713b0d20a37a0	Addis_Ababa	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Addis_Ababa									
2	OS	436d2e2d33c60b2413cfb0ef0e27ca48	Algiers	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Algiers									
2	OS	667eaf22c7998d054df713b0d20a37a0	Asmara	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Asmara									
2	OS	667eaf22c7998d054df713b0d20a37a0	Asmera	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Asmera									
2	OS	c0b5a299d5de5e5cf2e55f399e8b5f67	Bamako	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Bamako									
2	OS	0b4cc560f192b0a3f5fcd0629f751da3	Bangui	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Bangui									
2	OS	12ad58b6b4f91b3e0ebaf5421b60312f	Banjul	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Banjul									
2	OS	33235e69dbf1a837a0c788e065857a46	Bissau	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Bissau									
2	OS	0a96e887c7105299e4e6e7873e9b5e9f	Blantyre	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Blantyre									
2	OS	3b5556871272606fc69869285d22bbbb	Brazzaville	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Brazzaville									
2	OS	77cc861e2fc25001a436c70f092e0976	Bujumbura	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Bujumbura									
2	OS	c79cfc2f93856b816adb63b52a2e8568	Cairo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Cairo									
2	OS	36d89cbb361f55804658528fa4706a0f	Casablanca	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Casablanca									
2	OS	e91dee271de7431c3448dd6a2519572b	Ceuta	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Ceuta									
2	OS	acea3944efa196ee332039d609039cb1	Conakry	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Conakry									
2	OS	2f636936a69f20af8c856a12dd3428ac	Dakar	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Dakar									
2	OS	f97931e6fac3c138b6a1c0a555fdd15f	Dar_es_Salaam	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Dar_es_Salaam									
2	OS	dbb78c5f87aaf959f43f4c273c90e020	Djibouti	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Djibouti									
2	OS	0acb9f98a8c3cb936b4342bf785c07fd	Douala	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Douala									
2	OS	fdbfeabed8c80fe4d190f32565819911	El_Aaiun	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/El_Aaiun									
2	OS	83c05207129cf0d5aa705fe0d4780a27	Freetown	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Freetown									
2	OS	f47be3c7c2549fc1234173bdb8b74e1c	Gaborone	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Gaborone									
2	OS	9f42ab696a1b4d189af06b861203fbf3	Harare	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Harare									
2	OS	21f86e3286e1b1adbc228fd2f0451fd3	Johannesburg	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Johannesburg									
2	OS	5b11b74cba33269ceb44c0a8744d6b09	Kampala	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Kampala									
2	OS	d8c4be0f2971f95ad5565d2fa8fe9169	Khartoum	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Khartoum									
2	OS	09bf9011e2b7bf228f9ae1c0ffdf490c	Kigali	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Kigali									
2	OS	4b37800d2aa9ddde113fc9d5d688af98	Kinshasa	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Kinshasa									
2	OS	6ac3db2b4eec920c21c7730317d4d4a3	Lagos	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Lagos									
2	OS	d1a2caa8b49269d3198e8f60b6f8b49b	Libreville	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Libreville									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	Lome	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Lome									
2	OS	c72811eb3992ce20c99128ad331c7ed9	Luanda	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Luanda									
2	OS	77cc861e2fc25001a436c70f092e0976	Lubumbashi	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Lubumbashi									
2	OS	12d2702a5857db8423563b69b8d79c55	Lusaka	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Lusaka									
2	OS	62f2befa2d2457cea5ae64a7f4c2d25d	Malabo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Malabo									
2	OS	e4fb673a6006b4249533054961b4c73d	Maputo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Maputo									
2	OS	ee02cb735dc89f13c4dc62da83c1f54c	Maseru	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Maseru									
2	OS	b82e195e075169e8966c3cdbf150c6b4	Mbabane	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Mbabane									
2	OS	1c0aeadcc0fe06fc197f38474b9a7c9a	Mogadishu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Mogadishu									
2	OS	cc159838a58ab5b7cc0e2b4d82ff0e76	Monrovia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Monrovia									
2	OS	68931c53fb9c89a3f762234d4066a9ad	Nairobi	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Nairobi									
2	OS	31cd003527d9b1fd4afe510b58c153cd	Ndjamena	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Ndjamena									
2	OS	2fcea9a476c14ef765c53df26196c32f	Niamey	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Niamey									
2	OS	23916f09b702bec5eebf66ce747c777a	Nouakchott	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Nouakchott									
2	OS	73bd2722f7f7f4d9ebb735c629e4cdef	Ouagadougou	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Ouagadougou									
2	OS	490197c4079132b3d13ff2d53b5f83e5	Porto-Novo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Porto-Novo									
2	OS	335e7e0ed7f2db50479e5c08feceacbe	Sao_Tome	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Sao_Tome									
2	OS	c0b5a299d5de5e5cf2e55f399e8b5f67	Timbuktu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Timbuktu									
2	OS	18167cde0c74d2c43a91e5945eb83548	Tripoli	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Tripoli									
2	OS	5343609fc18adb33c9d88c911940afa3	Tunis	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Tunis									
2	OS	df2200717e6335e9f8d626494d19f47f	Windhoek	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Africa/Windhoek									
2	OS	6fa956ed6227abd78894a642bd07e359	Adak	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Adak									
2	OS	ebc2ed4fcb5c9c2dee6b8ef4fe2e1cd9	Anchorage	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Anchorage									
2	OS	98128f8d5b758117f72db10200239e2a	Anguilla	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Anguilla									

2	OS	82c379afee77a10a2f222e901605c1c4	Antigua	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Antigua									
2	OS	413faebbb412711edce964d14f3d52ea	Araguaina	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Araguaina									
2	OS	af54267bb8a708bff17143226e45b425	Buenos_Aires	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Buenos_Aires									
2	OS	e65741afec1b4c50eecc6ecc04cf2fc5	Catamarca	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Catamarca									
2	OS	e65741afec1b4c50eecc6ecc04cf2fc5	ComodRivadavia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/ComodRivadavia									
2	OS	7d7414b5b0196464fc374f10959b5f5a	Cordoba	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Cordoba									
2	OS	78cea847932808364a71bfcc12369ebe	Jujuy	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Jujuy									
2	OS	702c0d24cdf513b5121e9631ef55ee7d	La_Rioja	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/La_Rioja									
2	OS	ee153072f6503844f0ae3c9c081bca1c	Mendoza	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Mendoza									
2	OS	31f1a559abeeefb3f4e5679ab057c2f5	Rio_Gallegos	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Rio_Gallegos									
2	OS	ae0923724e095f796b297064e7c06cd1	Salta	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Salta									
2	OS	4b544a82da9dbb7f7cd7b716f558f613	San_Juan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/San_Juan									
2	OS	a73cada9cd7fd4563a07546b2b9f5b7d	San_Luis	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/San_Luis									
2	OS	bf594754664475e8053fb78c175cb9c6	Tucuman	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Tucuman									
2	OS	7fd023eee0f68e135374f0ff1f5edae7	Ushuaia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Argentina/Ushuaia									
2	OS	729d7fc9c7ab0f95e41f1012489fcc60	Aruba	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Aruba									
2	OS	9b3efcf3c049faa4a7aa8c940d19e11b	Asuncion	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Asuncion									
2	OS	fc5507ad5fe66fed7004a00c45a63e79	Atikokan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Atikokan									
2	OS	6fa956ed6227abd78894a642bd07e359	Atka	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Atka									
2	OS	a2dbe2b9ba601b4af56d08e6a6d780a2	Bahia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Bahia									
2	OS	4740e465bb502628f55825f12d679fa9	Barbados	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Barbados									
2	OS	72618cc12c0a81bb8fa12456e67bb1a8	Belem	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Belem									
2	OS	90ee33c4bc621ac33f2bb1addb742a91	Belize	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Belize									
2	OS	c5c85703c7583877609891e176b721e0	Blanc-Sablon	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Blanc-Sablon									
2	OS	6448f638bd40665207249b94edb28bda	Boa_Vista	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Boa_Vista									
2	OS	e4c6983da75fe762292bbd0a4b409536	Bogota	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Bogota									
2	OS	ed121a16c5013ce95b211e4e3a4ecd4e	Boise	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Boise									
2	OS	af54267bb8a708bff17143226e45b425	Buenos_Aires	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Buenos_Aires									
2	OS	a280c02cba234d9d566a0f2415bbddc3	Cambridge_Bay	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Cambridge_Bay									
2	OS	e781a5e5e9f14f00b1e02e6b1a44fb21	Campo_Grande	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Campo_Grande									
2	OS	dead1c888613edd0d0dccc50a876ac3b	Cancun	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Cancun									
2	OS	b06261088c1fb7ecddafff9c2c5a8930	Caracas	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Caracas									
2	OS	e65741afec1b4c50eecc6ecc04cf2fc5	Catamarca	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Catamarca									
2	OS	b334d0ffdbf5c0507d8748241d9a19fc	Cayenne	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Cayenne									
2	OS	e5ec2d70551b76ec5893897527db3c39	Cayman	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Cayman									
2	OS	3fa8f0dc6fa2ab843dfa3dc1c0a0f72a	Chicago	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Chicago									
2	OS	35fa4f7b68b7151b992358aa81c48bcb	Chihuahua	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Chihuahua									
2	OS	fc5507ad5fe66fed7004a00c45a63e79	Coral_Harbour	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Coral_Harbour									
2	OS	7d7414b5b0196464fc374f10959b5f5a	Cordoba	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Cordoba									
2	OS	5512633fab501b4cbae9d164d5e8e2db	Costa_Rica	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Costa_Rica									
2	OS	ba121d344b3e7dd361f3421114e974bb	Cuiaba	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Cuiaba									
2	OS	05e9327f9e392e76eddab757d8e7efee	Curacao	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Curacao									
2	OS	248bd1fef6c539ed775ae27b6aa28051	Danmarkshavn	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Danmarkshavn									
2	OS	18f96f4be0aecc2c3e9ab3c753f2e4ed	Dawson	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Dawson									
2	OS	29b48ef269fda5c0fcbbe4d788a1272d	Dawson_Creek	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Dawson_Creek									
2	OS	db1d61b98712f8923bbb9d9708625432	Denver	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Denver									
2	OS	8742f5ca104dd4330d947a86efce1a6b	Detroit	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Detroit									
2	OS	d74349de372024d84bc00a7e9da378b4	Dominica	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Dominica									
2	OS	4f1f996bf8a059b5c0f6caa73c0fe7db	Edmonton	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Edmonton									
2	OS	d1eab0f8a23f576ddd7ee0c8dfa784ee	Eirunepe	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Eirunepe									
2	OS	952dc4c8b21a0fa860f6593bef6cddff	El_Salvador	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/El_Salvador									
2	OS	64eb211e4362ad4550c535eb88676f6b	Ensenada	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Ensenada									
2	OS	01f76c02facbee6cba7246bd88d07a59	Fort_Wayne	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Fort_Wayne									
2	OS	908655b4b2f6853b5bb4210214e02b78	Fortaleza	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Fortaleza									
2	OS	bbfe2376f5e0b9fc37883c9cb46167e9	Glace_Bay	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Glace_Bay									
2	OS	98903c40ef33a57353344f3c060ffd17	Godthab	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Godthab									
2	OS	e63d2117d7c81a58f2710dc7d8b7e105	Goose_Bay	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Goose_Bay									
2	OS	e42b94ba9e88bfc3a901a48f51a30f97	Grand_Turk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Grand_Turk									
2	OS	a9a531384a9f889f8a7dfd2a8abc4822	Grenada	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Grenada									
2	OS	c24061a202a2da55bbd2ca608e834204	Guadeloupe	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Guadeloupe									
2	OS	62086b178e989cda1e6f77b3c6c321ec	Guatemala	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Guatemala									
2	OS	a7983a99ae9e865cff90aca9a56ac0e7	Guayaquil	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Guayaquil									
2	OS	4d570b84954377012008972d34dfbbe0	Guyana	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Guyana									
2	OS	0446ea93da671cbd751933bfd10c7088	Halifax	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Halifax									
2	OS	6ea65224f35ad74ea50f56683068dba2	Havana	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Havana									
2	OS	1fb31b743501959933a3e7bb16a1913b	Hermosillo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Hermosillo									
2	OS	01f76c02facbee6cba7246bd88d07a59	Indianapolis	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indiana/Indianapolis									
2	OS	9b6c9c30d9ac3e7709bc5d42867b2f06	Knox	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indiana/Knox									
2	OS	e8aad460c36db485c517e9a210f5de87	Marengo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indiana/Marengo									
2	OS	e33ff3331b8ce868473f9a4c5891e0c1	Petersburg	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indiana/Petersburg									
2	OS	9c6f083f0f55c489623622625d45552e	Tell_City	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indiana/Tell_City									
2	OS	85210672e169fdbeb20308514f9b56ef	Vevay	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indiana/Vevay									
2	OS	23111e1ae3fb6bba4640946f6642456a	Vincennes	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indiana/Vincennes									

