DATA INTEGRITY VALIDATION OF OPEN SOURCE IDEVICE FORENSIC TOOLS WITH REFERENCE TO COMMERCIAL TOOL

By

Maryam Jalees Ahmed

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

May 2015

ABSTRACT

In early 2010, Apple launched its first tablet and named it iPad. With the passage of time different models were invented. Locally and internationally, such tablets are commonly used and are in demand. User data partition and system partition are the two partitions that an iPad holds. User data partition contains user's data and extra applications installed, whereas basic applications and iOS are covered by system partition. From forensics viewpoint, user data partition contains various applications e.g. Adobe Reader, File Manager etc. These applications have spreadsheets and text documents that are likely to hold financial and sensitive data. Other applications like Skype and Facebook are expected to have important information (e.g. chat history). GUI, core OS, standard applications (like Mail, iPod, Safari, Calendar etc.) and application binaries are present in system partition. But the related statistics (such as user mail) are kept in data partition.

Techniques used to acquire data from iPad include synchronizing method, using inbuilt operating system utilities and using forensic tools (open source, freeware, or commercial). Some methods provide fast data extraction; on the other hand some practices are slow. Some techniques involve jailbreaking and some tools claim to provide fast data extraction without jailbreaking the device. Data extraction methods and open source tools are either freely available or can be bought in low price, whereas commercial tools are closed source and are highly expensive. It is also hard to define that the stated methods are real and whether these methods and tools preserve legitimacy of the data stored in the device.

In this research NIST standard/test results for iPad acquisition tool has been established and iPad forensics using a commercial tool has been performed in order to develop a reference for comparison. Then, iPad forensics using open source tools has been carried out. The legitimacy of data obtained from open source forensic tools has been compared to the data obtained from a commercial tool.

Therefore, the research introduces a comparative study to illustrate complete forensic analysis of iPad, showing the changes that have taken place and the areas affected by these changes when the system is jailbreaked. The proposed research also concludes about data integrity validation of iPad forensics using open source tools. Focus of the research is to determine whether data extracted from open source tools are valid and to what extent. To check data integrity of open source tools, statistics extracted from a commercial tool are kept as a baseline (standard/model).

DEDICATION

All thanks and praise to Allah the Almighty, the most gracious and the most merciful.
I dedicate my work to my family, my best friend and my supervisor who have supported me throughout the process.

ACKNOWLEDGMENTS

I am grateful to Him for guiding me to the right path to achieve my goal. I would like to thank my supervisor, Dr. Baber Aslam from the Department of Information Security for constant support and guidance.

Special thanks to my external supervisor, Mr Ammar Jaffri, who has provided me costly forensic gadget to gather respective data for my work. I am also extremely thankful to my committee members Dr. Mehreen Afzal and Lec. Mian Muhammad Waseem Iqbal for instructing and sharing significant knowledge to complete my work. My heart felt gratitude to my family and my best friend whose prayers and immense love assisted me along this long but fulfilling road.

TABLE OF CONTENTS

1	**Introduction**	**1**
1.1	Overview	1
1.2	Problem Statement	3
1.3	Objectives	3
1.4	Research Methodologies and Goals	4
1.5	Thesis Organization	4
2	**Literature Review**	**6**
2.1	Introduction	6
2.2	Computer Forensics Tool Testing (CFTT) Program	6
2.3	Related Work	7
2.4	Summary	8
3	**Research Methodology**	**9**
3.1	Introduction	9
3.2	Advantages and Area of Application	9
3.3	Establishing Test Results for Mobile Acquisition Tool	9
3.4	Mobile Forensics Methodology	10
3.5	Device Setup	16
3.6	Test Data	16
3.7	Summary	18
4	**Test Results for Mobile Device Acquisition Tool: Micro Systemation XRY v6.7**	**19**
4.1	Introduction	19
4.2	Test Results for Mobile Device Data Acquisition Tool	19
4.3	Results Summary	19
4.4	Mobile Devices	20
4.5	Testing Environment	20
4.6	Test Results	22
4.7	Summary	28

5 iPad Forensics Using Commercial Tool 29
5.1 Introduction 29
5.2 Acquisition 29
5.3 Examination and Analysis 30
5.4 Summary 35
6 iPad Forensics Using OS Utilities and Freeware 36
6.1 Introduction 36
6.2 Acquisition 36
6.3 Examination and Analysis 40
6.4 Summary 43
7 Comparison of Results and Discussion 44
7.1 Introduction 44
7.2 Comparison 44
7.3 Summary 52
8 Conclusion and Future Work 53
APPENDIX-I 54
BIBLIOGRAPHY 58
RELATED RESEARCH PUBLICATIONS 61