2	OS	72daa7d3ddfaae5937043ac1db99ed62	Winamac	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indiana/Winamac									
2	OS	01f76c02facbee6cba7246bd88d07a59	Indianapolis	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Indianapolis									
2	OS	79277321396ef003e6e4db746606b8c5	Inuvik	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Inuvik									
2	OS	3b556c64fd52143329ef90b38a4381f7	Iqaluit	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Iqaluit									
2	OS	598c3e5fa32cfd9ff03842dc3fc937e1	Jamaica	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Jamaica									
2	OS	78cea847932808364a71bfcc12369ebe	Jujuy	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Jujuy									
2	OS	01d344dec59bdbd51ea05f23d7749741	Juneau	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Juneau									
2	OS	77d9ea1a013b8554a5cf3bd61b0fb001	Louisville	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Kentucky/Louisville									
2	OS	1348cd856a07bf9cd2076b9af31df71a	Monticello	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Kentucky/Monticello									
2	OS	9b6c9c30d9ac3e7709bc5d42867b2f06	Knox_IN	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Knox_IN									
2	OS	bc193016a96ff178a7db1d425aca0378	La_Paz	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/La_Paz									
2	OS	c1128c410ce5aa69cf6a501bea580fd0	Lima	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Lima									
2	OS	ad7be76a1d7216104d9004a73e200efc	Los_Angeles	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Los_Angeles									
2	OS	77d9ea1a013b8554a5cf3bd61b0fb001	Louisville	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Louisville									
2	OS	a14e2ff78996fc00e93d2c2942351717	Maceio	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Maceio									
2	OS	ce59ed877e436c002420a21d46ba8aae	Managua	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Managua									
2	OS	24210f1a2615a304bf58b9f07f4f326a	Manaus	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Manaus									
2	OS	c24061a202a2da55bbd2ca608e834204	Marigot	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Marigot									
2	OS	198a79b22ed0a313b38cfd7d4116f199	Martinique	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Martinique									
2	OS	aebae9a378965894a3c40cf4e1a3c1c2	Mazatlan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Mazatlan									
2	OS	ee153072f6503844f0ae3c9c081bca1c	Mendoza	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Mendoza									
2	OS	f0b3e3915172da7c0bbb4399dfde4df6	Menominee	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Menominee									
2	OS	490707831b601273e48b8e12e8da5c79	Merida	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Merida									
2	OS	a6d2cd65c99b1991c70925b0146001e7	Mexico_City	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Mexico_City									
2	OS	272f644d27974cd152943a7e5fceea51	Miquelon	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Miquelon									
2	OS	fb1fc068cfe5700d08bbd6cbce3c892f	Moncton	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Moncton									
2	OS	c1ef9df81967e25a2bd98acea53fca6e	Monterrey	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Monterrey									
2	OS	2b8c71ceb70debaa68ce3d977722819b	Montevideo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Montevideo									
2	OS	8dde031b248d7e61f40f7849d9e9a0df	Montreal	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Montreal									
2	OS	f47d234597db32361c30171c0806223f	Montserrat	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Montserrat									
2	OS	4cd6b13fd0b37503ced04b75b232aa12	Nassau	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Nassau									
2	OS	3cf0ccc7d6b240390188367933c9cd90	New_York	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/New_York									
2	OS	d54d2ca6ebf3345ad40f821993ab1569	Nipigon	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Nipigon									
2	OS	c898d31a352e6595f1dcc2eed7d943fa	Nome	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Nome									
2	OS	b3763578fe1f4575cb65f33c2d3d1c5a	Noronha	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Noronha									
2	OS	3e2886da620a20a8bcf82e75bb744277	Center	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/North_Dakota/Center									
2	OS	2526da9962b5dd51d818e2aaf54965fb	New_Salem	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/North_Dakota/New_Salem									
2	OS	305352fce44f3d8c36cfb316abf4904a	Panama	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Panama									
2	OS	ecb49133463758096e9b12c93f7779cc	Pangnirtung	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Pangnirtung									
2	OS	a0d8be7821c1b5f8d1a9a3a32d73d0fd	Paramaribo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Paramaribo									
2	OS	3d786c31307428005972ee5b6f2a3659	Phoenix	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Phoenix									
2	OS	c1a444ee4f999cfffcdf8521c38ea637	Port-au-Prince	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Port-au-Prince									
2	OS	9aaa7582599d6721d6e58f652e081bf5	Port_of_Spain	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Port_of_Spain									
2	OS	0e57862dbc12163ef9f2788d13b8d5ea	Porto_Acre	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Porto_Acre									
2	OS	dd12bae88306b56b7747a2159b2dac2f	Porto_Velho	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Porto_Velho									
2	OS	01acd25614ed191e6d81f20595f83e49	Puerto_Rico	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Puerto_Rico									
2	OS	c07109bcd9850d9a02006a82738229c6	Rainy_River	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Rainy_River									
2	OS	1d36d4b59b1183c228b0e2b18e9cb010	Rankin_Inlet	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Rankin_Inlet									
2	OS	3b78e10b0c5360a6bdac7305872fa3b1	Recife	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Recife									
2	OS	988a01f8ecfaf4c6e91d3315b86c52cf	Regina	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Regina									
2	OS	d080c51918ff284f132de77ddd4533ed	Resolute	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Resolute									
2	OS	0e57862dbc12163ef9f2788d13b8d5ea	Rio_Branco	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Rio_Branco									
2	OS	7d7414b5b0196464fc374f10959b5f5a	Rosario	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Rosario									
2	OS	87aba19ce010894678da14d7673dfac6	Santarem	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Santarem									
2	OS	f9664d412a224a98c79c49e04c7e0281	Santiago	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Santiago									
2	OS	c3fc9a93821b71a0ff49785e7cb104ba	Santo_Domingo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Santo_Domingo									
2	OS	9d1d4990eb40b53bf1b9688caf690e9d	Sao_Paulo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Sao_Paulo									
2	OS	8f5cd60f9e3f84032ca803c514e4e420	Scoresbysund	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Scoresbysund									
2	OS	db1d61b98712f8923bbb9d9708625432	Shiprock	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Shiprock									
2	OS	c24061a202a2da55bbd2ca608e834204	St_Barthelemy	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/St_Barthelemy									
2	OS	1544a77fe6bcf16d429fcf0d6b82f767	St_Johns	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/St_Johns									
2	OS	687bc5ebdecb0e3965c3486659deac9d	St_Kitts	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/St_Kitts									
2	OS	0b5cca27563a5f5954dad0838830a1c2	St_Lucia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/St_Lucia									
2	OS	79ac74f0d29b663c3cce497765f83a1a	St_Thomas	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/St_Thomas									
2	OS	81f20c4e314b323c256f99995c25554a	St_Vincent	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/St_Vincent									
2	OS	984a877e768241bbe22cc8b639ae7038	Swift_Current	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Swift_Current									
2	OS	19eed85a5b6ff9a154c7826859af21db	Tegucigalpa	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Tegucigalpa									
2	OS	d1bc9f1437a8c7d50db775a83d8570de	Thule	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Thule									
2	OS	f3366ea3582eb4ef45ddc35128fd8e52	Thunder_Bay	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Thunder_Bay									
2	OS	64eb211e4362ad4550c535eb88676f6b	Tijuana	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Tijuana									
2	OS	82980b1345aab5a97d90307edfefb6da	Toronto	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Toronto									
2	OS	92f5c4620f3d50245fa23fdbf132c006	Tortola	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Tortola									
2	OS	ed5406f379fa648906bc366499ae087d	Vancouver	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Vancouver									