LIST OF FIGURES

Figure 1.1: Data Residing in User Partition 2
Figure 3.1: Proposed Framework 10
Figure 3.2: Flowchart of Investigation Methodology 12
Figure 4.1: MSISDN was not Stated (Test case: Equipment Data) 24
Figure 4.2: MSISDN was not Launched (Test case: Equipment Data) 26
Figure 4.3: MSISDN File Opened in Hex Editor 26
Figure 4.4: Name *police* Replaced by *rescue* (Test case: Case File Data Protection) 27
Figure 5.1: XRY Logical Failed to Read .pdf File 31
Figure 5.2: File Size Variation in Consecutive XRY Logical Extractions 31
Figure 5.3 *ResetCounter.plist* found in second logical extraction 33
Figure 5.4: Access Count Incremented in Second Logical Extraction 34
Figure 6.1: Device Connection Diagram 38
Figure 6.2: Connection Recommendations 38
Figure 6.3: Device Detect LED of Forensic USB Bridge does not Give Steady Illumination when Connected to iPad. 39
Figure 6.4: Device Detect LED of Forensic USB Bridge Gives Steady Illumination when Connected to iPod. 39
Figure 6.5: iPad's User Data Found via Ubuntu Machine 41
Figure 6.6: iPad's Application Documents Found via Ubuntu Machine 41
Figure 7.1: XRY Logical Failed to Retrieve Live .pdf Document from iPad 47
Figure 7.2: *Media* Folder Contained Few Additional Subfolders 48
Figure 7.3: Hackstore Subfolder Comprised Few Similar Folders As Present in *Media* Folder 48
Figure 7.4: Various Files Related to Jailbreaking were Present in *jb-install* 49
Figure 7.5: *Books* Subfolder Contained Various Folders 49
Figure 7.6: *var* Subfolder Contained Similar Artifacts as Associated with *Media* Folder and Artifacts of *Books* Subfolder were Infinitely Repeated. 50
Figure 7.7: Endless Iteration of *_ncurses* Subfolder 50
Figure 7.8: Endless Iteration of *mobile* Subfolder 51
Figure 7.9: Endless Iteration of *Media* Subfolder 51
Figure 7.10: Endless Iteration of *var* Subfolder 52

LIST OF TABLES

Table 3.1: Features of iPad 13
Table 3.2: iPad Identity on Different OS Platform 14
Table 3.3: Forensic Tool Breakdown by OS and Type 14
Table 3.4: Details of Data Associated With Each Application 17
Table 4.1: Mobile Devices 20
Table 4.2: Internal Memory Data Objects 21
Table 4.3: UICC Data Objects 22
Table 4.4: iPad 24
Table 4.5: Universal Integrated Circuit Cards 27
Table 5.1: Data Acquisition Steps 29
Table 5.2: Modified Files in XRY Acquisition Process 32
Table 5.3: Additional Files in Consecutive XRY Logical Acquisition 34
Table 5.4: Additional Files in Consecutive XRY Physical Acquisition 35
Table 6.1: Steps for Jailbreaking iPad 37
Table 6.2: Steps for Imaging iPad 37
Table 6.3: Specifics of Forensic USB Bridge 39
Table 6.4: Steps to Acquire iPad's Folder via iBrowse 40
Table 6.5: List of File Types Acquired from Ubuntu Platform 42
Table 7.1: Comparison of Folders Obtained from Various Acquisition Methods 44
Table 7.2: Hash Values of User Files Obtained from Various Acquisition Methods 45
Table 7.3: Differences in *persistent_manager_kind* Table 46

LIST OF ABBREVIATIONS

CFTT	Computer Forensics Tool Testing
SIM	Subscriber Identity Module
UICC	Universal Integrated Circuit Card
GPS	Global Positioning System
MSISDN	Mobile Station International Subscriber Directory Number

.

Chapter 1

Introduction

1.1 Overview

iDevices are being used by millions of people all around the world. There are different types of iDevices which can be used in criminal activities. These devices hold personal and organizational data which has forensic importance. [1] iDevices are characterized as portable devices which are generally closed embedded systems [2, 3]. Such systems prohibit direct access to the devices memory when connected to a personal computer [1, 3].

The widely used gadget in the field of embedded portable iDevices is the iPad. From storage/data point of view, an iPad comprises of system-partition and data-partition. System partition holds operating system and factory installed applications, while user's data and applications installed by the consumer are stored in data partition. As the system partition cannot be modified by user so it makes it non-evidential. Conversely, user partition has user specific data and hence assists the forensic investigator.

User partition contains various folders such as *Keychains, Mobile, Preferences, Root* and *Wireless*. *Keychains* folder stores the passwords used within iOS. *Mobile* folder comprises of three subfolders: Application, Library and Media. Application subfolder contains Cache, Preferences, Cookies, Webkits and applications itself. Library subfolder holds data like settings for system and system applications (Safari, Maps, Mail, Notes, Calendars, Address Book and Voicemail). Media subfolder holds user's Video's, Podcast's, Book's, Download's, Photo's, iTunes Data, Purchase's and Music data [1]. *Preferences* folder contains files related to system configuration, power management, network interfaces and wifi. Data related to location services is located in *Root* folder. Whereas, call history records from MobilePhone.app reside in *Wireless* folder. These folders are important for forensic investigator.

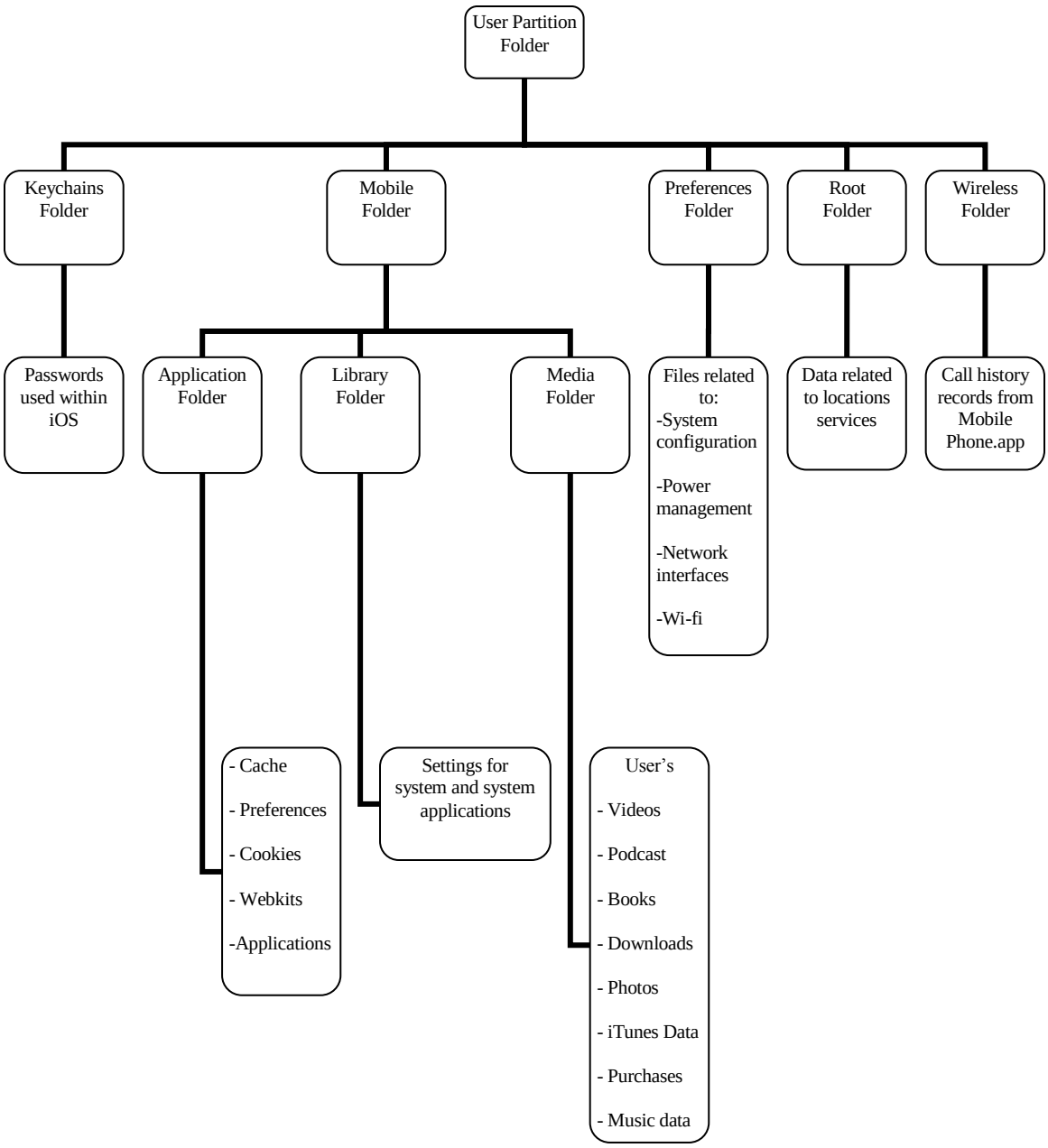


Figure 1.1: Data Residing in User Partition

There are few methods available through which data can be collected from iDevices. Synchronizing, jail breaking, using inbuilt operating system facility and using freeware/open-source tools are among free options for data acquisition. However, data retrieved through these techniques lack legitimacy. Conversely, commercial tools claim to provide legitimacy but they are proprietary software and expensive. Thus, it is tough to define that the stated methods are reliable and preserve data integrity [2, 3].

However an emerging challenge to digital forensic researchers is to guarantee data integrity of the retrieved artifacts. Data integrity has been identified as a vital element of digital forensics which must be ensured for acceptability of findings (retrieved forensic artifacts) in a court of law.

1.2 Problem Statement

New methods in the arena of computer forensics are introduced due to different features and type of statistics associated with the iPad. Because of high market demand and extensive use, such devices have become common. iPad delivers user's information and it can be a vital source of evidence for crime investigators, which can later be presented in a court [1]. In order to extract data from iPad, many techniques and tools have been introduced, but it is still very challenging to detect whether the proposed methods provide data integrity. Open source tools are freely available but have no assurance about data validity. On the other hand, commercial tools claim to provide legitimacy but are expensive.

Digital forensics solution providers offer different commercial tools. These tools are greatly used by law enforcement agencies and national security agencies to find digital evidence. Vendors of these tools claim that digital forensic investigator can acquire digital evidence in forensically secure manner.

The proposed work will compare the validity of data extracted from open source tools with the data obtained from commercial. The proposed work will also establish the validity (and its extent) of data that is obtained from open source tools thus enabling the use of open source tools for iPad forensics. The outcomes of this research study will help the law enforcement agencies in deciding the best tool for iPad forensic. The proposed work will also provide guidance about modified data and areas where alternations have taken place. It will also play a great role in defining laws for jail-broken devices.