2	OS	79ac74f0d29b663c3cce497765f83a1a	Virgin	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Virgin									
2	OS	1f6419c3be16190917b018b8a61db105	Whitehorse	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Whitehorse									
2	OS	97d2e564f4bf3855f1d52c2f738358fc	Winnipeg	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Winnipeg									
2	OS	811cdcf1f0427664ff6833dc8835a267	Yakutat	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Yakutat									
2	OS	3a84e72bae741466ac278a78dac66302	Yellowknife	/Volumes/Data/stash/share.R9s6NA/zoneinfo/America/Yellowknife									
2	OS	472572722019350 0e3052a5fafa7d3ce	Casey	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/Casey									
2	OS	4a45942116607d299093005c46d1e900	Davis	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/Davis									
2	OS	a61a04d3dbc06b6e5ae0b110b74cf264	DumontDUrville	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/DumontDUrville									
2	OS	b4afd2c75b40333ed131c2a09964a665	Mawson	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/Mawson									
2	OS	ea22795ffb01d236420d133c2c0e374b	McMurdo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/McMurdo									
2	OS	74252c349649a70237d302bf234266cd	Palmer	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/Palmer									
2	OS	24a43e43955b8e0c4cdf911613a08bc2	Rothera	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/Rothera									
2	OS	ea22795ffb01d236420d133c2c0e374b	South_Pole	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/South_Pole									
2	OS	5ea2662bf9da256e6c25d9d53a22aabf	Syowa	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/Syowa									
2	OS	a4175484f9957947ca47db3a3895fdc2	Vostok	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Antarctica/Vostok									
2	OS	fd888c3218f34e71dc57221143d44ccb	Longyearbyen	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Arctic/Longyearbyen									
2	OS	e45ce4fd28f793ffffc95c7de79e770e	Aden	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Aden									
2	OS	8efd7769bc41484611c77919fd8ab1b4	Almaty	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Almaty									
2	OS	d72f3e9e121164594dbb3d6652b80505	Amman	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Amman									
2	OS	7b3ef232f15fb07cebe16a07a9b6ebe6	Anadyr	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Anadyr									
2	OS	e03a57052925b41e0bb8e079f0082160	Aqtau	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Aqtau									
2	OS	508dca41f406a2f173d5b754e4ebcc6d	Aqtobe	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Aqtobe									
2	OS	46862b46efd2727c2f7fec77c136898f	Ashgabat	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Ashgabat									
2	OS	46862b46efd2727c2f7fec77c136898f	Ashkhabad	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Ashkhabad									
2	OS	878f93457b7af3c845df45a912c6fd0d	Baghdad	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Baghdad									
2	OS	7ddf8abb9dc96b10dd122c1b66d01055	Bahrain	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Bahrain									
2	OS	28831f29bb8e69feda042cc2233a4630	Baku	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Baku									
2	OS	4a296953fb56070ac1968ab136c78e99	Bangkok	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Bangkok									
2	OS	d1164209c41866e990f71f4dbf775208	Beirut	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Beirut									
2	OS	683d71249beb08c7e04f183575579668	Bishkek	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Bishkek									
2	OS	fc62f2d94fcfb0909ff156e2174d3092	Brunei	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Brunei									
2	OS	131b24e6ae1aa244bbcfc2c81ef94359	Calcutta	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Calcutta									
2	OS	ffe16bae24ba62dae5cfd2fe6a6ac4c4	Choibalsan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Choibalsan									
2	OS	147e5196986a7e66ab8c391fb421cbd5	Chongqing	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Chongqing									
2	OS	147e5196986a7e66ab8c391fb421cbd5	Chungking	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Chungking									
2	OS	5d8d63301ae6ac71049561623d19fc43	Colombo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Colombo									
2	OS	d8bd72cd4481d2cbfd4e964d493a59a1	Dacca	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Dacca									
2	OS	80e524b535492d542e3e4e09dd3daaec	Damascus	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Damascus									
2	OS	d8bd72cd4481d2cbfd4e964d493a59a1	Dhaka	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Dhaka									
2	OS	8cd04390bb157c1fff45645be584c74d	Dili	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Dili									
2	OS	06207c7a51fa7d7be81eed23832039f0	Dubai	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Dubai									
2	OS	23b477db0cc84a740431accfc56f0f53	Dushanbe	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Dushanbe									
2	OS	4963bc0d2773ed466c876cdb045e3e83	Gaza	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Gaza									
2	OS	e73f9157c6d6fee815f3ec20d1a320c8	Harbin	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Harbin									
2	OS	5ddad36c73abb0de70185a4e9a7fd2cc	Ho_Chi_Minh	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Ho_Chi_Minh									
2	OS	69576b56ab708dbaeb70a132265f273c	Hong_Kong	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Hong_Kong									
2	OS	c321f0ad4ca9951684bc3cc272722c79	Hovd	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Hovd									
2	OS	e92131416d9a26ca466c88ecc0d0bb22	Irkutsk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Irkutsk									
2	OS	1174fc7301b9e2288760a194d868fa34	Istanbul	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Istanbul									
2	OS	e779165b2d5b6adb7fb680025b9c128f	Jakarta	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Jakarta									
2	OS	95e467f1529a3bdeeed9f28b2f94a1b4	Jayapura	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Jayapura									
2	OS	1d1a039291c44cc0f87f392aa33f0821	Jerusalem	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Jerusalem									
2	OS	468adadd1ad58f27408f74ea42bd0bbd	Kabul	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Kabul									
2	OS	0ad5098ff1690a589a563d0c3594b4f9	Kamchatka	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Kamchatka									
2	OS	81de9f2ef3c59d852ac1f5a91f090986	Karachi	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Karachi									
2	OS	e1d19e33a6572dc19d93168398412656	Kashgar	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Kashgar									
2	OS	51bd74fc2097ed0e3a843f8ea89d8106	Kathmandu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Kathmandu									
2	OS	51bd74fc2097ed0e3a843f8ea89d8106	Katmandu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Katmandu									
2	OS	131b24e6ae1aa244bbcfc2c81ef94359	Kolkata	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Kolkata									
2	OS	90ffefeeb16b04f37d3c4cc340223643	Krasnoyarsk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Krasnoyarsk									
2	OS	e928395ddd4f0a0febf75cec8d8c1d77	Kuala_Lumpur	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Kuala_Lumpur									
2	OS	34541d1bc4cc6934a777916c45cb275e	Kuching	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Kuching									
2	OS	ff78a86473d2feb35a3155a7a7191f25	Kuwait	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Kuwait									
2	OS	c5fe6e2975c4a8ad1be4c7f8f1924303	Macao	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Macao									
2	OS	c5fe6e2975c4a8ad1be4c7f8f1924303	Macau	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Macau									
2	OS	a418faef6059b788c56a2ad37cf42c83	Magadan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Magadan									
2	OS	d88e2ea86448539b26cbb17781092fd2	Makassar	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Makassar									
2	OS	fa08b8c70df808269dfc40c6391fa47f	Manila	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Manila									
2	OS	c9e99d8184b54d6e50c21e78e9e7499f	Muscat	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Muscat									
2	OS	42135bbd5f922141b0bdf101c71cd82e	Nicosia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Nicosia									
2	OS	924b06c218d919282501f338778aa495	Novosibirsk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Novosibirsk									
2	OS	69c30f6d4bc7d7d1a4e1d93f793739ad	Omsk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Omsk									
2	OS	45491c2985181e385de663faa14ffc7f	Oral	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Oral									

2	OS	dd3412f536357a288cdb1fd4524ac8a1	Phnom_Penh	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Phnom_Penh									
2	OS	b398ca80421d63ed4f96c6281c1b046f	Pontianak	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Pontianak									
2	OS	e9e43558ead9a7379c3796cb80bf97f9	Pyongyang	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Pyongyang									
2	OS	bde939d0b44ac698afc4792e8646471d	Qatar	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Qatar									
2	OS	704cf7c1767c96093124d738fb3ecf37	Qyzylorda	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Qyzylorda									
2	OS	fbfc48ee066c1205d7fec64a3fc05706	Rangoon	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Rangoon									
2	OS	01237c88153dd1201b7d6fb9ddd6a74b	Riyadh	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Riyadh									
2	OS	bdc0e2897ff8843a59b667d240f9efad	Riyadh87	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Riyadh87									
2	OS	ec2aed044da28c4b4e1ebc0a21f62889	Riyadh88	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Riyadh88									
2	OS	411fcf430fc1876f7dc7f25b9e2a9fd1	Riyadh89	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Riyadh89									
2	OS	5ddad36c73abb0de70185a4e9a7fd2cc	Saigon	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Saigon									
2	OS	7c24cb5de9f63adf90bac60ca4e81daa	Sakhalin	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Sakhalin									
2	OS	0012672d12a5b18167941114494bf38a	Samarkand	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Samarkand									
2	OS	49b064a11f619899d63d1cc455406995	Seoul	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Seoul									
2	OS	7f6b70f5f9d91b58b5d56c6a35faefb2	Shanghai	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Shanghai									
2	OS	027f249b61cff3e7f808a677644eacac	Singapore	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Singapore									
2	OS	2cb7700780c8b4963f72c9dab967cffa	Taipei	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Taipei									
2	OS	217a3d32b49ca0d36144bd3e975d251f	Tashkent	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Tashkent									
2	OS	60b16fc587db5d7cb9ac3cc47ee56376	Tbilisi	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Tbilisi									
2	OS	f9b1a4c19974edf6740be7614b4415d2	Tehran	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Tehran									
2	OS	1d1a039291c44cc0f87f392aa33f0821	Tel_Aviv	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Tel_Aviv									
2	OS	15345e63780afd3cbf0e0e6a8fa75313	Thimbu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Thimbu									
2	OS	15345e63780afd3cbf0e0e6a8fa75313	Thimphu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Thimphu									
2	OS	8470e9e89799169fde673f92103a72f8	Tokyo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Tokyo									
2	OS	d88e2ea86448539b26cbb17781092fd2	Ujung_Pandang	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Ujung_Pandang									
2	OS	6e3d491024af66efa3d1dcaff463f37c	Ulaanbaatar	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Ulaanbaatar									
2	OS	6e3d491024af66efa3d1dcaff463f37c	Ulan_Bator	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Ulan_Bator									
2	OS	b1fc15c3615e1df5a3472b4702c18df2	Urumqi	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Urumqi									
2	OS	05c1faba0d36e75e8ceaa6ad9c1105a1	Vientiane	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Vientiane									
2	OS	e4ecdaf53c898830e2bde1827568d535	Vladivostok	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Vladivostok									
2	OS	197dcf1878f925bb8af7a49b1007d1f4	Yakutsk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Yakutsk									
2	OS	0e03d10cad1bf5bbe85ce337ff191cfd	Yekaterinburg	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Yekaterinburg									
2	OS	701946c555d5e8de7e986330ae19b335	Yerevan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Asia/Yerevan									
2	OS	6d7ac5601a8e9f81e8cfc2bb3fc7f589	Azores	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Azores									
2	OS	3814dc7cb2acec956b76ae3ebce6c0c1	Bermuda	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Bermuda									
2	OS	b220ac66610da4a4d49dc58b2c81b85b	Canary	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Canary									
2	OS	5df95b7e8875a807f41e34a724671404	Cape_Verde	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Cape_Verde									
2	OS	493dc00cdad9f8f02daa6be311a13a27	Faeroe	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Faeroe									
2	OS	493dc00cdad9f8f02daa6be311a13a27	Faroe	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Faroe									
2	OS	fd888c3218f34e71dc57221143d44ccb	Jan_Mayen	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Jan_Mayen									
2	OS	fbc5061ab858c52b7c7da93508cd5c0f	Madeira	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Madeira									
2	OS	7e6686b4e68a68f5088d7b6784598dc6	Reykjavik	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Reykjavik									
2	OS	c03bfc048d3957a919fe34ea18b85254	South_Georgia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/South_Georgia									
2	OS	320a737880759fee2d65268af0c38986	St_Helena	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/St_Helena									
2	OS	a6cc1505807e094e9f2cf9e4bf959ce2	Stanley	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Atlantic/Stanley									
2	OS	e3d6afabf7acbedbeecd8aa3ea4e4e42	ACT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/ACT									
2	OS	2ec46d48ad3e92ee00e128db7a42724f	Adelaide	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Adelaide									
2	OS	eced5af13d64a6fab60e1826e75f62f4	Brisbane	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Brisbane									
2	OS	dcb828bbc651d1e43a49e9408678a0d3	Broken_Hill	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Broken_Hill									
2	OS	e3d6afabf7acbedbeecd8aa3ea4e4e42	Canberra	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Canberra									
2	OS	f751edc917c666755544b1c9e7787aa8	Currie	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Currie									
2	OS	c8fc212be11708b7ca96df5aa7c86a45	Darwin	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Darwin									
2	OS	48dd9e3a6d2edc6ce9d4050a9ba99ea9	Eucla	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Eucla									
2	OS	4b60a8a8fe6304a1f73fb9c9ba311bd5	Hobart	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Hobart									
2	OS	3d7fb1ef30f8854e14ab405882419646	LHI	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/LHI									
2	OS	a88a3d08c4635457f1714eaadc2906bd	Lindeman	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Lindeman									
2	OS	3d7fb1ef30f8854e14ab405882419646	Lord_Howe	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Lord_Howe									
2	OS	8980cf81d394b7172dd599599e656302	Melbourne	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Melbourne									
2	OS	e3d6afabf7acbedbeecd8aa3ea4e4e42	NSW	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/NSW									
2	OS	c8fc212be11708b7ca96df5aa7c86a45	North	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/North									
2	OS	a19d7dace613ccebb9ee1554997a0bae	Perth	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Perth									
2	OS	eced5af13d64a6fab60e1826e75f62f4	Queensland	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Queensland									
2	OS	2ec46d48ad3e92ee00e128db7a42724f	South	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/South									
2	OS	e3d6afabf7acbedbeecd8aa3ea4e4e42	Sydney	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Sydney									
2	OS	4b60a8a8fe6304a1f73fb9c9ba311bd5	Tasmania	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Tasmania									
2	OS	8980cf81d394b7172dd599599e656302	Victoria	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Victoria									
2	OS	a19d7dace613ccebb9ee1554997a0bae	West	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/West									
2	OS	dcb828bbc651d1e43a49e9408678a0d3	Yancowinna	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Australia/Yancowinna									
2	OS	0e57862dbc12163ef9f2788d13b8d5ea	Acre	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Brazil/Acre									
2	OS	b3763578fe1f4575cb65f33c2d3d1c5a	DeNoronha	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Brazil/DeNoronha									
2	OS	9d1d4990eb40b53bf1b9688caf690e9d	East	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Brazil/East									
2	OS	24210f1a2615a304bf58b9f07f4f326a	West	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Brazil/West									
2	OS	a3983ad699f80b8c1be5f7e29718368d	CET	/Volumes/Data/stash/share.R9s6NA/zoneinfo/CET									

2	OS	334a7aea822a5ca567f6f4a8d921c11c	CST6CDT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/CST6CDT									
2	OS	0446ea93da671cbd751933bfd10c7088	Atlantic	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/Atlantic									
2	OS	97d2e564f4bf3855f1d52c2f738358fc	Central	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/Central									
2	OS	988a01f8ecfaf4c6e91d3315b86c52cf	East-Saskatchewan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/East-Saskatchewan									
2	OS	82980b1345aab5a97d90307edfefb6da	Eastern	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/Eastern									
2	OS	4f1f996bf8a059b5c0f6caa73c0fe7db	Mountain	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/Mountain									
2	OS	1544a77fe6bcf16d429fcf0d6b82f767	Newfoundland	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/Newfoundland									
2	OS	ed5406f379fa648906bc366499ae087d	Pacific	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/Pacific									
2	OS	988a01f8ecfaf4c6e91d3315b86c52cf	Saskatchewan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/Saskatchewan									
2	OS	1f6419c3be16190917b018b8a61db105	Yukon	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Canada/Yukon									
2	OS	f9664d412a224a98c79c49e04c7e0281	Continental	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Chile/Continental									
2	OS	ccd58a41f9c3a19d7d9887d4e9022025	EasterIsland	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Chile/EasterIsland									
2	OS	6ea65224f35ad74ea50f56683068dba2	Cuba	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Cuba									
2	OS	fc29c7035a9de76a845bfd1af5bcffea	EET	/Volumes/Data/stash/share.R9s6NA/zoneinfo/EET									
2	OS	6fac20ee52a95b38ad0e1657f77aa4c4	EST	/Volumes/Data/stash/share.R9s6NA/zoneinfo/EST									
2	OS	87a75432ef636782207fa06d603585c0	EST5EDT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/EST5EDT									
2	OS	c79cfc2f93856b816adb63b52a2e8568	Egypt	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Egypt									
2	OS	1f0a6164226fe99d3297d897c0a81c0f	Eire	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Eire									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	GMT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	GMT+0	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+0									
2	OS	36c4ce7f05984aa56c34510ca2e0b36c	GMT+1	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+1									
2	OS	bca03c74466be764cbf63c27a79c0eea	GMT+10	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+10									
2	OS	2b3f6bb27ce40d88f4cf142ba8c89cdf	GMT+11	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+11									
2	OS	e8550a1acda4e26d24667cc59e4bbfbf	GMT+12	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+12									
2	OS	a90e1ace711116799c07b8beb0fb64ba	GMT+2	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+2									
2	OS	6fb2a054de96ce3d9ab54754a7ddc051	GMT+3	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+3									
2	OS	072f58e25eea1ccb0e3353ea68971378	GMT+4	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+4									
2	OS	0df2ef0f06aa7c2a1dbc3b13f4606c94	GMT+5	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+5									
2	OS	db5b0cea31c24f9599b452614ca58c43	GMT+6	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+6									
2	OS	1f690da32039499538c01e15427020f1	GMT+7	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+7									
2	OS	c2465b173a957e0b051a05494ce957c1	GMT+8	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+8									
2	OS	0852176aaf1e4f4c360fd80ea28fd102	GMT+9	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT+9									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	GMT-0	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-0									
2	OS	e23e54559a8c08a2b7f652e68e687269	GMT-1	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-1									
2	OS	9dd5d6915f94d527bbc6672214d17623	GMT-10	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-10									
2	OS	5e491446224f9c6a2a99cfe56f5b46bf	GMT-11	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-11									
2	OS	bff76629619f67b913a69788e84e542f	GMT-12	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-12									
2	OS	e5f0d6981aff6c0ccc14e4442cb71506	GMT-13	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-13									
2	OS	fc3753fef9fe1eab85c69eda08e9318e	GMT-14	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-14									
2	OS	fa2e1ea8e2e797aa74c676d9f9373065	GMT-2	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-2									
2	OS	789ea340de290609b9fd8439c46cc43a	GMT-3	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-3									
2	OS	c57e526d30986bdd1590f44d4ec25f5c	GMT-4	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-4									
2	OS	b0cda2675d03846dcbfd7ac8aae0928f	GMT-5	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-5									
2	OS	8c79960d1267e617ab6cbed3d682479b	GMT-6	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-6									
2	OS	1d93177b840be09f0775123d323b370f	GMT-7	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-7									
2	OS	3403d59765c40442c6db0a0a6b7c82b3	GMT-8	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-8									
2	OS	0adf4041fce6f4d15dceee7353203588	GMT-9	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT-9									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	GMT0	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/GMT0									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	Greenwich	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/Greenwich									
2	OS	58509d20328588b047b8af8673e9c3ad	UCT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/UCT									
2	OS	9bd0933136f45090855cdd09c1be16c6	UTC	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/UTC									
2	OS	9bd0933136f45090855cdd09c1be16c6	Universal	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/Universal									
2	OS	9bd0933136f45090855cdd09c1be16c6	Zulu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Etc/Zulu									
2	OS	312cff0c326c71b2f628fd631a5978b2	Amsterdam	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Amsterdam									
2	OS	e32686836465e564be49d040591b070d	Andorra	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Andorra									
2	OS	7ca967dbcaaddccf72c764f0934dec58	Athens	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Athens									
2	OS	4c9f9c5c5f86bcc5465c08831ef59e75	Belfast	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Belfast									
2	OS	11088657fae25cf9e0bed960f07b8388	Belgrade	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Belgrade									
2	OS	6086905ed1306caeb6ee62148469312f	Berlin	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Berlin									
2	OS	b1ba486a583fb73f1306d1e6cf7366e6	Bratislava	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Bratislava									
2	OS	f83bbf5df0b4046d357eed0c782eed2a	Brussels	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Brussels									
2	OS	13a41b93ea77857328185171c58313f2	Bucharest	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Bucharest									
2	OS	6c2fadbe34c145185dc255532917b401	Budapest	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Budapest									
2	OS	8d6a9e7007fe2a32165d9f5a5c918c6e	Chisinau	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Chisinau									
2	OS	8efc72daacd8884fa3c64cedf19cd8ee	Copenhagen	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Copenhagen									
2	OS	1f0a6164226fe99d3297d897c0a81c0f	Dublin	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Dublin									
2	OS	ea65813d9e8dd6f89b6e7f45af736e2c	Gibraltar	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Gibraltar									
2	OS	4c9f9c5c5f86bcc5465c08831ef59e75	Guernsey	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Guernsey									
2	OS	db64f0bedf936d442466acffa382cd28	Helsinki	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Helsinki									
2	OS	4c9f9c5c5f86bcc5465c08831ef59e75	Isle_of_Man	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Isle_of_Man									
2	OS	1174fc7301b9e2288760a194d868fa34	Istanbul	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Istanbul									
2	OS	4c9f9c5c5f86bcc5465c08831ef59e75	Jersey	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Jersey									
2	OS	8875762a2881a809475a1ef436df3534	Kaliningrad	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Kaliningrad									