1.3 Objectives

The main objectives of thesis are:-

a. Study NIST standards/test results for mobile device acquisition tool to establish test results for iPad acquisition tool.
b. Carryout iPad forensics using a commercial tool and establish a reference for comparison.

c. Carryout iPad forensics using open source tools.

d. Compare the legitimacy of data obtained from open source forensics tools with the data obtained from a commercial tool-illustrating:

I. Complete forensic analysis of iPad.

II. Validation of artifacts extracted from open source tools.

III. Extent of data validity.

e. Recommend the best acquisition tool depending on the requirement of forensic examiner.

1.4 Research Methodologies and Goals

The research work was divided into four phases. In the first phase, NIST standards/test results for mobile device acquisition tool were studied in detail, in order to establish guidlines for iPad acquisition tool. In the second phase, iPad forensics using a commercial tool had been performed. Data obtained via the commercial tool had been thoroughly analyzed. Moreover, various consecutive extractions of the data with the help of a commercial tool were performed with the purpose to identify unique facts and figures in commercial forensic tool operations. In third phase, iPad's data had been acquired using operating system utilities, freeware and jail breaking technique. In fourth phase, the forensic artifacts acquired from different tools and techniques were compared to ascertain their data integrity. The results have shown that on one hand the freeware tools, under certain circumstance, also preserve data integrity as their commercial counterparts but on the other hand the commercial tools, under certain circumstance, also make data integrity doubtful as generally believed for freeware tools. Based on the results, the research has also recommended various data acquisition tools that the forensic examiner can select depending on the requirement.

1.5 Thesis Organization

The thesis is outlined as follows. The second chapter covers the level of research already carried out on the proposed area. The third chapter describes various setups and procedures being used for each investigation. This chapter also gives an understanding of investigation methodology. The fourth, fifth and sixth chapters provide outcome of various investigation processes. The seventh chapter discusses and compares the results of the assessment and brings out interesting facts and figures. This chapter also recommends

various acquisition techniques depending on forensic investigator requirement. The eighth chapter concludes the aim of this research accompanied by all executed procedures and steps and also proposes an area for future research.

Chapter 2

Literature Review

2.1 Introduction

The chapter discusses the work already been done by Computer Forensics Tool Testing (CFTT) Program for the validation of forensic tools. The chapter also discusses various tools and techniques which have been developed to extract data from digital devices. Moreover, the level of research already carried out on these tools/techniques and the relevant researches have been highlighted below.

2.2 Computer Forensics Tool Testing (CFTT) Program

CFTT program is the project at National Institute of Standards and Technology (NIST). Basically it is the combine project of various national institutes and is supported by numerous crime centers and investigation organizations. The objective of this program is to give assurance to the investigators that the respective computer forensic tool used for the investigation offers precise results. In order to achieve accurate results, the specifications and test methods for forensic tools are developed and the tools are tested against these specifications. [4, 5]

The test results give essential information for forensic tool developers, users and legal community. Based on the test results developers can improve forensic tools, users can make knowledgeable choices about using tools, and legal community can understand the capabilities of the tools. For conformance testing and quality testing, the approach for testing computer forensic tools is based on renowned international methodologies. For review and comment by the computer forensics community, the specifications and test methods are available on the CFTT website [5]. Various versions of the XRY tool have been tested against the Smart Phone Tool Test Assertions and Test Plan [6]. These assertions and test plan is available at the CFTT website. In this research Micro Systemation XRY version 6.7 has been tested against available test assertions and test plan. See chapter 4 for the details. Moreover, the test results from other tools and the CFTT tool methodology are available on NIJ's computer forensics tool testing web page [7].

2.3 Related Work

Different methods have been explored to acquire data from iDevices. Most relevant work has been discussed below:

Zdziarski [8], offered a way to gather iPhone forensic image through Wi-Fi and serial port. Method involved few steps like device jailbreaking, usage of SSH access and some regular UNIX tools. Image was transferred using Wi-Fi that was fairly slow.

Gomez [2], carried out analysis of data extraction by connecting iPad to iTunes installed system via normal USB. The software harmonizes current data and recovers backup from the portable device. To synchronize, proper pairing between the device and the software is required. The paper also proposed a fast method of imaging an iPad directly to the attached USB drive by using a cheap iPad accessory. This research concluded that commercial tools can give same imaging rate but there is no surety about data integrity.

Kubi [9], evaluated UFED and XRY tools which are used to extract evidence from mobile devices. The paper investigated these tools in order to provide convenience to mobile investigator for selecting suitable tool for a particular scenario. NIST smartphone tool specification was made the base for this evaluation. Results of the evaluation were represented graphically showing that XRY outdid UFED in many circumstances.

Sigwald [10, 11], discussed a tool for automatic SSH ramdisk creation and loading. Suggested method supported devices with A4 chips and lower. Required files from Apple were automatically downloaded by the tool and SSH client was used to run different commands. The tool performed DD and NAND dump.

Iqbal [1], developed a technique to gather records without jailbreaking the iDevices. Focus of the proposed technique was to provide data extraction in less than half an hour while preserving integrity of the evidence. The paper explains that to get a root access, weakness was exploited in the booting phase. Tool for analysis of extracted data was also developed. The paper also discussed that integrity factor is doubtful when a device is jailbreaked or a commercial tool is used for data mining.

Abalenkovs [3], discussed the security features of two operating systems i.e. iOS and Android in detail. The paper compared the existing techniques on data retrieval and presented a way to examine extracted data. Various open source and closed source tools

were also discussed. The paper also concluded that integrity factor is doubtful when a device is jailbroken or rooted.

The above mentioned studies conclude that many techniques and tools have been suggested for extracting data from iDevices, but ensuring data integrity is still very challenging. Open source tools are freely available but do not provide any assurance about data validity. On the other hand, commercial tools claim to provide reliability but are expensive.

Despite the importance of data integrity in the digital forensic, there is no study available in the literature that has compared the validity of data extracted from open source tools with the data obtained from commercial tools. The proposed work will establish the validity (and its extent) of data that is obtained from open source tools thus enabling the use of open source tools for iPad forensics.

2.4 Summary

The chapter has thoroughly explained the purpose and objective of CFTT program. The relevant work on open source and commercial forensic tools has also been discussed in this chapter. Moreover, the main concept of the current research work has been properly explained in this chapter

Chapter 3

Research Methodology

3.1 Introduction

The chapter highlights the advantages and the areas where this research can be utilized. This chapter also highlights the proposed research methodology being adopted using the existing frame work. Therefore, the chapter gives an understanding of existing mobile forensic frame work in order to develop the proposed methodology for iDevice. Moreover, different arrangements and techniques used for the forensic investigation are also discussed in this chapter.