2	OS	8c27616184882f372dfda7aad2c00fcb	Kiev	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Kiev									
2	OS	36c3c9717b29e9945712a12b80967a72	Lisbon	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Lisbon									
2	OS	11088657fae25cf9e0bed960f07b8388	Ljubljana	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Ljubljana									
2	OS	4c9f9c5c5f86bcc5465c08831ef59e75	London	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/London									
2	OS	80b565d3b24ac95c91d7a91a304a8956	Luxembourg	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Luxembourg									
2	OS	b72dc2756c0db29b6c98d00fa3a05ef6	Madrid	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Madrid									
2	OS	d9169baa1c86f4b50ae89fc9ee66d865	Malta	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Malta									
2	OS	db64f0bedf936d442466acffa382cd28	Mariehamn	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Mariehamn									
2	OS	2c8bf97a06c3a5efb18e053407255554	Minsk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Minsk									
2	OS	1a41ac975eef6a17a3e03ac85f8be9f1	Monaco	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Monaco									
2	OS	c4f28389191f01c90e1e748ab4960350	Moscow	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Moscow									
2	OS	42135bbd5f922141b0bdf101c71cd82e	Nicosia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Nicosia									
2	OS	fd888c3218f34e71dc57221143d44ccb	Oslo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Oslo									
2	OS	6a39c7fb5d84f0408fce26b44268f56a	Paris	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Paris									
2	OS	11088657fae25cf9e0bed960f07b8388	Podgorica	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Podgorica									
2	OS	b1ba486a583fb73f1306d1e6cf7366e6	Prague	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Prague									
2	OS	581dbed5d25edc11160d734a48c94182	Riga	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Riga									
2	OS	a3e8171971ae213aa3e656712f9bd24e	Rome	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Rome									
2	OS	3aa9d48490198bd8b1c98aac45b0ee2a	Samara	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Samara									
2	OS	a3e8171971ae213aa3e656712f9bd24e	San_Marino	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/San_Marino									
2	OS	11088657fae25cf9e0bed960f07b8388	Sarajevo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Sarajevo									
2	OS	4b55740a09f827dcb9e7fcbd914f6b3d	Simferopol	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Simferopol									
2	OS	11088657fae25cf9e0bed960f07b8388	Skopje	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Skopje									
2	OS	cdf3a043b9d53ac26c0ed0c16483a12e	Sofia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Sofia									
2	OS	a130ac91586eda266c961441c78d7715	Stockholm	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Stockholm									
2	OS	203136a5c46f611029a711e20c4a4011	Tallinn	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Tallinn									
2	OS	1cd0f0ee521ff80127e1199c0a06c752	Tirane	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Tirane									
2	OS	8d6a9e7007fe2a32165d9f5a5c918c6e	Tiraspol	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Tiraspol									
2	OS	af884e5fce47769448a72600ff7fb7e2	Uzhgorod	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Uzhgorod									
2	OS	626060e7c35fdffdcf59e50eb8983515	Vaduz	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Vaduz									
2	OS	a3e8171971ae213aa3e656712f9bd24e	Vatican	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Vatican									
2	OS	fea87abd889dfba16914b317ec5c471a	Vienna	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Vienna									
2	OS	c9ec8b06246cdcb58e60d1bb80704255	Vilnius	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Vilnius									
2	OS	af40b5c3842338d368d60c01e72e80aa	Volgograd	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Volgograd									
2	OS	2461b2a3b6203f194e0709a9f828163d	Warsaw	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Warsaw									
2	OS	11088657fae25cf9e0bed960f07b8388	Zagreb	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Zagreb									
2	OS	930cfc6e6b2191161aa582cac7120010	Zaporozhye	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Zaporozhye									
2	OS	a233078bf958f497a6ec7c52a39e3f67	Zurich	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Europe/Zurich									
2	OS	e8fb7d33b7ba858af40f322da1b72a8b	Factory	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Factory									
2	OS	4c9f9c5c5f86bcc5465c08831ef59e75	GB	/Volumes/Data/stash/share.R9s6NA/zoneinfo/GB									
2	OS	4c9f9c5c5f86bcc5465c08831ef59e75	GB-Eire	/Volumes/Data/stash/share.R9s6NA/zoneinfo/GB-Eire									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	GMT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/GMT									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	GMT+0	/Volumes/Data/stash/share.R9s6NA/zoneinfo/GMT+0									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	GMT-0	/Volumes/Data/stash/share.R9s6NA/zoneinfo/GMT-0									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	GMT0	/Volumes/Data/stash/share.R9s6NA/zoneinfo/GMT0									
2	OS	4ae21abf65ef26d2d732662e44f8fbbe	Greenwich	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Greenwich									
2	OS	f8396ef2ee186ffeedea71dea3d365c9	HST	/Volumes/Data/stash/share.R9s6NA/zoneinfo/HST									
2	OS	69576b56ab708dbaeb70a132265f273c	Hongkong	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Hongkong									
2	OS	7e6686b4e68a68f5088d7b6784598dc6	Iceland	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Iceland									
2	OS	fd4793a674181b81617ec423b4abc471	Antananarivo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Antananarivo									
2	OS	08e4ac1daa8f21dc146500960c51c9ac	Chagos	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Chagos									
2	OS	7ba142accad2cc3cb00c711191918317	Christmas	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Christmas									
2	OS	ececabcfda16ade35cbcb38ebe7f3715	Cocos	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Cocos									
2	OS	ff05e5859f5d9f3d557d68707e41379e	Comoro	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Comoro									
2	OS	86d5bbf944ef1451d930999bf33a3429	Kerguelen	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Kerguelen									
2	OS	f33a8cc5b19c55dded9e98f6b7befe94	Mahe	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Mahe									
2	OS	792f3b4fce39b0f9003987f976b6a9bb	Maldives	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Maldives									
2	OS	a9844964e39153626e9b4c29dbae66f9	Mauritius	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Mauritius									
2	OS	099f0cdf23789a72e314617ab5a6b84e	Mayotte	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Mayotte									
2	OS	cf00aa3f17e21108f61d2467c6813b6e	Reunion	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Indian/Reunion									
2	OS	f9b1a4c19974edf6740be7614b4415d2	Iran	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Iran									
2	OS	1d1a039291c44cc0f87f392aa33f0821	Israel	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Israel									
2	OS	598c3e5fa32cfd9ff03842dc3fc937e1	Jamaica	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Jamaica									
2	OS	8470e9e89799169fde673f92103a72f8	Japan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Japan									
2	OS	678f42d72b213b0ac6bb666a77430e75	Kwajalein	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Kwajalein									
2	OS	18167cde0c74d2c43a91e5945eb83548	Libya	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Libya									
2	OS	4f42f5c0105c7b9073479a0a07194833	MET	/Volumes/Data/stash/share.R9s6NA/zoneinfo/MET									
2	OS	33994f847c1f4e85e38f6fd00b5b3c27	MST	/Volumes/Data/stash/share.R9s6NA/zoneinfo/MST									
2	OS	f132a4a8ad5ea9d39db1fd3eede4b2ae	MST7MDT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/MST7MDT									
2	OS	64eb211e4362ad4550c535eb88676f6b	BajaNorte	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Mexico/BajaNorte									
2	OS	aebae9a378965894a3c40cf4e1a3c1c2	BajaSur	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Mexico/BajaSur									
2	OS	a6d2cd65c99b1991c70925b0146001e7	General	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Mexico/General									
2	OS	bdc0e2897ff8843a59b667d240f9efad	Riyadh87	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Mideast/Riyadh87									

2	OS	ec2aed044da28c4b4e1ebc0a21f62889	Riyadh88	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Mideast/Riyadh88									
2	OS	411fcf430fc1876f7dc7f25b9e2a9fd1	Riyadh89	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Mideast/Riyadh89									
2	OS	28e3497aa0acae03edee06ed4d7dc72b	NZ	/Volumes/Data/stash/share.R9s6NA/zoneinfo/NZ									
2	OS	0b2a751ca575143fc14abb21ea3454ae	NZ-CHAT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/NZ-CHAT									
2	OS	db1d61b98712f8923bbb9d9708625432	Navajo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Navajo									
2	OS	7f6b70f5f9d91b58b5d56c6a35faefb2	PRC	/Volumes/Data/stash/share.R9s6NA/zoneinfo/PRC									
2	OS	b04417d20583bdc21e0e6f27f48170fe	PST8PDT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/PST8PDT									
2	OS	908765c9c1a082d518c528a7a2e99bea	Apia	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Apia									
2	OS	28e3497aa0acae03edee06ed4d7dc72b	Auckland	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Auckland									
2	OS	0b2a751ca575143fc14abb21ea3454ae	Chatham	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Chatham									
2	OS	ccd58a41f9c3a19d7d9887d4e9022025	Easter	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Easter									
2	OS	a46dfbbf2699ea24c2f2a24591af927c	Efate	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Efate									
2	OS	cf8b8ee77acd84e79cb663396b72b1f5	Enderbury	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Enderbury									
2	OS	ac65a8fc478c8b251e565dfeef48a165	Fakaofo	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Fakaofo									
2	OS	02e000a2c60e2f218005fc881d914b04	Fiji	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Fiji									
2	OS	b7ec1a9e76e70712de3467696dab9827	Funafuti	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Funafuti									
2	OS	4d1e72203c65e5286d73247fd4b770e5	Galapagos	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Galapagos									
2	OS	2336932dd6d10aae3279a57c409d80d9	Gambier	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Gambier									
2	OS	e9f45cd19181a0b9fd925eb76d3b68fe	Guadalcanal	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Guadalcanal									
2	OS	781c64db5da51ed2a8af9b0288a81d71	Guam	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Guam									
2	OS	ef02ff0df83fbe3094052fda06e2eff1	Honolulu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Honolulu									
2	OS	f8396ef2ee186ffeedea71dea3d365c9	Johnston	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Johnston									
2	OS	2f2b4906aefd76376a5a74c716e47e96	Kiritimati	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Kiritimati									
2	OS	bd4a00e972fb4129e8da5c9d276fcd6d	Kosrae	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Kosrae									
2	OS	678f42d72b213b0ac6bb666a77430e75	Kwajalein	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Kwajalein									
2	OS	175961b6f4197f574696de9efe66b151	Majuro	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Majuro									
2	OS	40cab80dea39f28162c605450d2c20f9	Marquesas	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Marquesas									
2	OS	7193186ca0540dd701900378f1579d40	Midway	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Midway									
2	OS	48114cd7aecba8fd6579733621a8efa6	Nauru	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Nauru									
2	OS	a33ec92471e2c5be3e4de7fa3f91a8ac	Niue	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Niue									
2	OS	8b4fb04f78a766ff9279fb6167a86276	Norfolk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Norfolk									
2	OS	3a046d3b7e690b85b8fb37438e792767	Noumea	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Noumea									
2	OS	eeb45f6c2811b0f031ce72edbb432451	Pago_Pago	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Pago_Pago									
2	OS	439646ae0d40eb4f79e4fb862f5c8235	Palau	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Palau									
2	OS	dcd1092bffe3f9b8a6ac33af5d123980	Pitcairn	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Pitcairn									
2	OS	76a122df837ebaf51f0534a968234c65	Ponape	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Ponape									
2	OS	5453a9b23a53d9dbc4fbafbfc00a5b66	Port_Moresby	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Port_Moresby									
2	OS	90a2152b7ee36632918fe557392c3b5a	Rarotonga	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Rarotonga									
2	OS	dbb8906b85fe8771242d2039633fa2c9	Saipan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Saipan									
2	OS	eeb45f6c2811b0f031ce72edbb432451	Samoa	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Samoa									
2	OS	55763a3e3be9d03118f10afc4817dddc	Tahiti	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Tahiti									
2	OS	bfd34314baf263e2c5b250cc63a71eea	Tarawa	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Tarawa									
2	OS	8e5b70cc664bfdbfa2144a8303636225	Tongatapu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Tongatapu									
2	OS	4acb57708aa158ffcba514c33051fb90	Truk	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Truk									
2	OS	045bd8ec51bf5413356d28ce81400e2f	Wake	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Wake									
2	OS	d1274e9c574383efa60311ca942938e3	Wallis	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Wallis									
2	OS	4acb57708aa158ffcba514c33051fb90	Yap	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Pacific/Yap									
2	OS	2461b2a3b6203f194e0709a9f828163d	Poland	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Poland									
2	OS	36c3c9717b29e9945712a12b80967a72	Portugal	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Portugal									
2	OS	2cb7700780c8b4963f72c9dab967cffa	ROC	/Volumes/Data/stash/share.R9s6NA/zoneinfo/ROC									
2	OS	49b064a11f619899d63d1cc455406995	ROK	/Volumes/Data/stash/share.R9s6NA/zoneinfo/ROK									
2	OS	027f249b61cff3e7f808a677644eacac	Singapore	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Singapore									
2	OS	1174fc7301b9e2288760a194d868fa34	Turkey	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Turkey									
2	OS	58509d20328588b047b8af8673e9c3ad	UCT	/Volumes/Data/stash/share.R9s6NA/zoneinfo/UCT									
2	OS	ebc2ed4fcb5c9c2dee6b8ef4fe2e1cd9	Alaska	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Alaska									
2	OS	6fa956ed6227abd78894a642bd07e359	Aleutian	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Aleutian									
2	OS	3d786c31307428005972ee5b6f2a3659	Arizona	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Arizona									
2	OS	3fa8f0dc6fa2ab843dfa3dc1c0a0f72a	Central	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Central									
2	OS	01f76c02facbee6cba7246bd88d07a59	East-Indiana	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/East-Indiana									
2	OS	3cf0ccc7d6b240390188367933c9cd90	Eastern	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Eastern									
2	OS	ef02ff0df83fbe3094052fda06e2eff1	Hawaii	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Hawaii									
2	OS	9b6c9c30d9ac3e7709bc5d42867b2f06	Indiana-Starke	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Indiana-Starke									
2	OS	8742f5ca104dd4330d947a86efce1a6b	Michigan	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Michigan									
2	OS	db1d61b98712f8923bbb9d9708625432	Mountain	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Mountain									
2	OS	ad7be76a1d7216104d9004a73e200efc	Pacific	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Pacific									
2	OS	eeb45f6c2811b0f031ce72edbb432451	Samoa	/Volumes/Data/stash/share.R9s6NA/zoneinfo/US/Samoa									
2	OS	9bd0933136f45090855cdd09c1be16c6	UTC	/Volumes/Data/stash/share.R9s6NA/zoneinfo/UTC									
2	OS	9bd0933136f45090855cdd09c1be16c6	Universal	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Universal									
2	OS	c4f28389191f01c90e1e748ab4960350	W-SU	/Volumes/Data/stash/share.R9s6NA/zoneinfo/W-SU									
2	OS	67057dba8db072f6d35a232bc314e9c6	WET	/Volumes/Data/stash/share.R9s6NA/zoneinfo/WET									
2	OS	9bd0933136f45090855cdd09c1be16c6	Zulu	/Volumes/Data/stash/share.R9s6NA/zoneinfo/Zulu									
2	OS	31555a01e516b8a6fbac7a0bd8009914	iso3166.tab	/Volumes/Data/stash/share.R9s6NA/zoneinfo/iso3166.tab									
2	OS	3cf0ccc7d6b240390188367933c9cd90	posixrules	/Volumes/Data/stash/share.R9s6NA/zoneinfo/posixrules									