3.2 Advantages and Area of Application

By inspecting and conducting a comparative study, we have achieved various goals These goals include a complete data image, deleted data extraction, forensic analysis of iPad, artifacts of iPad's applications, assurance of data integrity, confirmation for premium iPad forensic tool and useful information for making and modifying jailbreaking laws. Area where this research can be used are digital forensics solution providers, forensics and IT security companies, law enforcement agencies, data discovery, data recovery, law firms, national corporations and government agencies

3.3 Establishing Test Results for Mobile Acquisition Tool

As mentioned in the first chapter, to check the data integrity of the open source tools, a consistent commercial tool is taken as base/reference for the comparison. The commercial tool named: Micro Systemation XRY version 6.7 has been selected for the proposed use. Before the comparison process, XRY 6.7 has been tested according to the Computer Forensics Tool Testing (CFTT) program [4]. Before the commencement of the test for XRY version 6.7, existing test results reports for .XRY v 3.6, v 5.0.2 and v 6.3.1 were studied in detail [5, 12, 13]. Existing reports explain that capability of XRY (v 3.6, v 5.0.2 and v 6.3.1) has been tested using various mobile phones and SIMs. However, in this research XRY v 6.7 has been tested for its capability to obtain data from the tablet (i.e. iPad) and SIM. Details of the testing process are mentioned in chapter 4.

3.4 Mobile Forensics Methodology

The mobile forensics methodology adopted for this research has been discussed in the following section.

3.4.1 Proposed Methodology

In order to carryout appropriate mobile forensic investigation and to maintain integrity of a device, the investigator must follow a standard procedure. Mobile forensic methodology adopted for this research is based on the investigation process mentioned in "**Guidelines on Mobile Device Forensics**" [14]. Keeping in view the forensic steps mentioned in the publication, a better methodology/frame has been proposed.

Figure 3.1: Proposed Framework

The steps mentioned in the above framework are described below.

1. **Scope:** In this step, the room/area for the investigation is decided. This step should clearly mention the existing and installed applications to be examined.
2. **Preservation:** In this step evidence is gathered in such a manner that the data residing in the device is not altered or damaged and it is acceptable in a court of law.
3. **Acquisition:** In this step, data is acquired from the device using different tools and techniques. Different approaches to acquire data from the device are creating forensic image of a device, using write protection method, using commercial and open source tools. The forensic investigation starts by identifying the device. This step should clearly mention the characteristics of a device and requirement of incident/case, as it directs in selecting the data acquisition technique for an investigation. At the commencement of acquisition, version of the tool being used should also be properly documented. Moreover, a proper connection between the device and forensics workstation must be maintained to attain artifacts from the target device.

4. **Examination and Analysis:** Examination step reveals/exposes hidden digital evidence. This step involves technical procedures to achieve the results and is performed by a forensic specialist. However, the analysis step sees the outcomes of the examination for its importance/worth and truthfulness to the incident/case. Analysis is carried out by the investigator, the forensic examiner or analyst.
5. **Reporting**: In this step, complete details of performed activities and results of the examination are recorded. A fine report includes all the executed actions, outcomes of investigation, snapshots and the content generated by a tool. As we know digital evidence and tools/techniques used for an investigation can be challenged in a court of law, therefore an appropriate documentation along with copy of the software used must exist.

3.4.2 Application of Forensics Methodology

For the forensic investigation of iPad, all the phases described in the proposed framework are followed. The forensic investigation methodology adopted for iDevice is shown in figure 3.2.