2	OS	b35b4b1efbef47594736146e1adb7796	zone.tab	/Volumes/Data/stash/share.R9s6NA/zoneinfo/zone.tab									
2	OS	d41d8cd98f00b204e9800998ecf8427e	BackupRunning	/Volumes/Data/tmp/BackupRunning	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	d41d8cd98f00b204e9800998ecf8427e	DAAccountsLoading.lock	/Volumes/Data/tmp/DAAccountsLoading.lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	d41d8cd98f00b204e9800998ecf8427e	OTASyncRunning.lock	/Volumes/Data/tmp/OTASyncRunning.lock	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	OS	d41d8cd98f00b204e9800998ecf8427e	com.apple.Bookmarks.lock	/Volumes/Data/tmp/com.apple.Bookmarks.lock	Y	Y	Y	Y	Y	Y	Y	Y	Y

Appendix B - Extraction Log
MD5

	DD (Jailbroken)			iTunes Backup		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	12963			343		
DD (Jailbroken)				247	96	72.01%
iTunes Backup	269	12694	2.08%			
iTunes Backup (Jailbroken)	268	12695	2.07%	333	10	97.08%
Device Seizure	178	12785	1.37%	213	130	62.10%
iPhone Explorer	555	12408	4.28%	10	333	2.92%
MobileSyncBrowser	198	12765	1.53%	256	87	74.64%
Mobilyze	269	12694	2.08%	340	3	99.13%
Mobilyze (Jailbroken)	268	12695	2.07%	333	10	97.08%
Oxygen Forensics	797	12166	6.15%	340	3	99.13%
Oxygen Forensics (Jailbroken)	796	12167	6.14%	333	10	97.08%

	iTunes Backup (Jailbroken)			Device Seizure		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	343			549		
DD (Jailbroken)	246	97	71.72%	157	392	28.60%
iTunes Backup	333	10	97.08%	214	335	38.98%
iTunes Backup (Jailbroken)				211	338	38.43%
Device Seizure	210	133	61.22%			
iPhone Explorer	10	333	2.92%	7	542	1.28%
MobileSyncBrowser	246	97	71.72%	157	392	28.60%
Mobilyze	334	9	97.38%	214	335	38.98%
Mobilyze (Jailbroken)	340	3	99.13%	211	338	38.43%
Oxygen Forensics	334	9	97.38%	214	335	38.98%
Oxygen Forensics (Jailbroken)	340	3	99.13%	211	338	38.43%

	iPhone Explorer			MobileSyncBrowser		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	560			336		
DD (Jailbroken)	535	25	95.54%	174	162	51.79%
iTunes Backup	13	547	2.32%	254	82	75.60%
iTunes Backup (Jailbroken)	13	547	2.32%	244	92	72.62%
Device Seizure	9	551	1.61%	156	180	46.43%
iPhone Explorer				10	326	2.98%
MobileSyncBrowser	13	547	2.32%			
Mobilyze	13	547	2.32%	251	85	74.70%
Mobilyze (Jailbroken)	13	547	2.32%	244	92	72.62%
Oxygen Forensics	560	0	100.00%	251	85	74.70%
Oxygen Forensics (Jailbroken)	556	4	99.29%	244	92	72.62%

	Mobilyze			Mobilyze (Jailbroken)		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	346			346		
DD (Jailbroken)	247	99	71.39%	246	100	71.10%
iTunes Backup	340	6	98.27%	333	13	96.24%
iTunes Backup (Jailbroken)	334	12	96.53%	340	6	98.27%
Device Seizure	213	133	61.56%	210	136	60.69%
iPhone Explorer	10	336	2.89%	10	336	2.89%
MobileSyncBrowser	253	93	73.12%	246	100	71.10%
Mobilyze				334	12	96.53%
Mobilyze (Jailbroken)	334	12	96.53%			
Oxygen Forensics	341	5	98.55%	333	13	96.24%
Oxygen Forensics (Jailbroken)	333	13	96.24%	341	5	98.55%

	Oxygen Forensics			Oxygen Forensics (Jailbroken)		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	903			903		
DD (Jailbroken)	782	121	86.60%	781	122	86.49%
iTunes Backup	353	550	39.09%	346	557	38.32%
iTunes Backup (Jailbroken)	347	556	38.43%	353	550	39.09%
Device Seizure	222	681	24.58%	219	684	24.25%
iPhone Explorer	570	333	63.12%	566	337	62.68%
MobileSyncBrowser	266	637	29.46%	259	644	28.68%
Mobilyze	354	549	39.20%	346	557	38.32%
Mobilyze (Jailbroken)	346	557	38.32%	354	549	39.20%
Oxygen Forensics				889	14	98.45%
Oxygen Forensics (Jailbroken)	889	14	98.45%			

	Importance Rating 0					
	Total	Percentage Match	Jailbreak	Percentage Match	iPod Music	Percentage Match
	786		237		549	
iTunes Backup	3	0.38%	0	0.00%	3	0.55%
iTunes Backup (Jailbroken)	3	0.38%	0	0.00%	3	0.55%
Device Seizure	1	0.13%	0	0.00%	1	0.18%
iPhone Explorer	531	67.56%	0	0.00%	531	96.72%
MobileSyncBrowser	2	0.25%	0	0.00%	2	0.36%
Mobilyze	2	0.25%	0	0.00%	2	0.36%
Mobilyze (Jailbroken)	2	0.25%	0	0.00%	2	0.36%
Oxygen Forensics	531	67.56%	0	0.00%	531	96.72%
Oxygen Forensics (Jailbroken)	531	67.56%	0	0.00%	531	96.72%

	Importance Rating 1					
	Total	Percentage Match	AppStore	Percentage Match	Apple Apps	Percentage Match
	10873		7491		3382	
iTunes Backup	195	1.79%	195	2.60%	0	0.00%
iTunes Backup (Jailbroken)	195	1.79%	195	2.60%	0	0.00%
Device Seizure	124	1.14%	124	1.66%	0	0.00%
iPhone Explorer	0	0.00%	0	0.00%	0	0.00%
MobileSyncBrowser	124	1.14%	124	1.66%	0	0.00%
Mobilyze	195	1.79%	195	2.60%	0	0.00%
Mobilyze (Jailbroken)	195	1.79%	195	2.60%	0	0.00%
Oxygen Forensics	195	1.79%	195	2.60%	0	0.00%
Oxygen Forensics (Jailbroken)	195	1.79%	195	2.60%	0	0.00%

	Importance Rating 2					
	Total	Percentage Match	AddressBook	Percentage Match	Cache	Percentage Match
	1304		3		144	
iTunes Backup	71	5.44%	0	0.00%	4	2.78%
iTunes Backup (Jailbroken)	70	5.37%	0	0.00%	4	2.78%
Device Seizure	52	3.99%	0	0.00%	4	2.78%
iPhone Explorer	24	1.84%	0	0.00%	3	2.08%
MobileSyncBrowser	71	5.44%	0	0.00%	4	2.78%
Mobilyze	71	5.44%	0	0.00%	4	2.78%
Mobilyze (Jailbroken)	70	5.37%	0	0.00%	4	2.78%
Oxygen Forensics	71	5.44%	0	0.00%	4	2.78%
Oxygen Forensics (Jailbroken)	70	5.37%	0	0.00%	4	2.78%

	Calendar	Percentage Match	Call History	Percentage Match	Camera	Percentage Match
	1		1		1	
iTunes Backup	0	0.00%	0	0.00%	1	100.00%
iTunes Backup (Jailbroken)	0	0.00%	0	0.00%	1	100.00%
Device Seizure	0	0.00%	0	0.00%	0	0.00%
iPhone Explorer	0	0.00%	0	0.00%	1	100.00%
MobileSyncBrowser	0	0.00%	0	0.00%	1	100.00%
Mobilyze	0	0.00%	0	0.00%	1	100.00%
Mobilyze (Jailbroken)	0	0.00%	0	0.00%	1	100.00%
Oxygen Forensics	0	0.00%	0	0.00%	1	100.00%
Oxygen Forensics (Jailbroken)	0	0.00%	0	0.00%	1	100.00%

	Cookies	Percentage Match	Mail	Percentage Match	Maps	Percentage Match
	3		16		2	
iTunes Backup	0	0.00%	1	6.25%	2	100.00%
iTunes Backup (Jailbroken)	0	0.00%	1	6.25%	2	100.00%
Device Seizure	0	0.00%	1	6.25%	1	50.00%
iPhone Explorer	0	0.00%	0	0.00%	0	0.00%
MobileSyncBrowser	0	0.00%	1	6.25%	2	100.00%
Mobilyze	0	0.00%	1	6.25%	2	100.00%
Mobilyze (Jailbroken)	0	0.00%	1	6.25%	2	100.00%
Oxygen Forensics	0	0.00%	1	6.25%	2	100.00%
Oxygen Forensics (Jailbroken)	0	0.00%	1	6.25%	2	100.00%

	Notes	Percentage Match	OS	Percentage Match	Safari	Percentage Match	SMS	Percentage Match
	2		1118		11		2	
iTunes Backup	1	50.00%	56	5.01%	5	45.45%	1	50.00%
iTunes Backup (Jailbroken)	1	50.00%	55	4.92%	5	45.45%	1	50.00%
Device Seizure	1	50.00%	41	3.67%	4	36.36%	0	0.00%
iPhone Explorer	0	0.00%	20	1.79%	0	0.00%	0	0.00%
MobileSyncBrowser	1	50.00%	56	5.01%	5	45.45%	1	50.00%
Mobilyze	1	50.00%	56	5.01%	5	45.45%	1	50.00%
Mobilyze (Jailbroken)	1	50.00%	55	4.92%	5	45.45%	1	50.00%
Oxygen Forensics	1	50.00%	56	5.01%	5	45.45%	1	50.00%
Oxygen Forensics (Jailbroken)	1	50.00%	55	4.92%	5	45.45%	1	50.00%

Appendix B - Extraction Log Files

	DD (Jailbroken)			iTunes Backup		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	12963			343		
DD (Jailbroken)				316	27	92.13%
iTunes Backup	448	12515	3.46%			
iTunes Backup (Jailbroken)	448	12515	3.46%	343	0	100.00%
Device Seizure	0	12963	0.00%	0	343	0.00%
iPhone Explorer	108	12855	0.83%	9	334	2.62%
MobileSyncBrowser	448	12515	3.46%	343	0	100.00%
Mobilyze	448	12515	3.46%	343	0	100.00%
Mobilyze (Jailbroken)	448	12515	3.46%	343	0	100.00%
Oxygen Forensics	482	12481	3.72%	343	0	100.00%
Oxygen Forensics (Jailbroken)	482	12481	3.72%	343	0	100.00%

	iTunes Backup (Jailbroken)			Device Seizure		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	343			549		
DD (Jailbroken)	316	27	92.13%	0	549	0.00%
iTunes Backup	343	0	100.00%	0	549	0.00%
iTunes Backup (Jailbroken)				0	549	0.00%
Device Seizure	0	343	0.00%			
iPhone Explorer	9	334	2.62%	0	549	0.00%
MobileSyncBrowser	343	0	100.00%	0	549	0.00%
Mobilyze	343	0	100.00%	0	549	0.00%
Mobilyze (Jailbroken)	343	0	100.00%	0	549	0.00%
Oxygen Forensics	343	0	100.00%	0	549	0.00%
Oxygen Forensics (Jailbroken)	343	0	100.00%	0	549	0.00%

	iPhone Explorer			MobileSyncBrowser		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	560			336		
DD (Jailbroken)	36	524	6.43%	227	109	67.56%
iTunes Backup	8	552	1.43%	254	82	75.60%
iTunes Backup (Jailbroken)	8	552	1.43%	254	82	75.60%
Device Seizure	0	560	0.00%	0	336	0.00%
iPhone Explorer				9	327	2.68%
MobileSyncBrowser	8	552	1.43%			
Mobilyze	8	552	1.43%	254	82	75.60%
Mobilyze (Jailbroken)	8	552	1.43%	254	82	75.60%
Oxygen Forensics	560	0	100.00%	254	82	75.60%
Oxygen Forensics (Jailbroken)	560	0	100.00%	254	82	75.60%