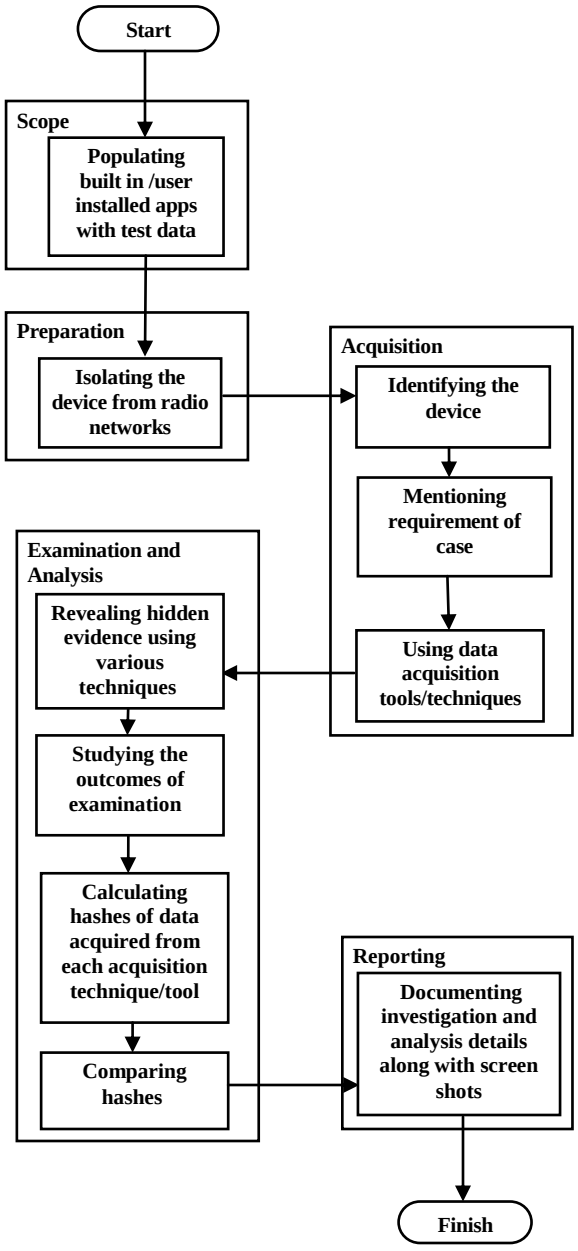


Figure 3.2: Flowchart of Investigation Methodology

The succeeding section explains how each action is performed in the investigation of iPad.

3.4.2.1 Scope

Data associated with basic/built-in applications on iPad1 (version 5.1.1) and other applications installed by the user come under the scope of this research. Built-in applications include: Safari, Messages, Calendar, Notes, Reminders, Videos, iTunes,

Music, Photos, Mail, Contacts and Maps. Whereas, other applications such as Adobe Reader, Skype, FileManager, and Temple Run were installed by the user. All applications of iPad were populated with various test data. Test data is mentioned in section 3.6. The purpose of this attempt was to locate the files containing artifacts in the respective folders when the specific investigation was performed.

3.4.2.2 Preservation

The first step in any forensic investigation is to gather evidence in a forensically secure manner. In this research the target device was already known so there was no need to search evidence. However, the iPad was isolated from various radio networks by disabling wifi, bluetooth and cellular options on target device. The purpose of isolation was to avoid synchronization and modification of the data residing in various applications of iPad.

3.4.2.3 Acquisition

For the acquisition (throughout this research work) a forensics workstation, data acquisition tools and an iPad were used.

Device Identification

In this research, the iPad characteristics were first identified. Make and Model of iPad are mentioned in Table 3.1. After the recognition of iPad characteristics, different manuals and manufacturing website were consulted to get detail information about iPad. According to the studies, idiosyncrasies of the embedded portable devices like iPad hinder access to its partitions without using forensic softwares.

Table 3.1: Features of iPad

Device	Details
iPad 1	Capacity: 64 GB Version: 5.1.1 (9B206) Model: A1337 IMEI: 012328008813090 Serial: V5036ZH9ETV

Requirement of Event/Case

The main purpose of this research was to compare validity of iPad's data obtained via operating system utility and freewares to the data obtained through the commercial

tool. Another aspect of this research was to identify interesting patterns in consecutive extractions. These consecutive extractions were performed on iPad using a commercial tool.

Forensics tools and techniques

Keeping in view the characteristics of iPad and the data to be extracted (depending upon case requirement), this research work involved three data acquistions tools i.e., Windows 7 and Ubuntu - operating system with an inbuilt data extraction utility, libimobiledevice - a freeware and XRY Complete - a commercial tool were used.

For the investigation, the iPad was mounted to Windows 7 and Ubuntu machine separately. Appearance of an iPad on each operating system was different as shown in Table 3.2. The extraction was then performed on iPad with the help of libimobiledevice and XRY. Table 3.3 illustrates the two forensic tools used in this experiment with different operating systems.

Table 3.2: iPad Identity on Different OS Platform

Operating Sytem Platform	**Identity Status**
Microsoft Windows 7 – 32 bit	Portable Device
Ubuntu 12.04.3 LTS	MJ's iPad Documents on MJ's iPad

Table 3.3: Forensic Tool Breakdown by OS and Type

Tools	**Operating System Requirements**	**Type**
XRY Complete v6.7	Microsoft Windows 7	Commercial Tool
Libimobiledevice	Linux	Free Software

While iPad was mounted to operating system utilities and libimobiledevice installed workstation, data acquisition was performed in read mode only. Read mode avoids accidental change in device's state. However, the write protection method was not used when acquisition was performed via XRY Complete because XRY Complete has inbuilt write blocker.