	Mobilyze			Mobilyze (Jailbroken)		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	346			346		
DD (Jailbroken)	317	29	91.62%	317	29	91.62%
iTunes Backup	344	2	99.42%	344	2	99.42%
iTunes Backup (Jailbroken)	344	2	99.42%	344	2	99.42%
Device Seizure	0	346	0.00%	0	346	0.00%
iPhone Explorer	10	336	2.89%	10	336	2.89%
MobileSyncBrowser	344	2	99.42%	344	2	99.42%
Mobilyze				346	0	100.00%
Mobilyze (Jailbroken)	346	0	100.00%			
Oxygen Forensics	344	2	99.42%	344	2	99.42%
Oxygen Forensics (Jailbroken)	344	2	99.42%	344	2	99.42%

	Oxygen Forensics			Oxygen Forensics (Jailbroken)		
	Total Hashes	Didn't Match	Percentage Match	Total Hashes	Didn't Match	Percentage Match
	903			903		
DD (Jailbroken)	352	551	38.98%	352	551	38.98%
iTunes Backup	351	552	38.87%	351	552	38.87%
iTunes Backup (Jailbroken)	351	552	38.87%	351	552	38.87%
Device Seizure	0	903	0.00%	0	903	0.00%
iPhone Explorer	569	334	63.01%	569	334	63.01%
MobileSyncBrowser	351	552	38.87%	351	552	38.87%
Mobilyze	351	552	38.87%	351	552	38.87%
Mobilyze (Jailbroken)	351	552	38.87%	351	552	38.87%
Oxygen Forensics				903	0	100.00%
Oxygen Forensics (Jailbroken)	903	0	100.00%			

	Importance Rating 0					
	Total	Percentage Match	Jailbreak	Percentage Match	iPod Music	Percentage Match
	786		237		549	
iTunes Backup	5	0.64%	2	0.84%	3	0.55%
iTunes Backup (Jailbroken)	2	0.25%	2	0.84%	0	0.00%
Device Seizure	0	0.00%	0	0.00%	0	0.00%
iPhone Explorer	32	4.07%	1	0.42%	31	5.65%
MobileSyncBrowser	2	0.25%	2	0.84%	0	0.00%
Mobilyze	2	0.25%	2	0.84%	0	0.00%
Mobilyze (Jailbroken)	2	0.25%	2	0.84%	0	0.00%
Oxygen Forensics	33	4.20%	2	0.84%	31	5.65%
Oxygen Forensics (Jailbroken)	33	4.20%	2	0.84%	31	5.65%

	Importance Rating 1					
	Total	Percentage Match	AppStore	Percentage Match	Apple Apps	Percentage Match
	10873		7491		3382	
iTunes Backup	239	2.20%	195	2.60%	44	1.30%
iTunes Backup (Jailbroken)	239	2.20%	195	2.60%	44	1.30%
Device Seizure	124	1.14%	124	1.66%	0	0.00%
iPhone Explorer	25	0.23%	0	0.00%	25	0.74%
MobileSyncBrowser	168	1.55%	124	1.66%	44	1.30%
Mobilyze	239	2.20%	195	2.60%	44	1.30%
Mobilyze (Jailbroken)	239	2.20%	195	2.60%	44	1.30%
Oxygen Forensics	239	2.20%	195	2.60%	44	1.30%
Oxygen Forensics (Jailbroken)	239	2.20%	195	2.60%	44	1.30%

	Importance Rating 2					
	Total	Percentage Match	AddressBook	Percentage Match	Cache	Percentage Match
	1304		3		144	
iTunes Backup	93	7.13%	3	100.00%	2	1.39%
iTunes Backup (Jailbroken)	93	7.13%	3	100.00%	2	1.39%
Device Seizure	0	0.00%	0	0.00%	0	0.00%
iPhone Explorer	7	0.54%	0	0.00%	1	0.69%
MobileSyncBrowser	93	7.13%	3	100.00%	2	1.39%
Mobilyze	93	7.13%	3	100.00%	2	1.39%
Mobilyze (Jailbroken)	93	7.13%	3	100.00%	2	1.39%
Oxygen Forensics	96	7.36%	3	100.00%	2	1.39%
Oxygen Forensics (Jailbroken)	96	7.36%	3	100.00%	2	1.39%

Calendar	Percentage Match	Call History	Percentage Match	Camera	Percentage Match
1		1		1	
1	100.00%	1	100.00%	1	100.00%
1	100.00%	1	100.00%	1	100.00%
0	0.00%	0	0.00%	0	0.00%
0	0.00%	0	0.00%	1	100.00%
1	100.00%	1	100.00%	1	100.00%
1	100.00%	1	100.00%	1	100.00%
1	100.00%	1	100.00%	1	100.00%
1	100.00%	1	100.00%	1	100.00%
1	100.00%	1	100.00%	1	100.00%

Cookies	Percentage Match	Mail	Percentage Match	Maps	Percentage Match
3		16		2	
3	100.00%	1	6.25%	2	100.00%
3	100.00%	1	6.25%	2	100.00%
0	0.00%	0	0.00%	0	0.00%
0	0.00%	0	0.00%	0	0.00%
3	100.00%	1	6.25%	2	100.00%
3	100.00%	1	6.25%	2	100.00%
3	100.00%	1	6.25%	2	100.00%
3	100.00%	1	6.25%	2	100.00%
3	100.00%	1	6.25%	2	100.00%

Notes	Percentage Match	OS	Percentage Match	Safari	Percentage Match	SMS	Percentage Match
2		1118		11		2	
2	100.00%	67	5.99%	8	72.73%	2	100.00%
2	100.00%	67	5.99%	8	72.73%	2	100.00%
0	0.00%	0	0.00%	0	0.00%	0	0.00%
0	0.00%	3	0.27%	2	18.18%	0	0.00%
2	100.00%	67	5.99%	8	72.73%	2	100.00%
2	100.00%	67	5.99%	8	72.73%	2	100.00%
2	100.00%	67	5.99%	8	72.73%	2	100.00%
2	100.00%	69	6.17%	9	81.82%	2	100.00%
2	100.00%	69	6.17%	9	81.82%	2	100.00%

Appendix C - Journal

Date	Action	Result
3/06/2010	Download all firmware for the iPhone 3GS 3.0 to 3.1.3	Found that Apple only signs 3.1.3 now so the previous firmware revisions can't be installed. Research will be limited to 3.1.3 - Saurik method
	Reset settings as content	Only took a minute. - Deleted encryption keys - Didn't zero-out
	Installed 3.1.3. Jailbroke.	Used iWipe to zero-out free space - Will make a physical copy more readable
4/06/2010	Ran zero-out overnight	Completed successfully
	Restored non-jailbroken 3.1.3	Will have to set line in the sand date. OS 4 about to be released.
6/06/2010	Installed Windows 7 Enterprise 64-bit for windows based extraction tools	
	Activated iPhone with 3.1.3	
	Backed up with iTunes	All backup readers hardcode read directories. Symlink used to bypass.
	Created read-only dmg of backup files	
	Symlink to trick extraction tools "ln -s \Volume\[name]"	Backup - Must be as a sub-folder, not the root
	Extracted files from backup "ls -a -l -R" - list all files recursively	Saved file as "list of extracted files.txt"
	Installed Fink to get access to md5deep	Allows for recursive MD5 hashing
	Looked at Ubuntu PIN issue	Does not open any more access that iPhone Expolorer. Just doesn't require PIN to mount.
		PIN must ben required by iTunes. Software based.
	Generated MD5 hashes of all extracted files "md5deep -r *"	Saved to "list of all extracted files.txt"
	Imported in Excel	To columns: 1. Full path + filename 2. MD5 hash
	Installed Mac tools	All Mac tools
	Installed Mobiledit!	Does not appear to support the iPhone 3GS as it requires iTunes 8.x - Will investigate further
	Installed Device Seizure	- 4.0 hash been released. License doesn't work. - License has expired. Will request new one.
	Installed Oxygen Forensics	- Requires iTunes be installed. Version 9. Found iPhone once but crashed when acquiring. Will investigate later.
7/06/2010	Performed test acquisition with Mobilyze	- Can't seem to browse raw files - Hash it's own analysis interface - Keeps a log of files and MD5 hashes - Will comapre with manual backup
	Compare iTunes backup and Mobilyze	- Using an independent logging / hash system could be diffuclt due to the property evidence formats - Hashes match - Mobilyze hashes log files too - Will do straight compare -Rebuild firmware important
	Investigated Jonathan technique	- Supplied toolkit supports 1.x and 2.x firmware - Required access for 3.x - 2.x toolkit may be adoptable to 3.1.3
	Installed PwnageTool for 3.1.3	
	Installed XPWN for Mac OS X 10.6	Saved web site to "Resources"

	Jonathan method - Followed book	- Instructions in book work until restore "Error 1600" - Apparently you can't jailbreak 3.1.3 to 3.1.3 - Require apdated toolkit to perform this option
	Spirit jailbreka to get dd image	- Jailbroke 3.1.3 - USB sniffer?
	dd image of jailbroken iPhone	- Followed Jonathan book - Netcat and dd tools required
8/06/2010	Investiaged 4.0 firmware gold master	- Will stick to research on 3.1.3 for evaluation - Mobilyze could obtain a backup but the other tools couldn't
9/06/2010	Installed Device Seizure 4.0	- DongleManager must be installed - Selected not to install USB drivers as it doesn't include iPhone drivers - New version of iTunes required, iTunes provides USB drivers
	Tested Device Seizure with new license	- 4.0 license works - Requires old version of iTunes
	Attempted acquisition with Mobilyze	- Failed saving in lockdown mode or requires PIN
	Removed PIN code and auto screen lock	- Will investigate PIN later - Mobilyze still fails
10/06/2010	Installed iTunes for latest USB driver	- Quit iTunes helper background process
	Performed acquisition with Device Seizure	- iPhone Device (logical). Fails - iPhone Backup (Logical) - Should put into airplane mode prior to acquisition - What effect to files does airplane PIN and auto lock do? - Slow (20minss) - "Fill the sorter" - Y
	Installed Office 2010 for report to Excel	- Hash in app (Primary) - Export then hash (Secondary) - validates integrated hash
	Acquisition with Oxygen Forensics - Selected all options - Files on internal memory (not selected)	- 1 min to perform extraction - Must close app after disconnecting phone - can't find again - Property formats
	Performed acquisition with Mobilyze	- 9.2 beta iTunes has effected driver for backup - A few changes made to phone - Need to improve pre-acquisition process - Backup data files - excluded
	Analysis of Oxygen and Mobilyze data	Matched hashes
15/06/2010	Installed fresh copy of Mac OS X	
18/06/2010	Updated Mac OS X build to 10.6.4 with iTunens 9.2	- Testing will be solidified to iTunes 9.2 and firmware
	Updated Windows 7 build to iTunes 9.2	
	iTunes backup - files to read-only - hash of files	- Killed iTunes Helper process - Enabled airplane mode
	Mobilyze acquisition - log file saved out	
	iPhone Explorer acquisition - files copied out - files saved to read-only dmg - hash of files	
	Device Seizure acquisition - "iPhone Advanced (logical)" option selected	- Slow to acquired - Small data set
	Oxygen Forensic acquisition	- Doesn't work with iTunes 9.2, runtime error
	MOBILedit!	- Doesn't work with 9.2, 9.1.1 is fine - Access Denied on some filesystem components - Recommends jailbreaking
20/06/2010	Kep phone unchanged	Flight mode still active
	Jailbroke with Spirit jailbreak tool on Mac OS X while running 3.1.3 firmware	- Successful - Jailbreak process ran on phone - Flight mode was disabled - New mail came in

	Opened "Cydia" app and installed: - OpenSSH (5.2pl-8) - OpenSSL (pre-req) - netcat (0.7.1-2)	- Cydia organised categories and restarted - Downloaded new packages - Ignored updates
	Closed Cydia	
	Backed up with iTunes - Read-only dmg - Hash all files	
	Connected to local wireless network	Required for SSH access
	Set auto-lock to 'never'	- Stops SSH session from dropping out
	SSHed into iPhone User: root, Password: alpine	Had to accept encryption keys
	MD5 of partition	Failed - phone rebooted
	Uploaded MD5 from Jonathan supplie dfiles to /sbin	- Failed - package must be compiled for old firmware - Couldn't find on Cydia default repositories
	Used Jonathan method to send dd image off iPhone to computer - SSH - netcat - dd	- Section 3.2 of "iPhone Forensics" book - Should have used adhoc wireless network - Should set network settings to wireless only - disabling cellular network
	Remounted rdisk0s2 as read-only	
	Copied dd over wireless with netcat	
	Reran copy process with changes: - MD5 rdisk0s2 partition (user partition) - Flight mode with wireless only	
1/07/2010	Installed Encase 6.16.2	
	FlastBloc SE for external	Didn't work - GPT partitioned disk
	New case named "MFIT"	Encase will not be used to data storage - dmg read-only instead
4/07/2010	Extracted all evidence and hash infrmation where possible	Device Seizure - no file names: - Exported = Y, Calculated = Y iPhone Explorer: - Exported = N, Calculated = Y iTunes backup: - Exported = N, Calculated = Y MacLockPick: - Exported = Y, Calculated = N MobileSyncBrowser: - Exported = N, Calculated = Y Mobilyze: - Exported = Y, Calculated = Y Oxygen Forensics: - Exported = N (limitation of trial copy), Calculated = Y DD - Exported = N/A, Calculated = Y MOBILedit! (failed to recovery) - Exported = Y, Calculated = N
	Created read-only dmg files	
5/07/2010	Calculated hash file all exported files - md5deep "md5deep - r -z *" r = recursive z = display file size before hash	- Property date - invalide - Excel limited - Need to clarify relationships
14/07/2010	Mounted dd as read-only "hdiutil attach - readonly dd.dmg"	
	Imported dd hashes into analysis	Active logical files only
	Scanned deleted items (free space for SQLite + PLIST files) - Slow scan (byte-by-byte) - Added 10 examples of SQLite and PLIST files	

	Spreadsheet hash analysis	
	Classification of extracted files	
	Databases don't match but have same name	
20/07/2010	Database analysis	Database contents don't match - Reuslts show mismatched hashes - dd reimage each time would yeild better results - auto compact process?

Appendix D - Scenario Analysis

	Scenario A	MOBILedit! Forensic		Oxygen Forensics		Device Seizure		Mobiliyze		MacLockPick		MobileSyncBrowser		iPhone Explorer				
Extracts physical image	3	0		0		0		0		0		0						
Extracts logical image	3	3	3	3	3	3	3	3	3	1		2		2				
Supports non-jailbroken iPhones	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Supports jailbroken iPhones	3	0		3	3	0		3	3	3	3	3	3	3	3			
Supports writeblocking	0	0		0		0		0		0		0		0				
Extract of all files	3	0		0		0		0		0		0		0				
Can extract rating '2'	3	2		2		2		2		1		1		1				
Can extract rating '1'	3	2		2		2		2		2		2		1				
Can extract rating '0'	3	0		2		0		0		0		0		2				
Extraction took less than 12 hours	0	3		3		3		3		3		3		3				
Extraction took less than 1 hour	0	3		3		3		3		3		3		3				
Extraction took less than 10 minutes	0	0		0		0		3		3		3		3				
Filenames are retained	0	3		3		3		3		3		0		3				
Can extract files outside extraction tool	2	0		3	3	1		2	2	0		1		1		**MAX**	**MIN**	**AVG**
Support for hashing	1	3	3	3	3	3	3	3	3	3	3	0		0		18	6	11.333333
Support for logging extracted files	1	3	3	3	3	3	3	3	3	0		0		0		0.5806452	0.193548387	0.3655914
Extracts email messages	3	0		0		0		0		0		0		0		Oxygen	MobileSync	
	31		12		18		12		17		9		6		6		iPhone Explorer	

	Scenario B	MOBILedit! Forensic		Oxygen Forensics		Device Seizure		Mobiliyze		MacLockPick		MobileSyncBrowser		iPhone Explorer				
Extracts physical image	1	0		0		0		0		0		0		0				
Extracts logical image	3	3	3	3	3	3	3	3	3	1		2		2				
Supports non-jailbroken iPhones	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Supports jailbroken iPhones	3	0		3	3	0		3	3	3	3	3	3	3	3			
Supports writeblocking	3	0		0		0		0		0		0		0				
Extract of all files	0	0		0		0		0		0		0		0				
Can extract rating '2'	3	2		2		2		2		1		1		1				
Can extract rating '1'	1	2	2	2	2	2	2	2	2	2	2	2	2	1	1			
Can extract rating '0'	0	0		2		0		0		0		0		2				
Extraction took less than 12 hours	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Extraction took less than 1 hour	0	3		3		3		3		3		3		3				
Extraction took less than 10 minutes	0	0		0		0		3		3		3		3				
Filenames are retained	3	3	3	3	3	3	3	3	3	3	3	0		3	3			
Can extract files outside extraction tool	3	0		3	3	1		2		0		1		1		**MAX**	**MIN**	**AVG**
Support for hashing	3	3	3	3	3	3	3	3	3	3	3	0		0		26	11	18.333333
Support for logging extracted files	2	3	3	3	3	3	3	3	3	0		0		0		0.8387097	0.35483871	0.5913978
Extracts email messages	3	0		0		0		0		0		0		0		Oxygen	MobileSync	
	33		20		26		20		23		17		11		13			

	Scenario C	MOBILedit! Forensic		Oxygen Forensics		Device Seizure		Mobiliyze		MacLockPick		MobileSyncBrowser		iPhone Explorer				
Extracts physical image	1	0		0		0		0		0		0		0				
Extracts logical image	3	3	3	3	3	3	3	3	3	1		2		2				
Supports non-jailbroken iPhones	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Supports jailbroken iPhones	3	0		3	3	0		3	3	3	3	3	3	3	3			
Supports writeblocking	3	0		0		0		0		0		0		0				
Extract of all files	0	0		0		0		0		0		0		0				
Can extract rating '2'	3	2		2		2		2		1		1		1				
Can extract rating '1'	3	2		2		2		2		2		2		1				
Can extract rating '0'	0	0		2		0		0		0		0		2				
Extraction took less than 12 hours	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Extraction took less than 1 hour	0	3		3		3		3		3		3		3				
Extraction took less than 10 minutes	0	0		0		0		3		3		3		3				
Filenames are retained	3	3	3	3	3	3	3	3	3	3	3	0		3	3			
Can extract files outside extraction tool	3	0		3	3	1		2		0		1		1		**MAX**	**MIN**	**AVG**
Support for hashing	3	3	3	3	3	3	3	3	3	3	3	0		0		24	9	16.5
Support for logging extracted files	2	3	3	3	3	3	3	3	3	0		0		0		0.77	0.29	0.53
Extracts email messages	3	0		0		0		0		0		0		0		Oxygen	MobileSync	
	34		18		24		18		21		15		9		12			

	Scenario D	MOBILedit! Forensic		Oxygen Forensics		Device Seizure		Mobiliyze		MacLockPick		MobileSyncBrowser		iPhone Explorer				
Extracts physical image	2	0		0		0		0		0		0		0				
Extracts logical image	3	3	3	3	3	3	3	3	3	1		2		2				
Supports non-jailbroken iPhones	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Supports jailbroken iPhones	3	0		3	3	0		3	3	3	3	3	3	3	3			
Supports writeblocking	3	0		0		0		0		0		0		0				
Extract of all files	2	0		0		0		0		0		0		0				
Can extract rating '2'	3	2		2		2		2		1		1		1				
Can extract rating '1'	2	2	2	2	2	2	2	2	2	2	2	2	2	1				
Can extract rating '0'	2	0		2	2	0		0		0		0		2	2			
Extraction took less than 12 hours	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Extraction took less than 1 hour	0	3		3		3		3		3		3		3				
Extraction took less than 10 minutes	0	0		0		0		3		3		3		3				
Filenames are retained	3	3	3	3	3	3	3	3	3	3	3	0		3	3	**MAX**	**MIN**	**AVG**
Can extract files outside extraction tool	2	0		3	3	1		2	2	0		1		1		28	11	19.166667
Support for hashing	3	3	3	3	3	3	3	3	3	3	3	0		0		0.90	0.35	0.62
Support for logging extracted files	2	3	3	3	3	3	3	3	3	0		0		0		Oxygen	MobileSync	
Extracts email messages	3	0		0		0		0		0		0		0				
	37		20		28		20		25		17		11		14			

	Scenario E	MOBILedit! Forensic		Oxygen Forensics		Device Seizure		Mobiliyze		MacLockPick		MobileSyncBrowser		iPhone Explorer				
Extracts physical image	0	0		0		0		0		0		0		0				
Extracts logical image	0	3		3		3		3		1		2		2				
Supports non-jailbroken iPhones	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Supports jailbroken iPhones	3	0		3	3	0		3	3	3	3	3	3	3	3			
Supports writeblocking	0	0		0		0		0		0		0		0				
Extract of all files	0	0		0		0		0		0		0		0				
Can extract rating '2'	1	2	2	2	2	2	2	2	2	1	1	1	1	1	1			
Can extract rating '1'	0	2		2		2		2		2		2		1				
Can extract rating '0'	0	0		2		0		0		0		0		2				
Extraction took less than 12 hours	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Extraction took less than 1 hour	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3			
Extraction took less than 10 minutes	3	0		0		0		3	3	3	3	3	3	3	3			
Filenames are retained	3	3	3	3	3	3	3	3	3	3	3	0		3	3			
Can extract files outside extraction tool	3	0		3	3	1		2		0		1		1		**MAX**	**MIN**	**AVG**
Support for hashing	0	3		3		3		3		3		0		0		20	14	18
Support for logging extracted files	0	3		3		3		3		0		0		0		0.65	0.45	0.58
Extracts email messages	3	0		0		0		0		0		0		0		Oxygen	Device Seizure	
	25		14		20		14		20		19		16		19	Mobiliyze	MOBILedit!	