3.4.2.4 Examination and Analysis

Examination: The evidence acquired via each tool had different format. Depending upon the format, different examination process was used. The examination process for each acquisition is explained in chapter 5 and chapter 6.

Analysis: Various files and folders were exposed from the examination process. Keeping in view the requirement of this research, analysis process had recognized the particular directory/folder and comprehended what it holds. Various files of different types were present in each folder. Then, hashes were calculated for each file. MD5 is vulnerable to birthday attack which makes it less secure [15]. There is a high probability that two different inputs can get same hash values in our research. To complement the outcomes of MD5, we have also used SHA-256. SHA-256 is more secure and collision resistant. Hashes for files (artifacts) acquired from open source tools/freewares were compared to the hashes for files acquired from commercial tool in order to check data validity.

Moreover, interesting forensic patterns in the operations of closed source commercial tool were analyzed. Five consecutive extractions were performed on an iPad using XRY Complete. The files thus generated were compared for changes in the file size and hash values. This difference in file sizes and hashes aids the analyst to figure out the modifications in each of the XRY file. Unique facts and figures in commercial forensic tool operations were identified and are elaborated in chapter 6.

3.4.2.5 Reporting

For this research, the investigation report contained the software-generated data, artifacts gathered during the examination that outlines the actions executed, examination and analysis performed and the significance of the evidence revealed. There are different types of forensic tools used in this research; a commercial tool XRY Complete generates reports (in different formats like .doc and pdf).While, freewares like Ubuntu and Libimobiledevice do not provide report generation facility. To overcome reporting issue for freeware tools, distinct screenshots of each tool interface have been captured which were later assembled into a report format. Moreover, certain data (such as video and audio) was not presentable in a printed format and as a substitute was included with the report on DVD.

3.5 Device Setup

Before using the iPad, proper configuration of iPad was required. The following settings/ steps were performed to complete the arrangements.

Language: English

Country: Pakistan

Location Services: Enabled

Wi-Fi Network: Enabled

Setup as new iPad: Yes

Creating an Apple ID: Yes

Setup/Use iCloud: No

Find My iPad: Yes

Set Up Email: Yes

Snapshot of each step is included in the Appendix-I

3.6 Test Data

iPad contains two types of applications i.e. inbuilt and user installed applications. For the examination and application of proposed methodology, below mentioned activities were performed on the iPad.

Activity 1: Various applications were installed on iPad

Activity 2: Various data/files were then stored in built-in and user installed application.

Activity 3: Few files were then deleted from each application.

Details of each activity are mentioned in table 3.4. The built-in applications which are not important from forensics perspective were not taken into the scope of this research work (for the investigation) and thus were not populated with the data. These three applications are *YouTube*, *Game Center* and *Newsstand*. Two built-in applications like *App Store* and *Settings* were not populated with any data but were utilized for this research work. *App store* was used to download respective applications from the Apple store whereas *Settings* was used make required changes into the iPad.

Table 3.4: Details of Data Associated With Each Application

Name of Application	**Type of Application**	**Status**	**No. of Files Populated**	**No. of Deleted Files**
Safari	Inbuilt	Active	Bookmarks: 4 Bookmarks Bar: 2 Gmail Account: 4 emails Yahoo Account: 6 emails Hotmail Account: 2 emails No of facebook account signed in: 1 Google Maps: searched 3 locations	Bookmarks: 2 Bookmarks Bar: 1 Gmail Account: 3 emails Yahoo Account: 3 emails (And 1 unread) Hotmail Account: 1 email No. of contents deleted from signed in facebook account: 2 -
Messages	Inbuilt	Active	Sent: Messages and attachments Received: Messages and attachments	-
Calendar	Inbuilt	Active	8	1
Notes	Inbuilt	Active	4	2
Reminders	Inbuilt	Active	3	1
Videos	Inbuilt	Active	8 3 (.mp4) 3 (.m4v) 2 (.mov)	3 1 (.mp4) 1 (.m4v) 1 (.mov)
Music	Inbuilt	Active	7 (.mp3)	3 (.mp3)
Photos	Inbuilt	Active	2 (JPEG image) 2 (PNG image) 2 (GIF image)	1 (JPEG image) 1 (PNG image) 1 (GIF image)
Mail	Inbuilt	Active	2	1
Contacts	Inbuilt	Active	3	1
Maps	Inbuilt	Active	4	-
Adobe Reader	User Installed	Active	2 (.pdf)	1 (.pdf)
Skype	User Installed	Active	- No. of accounts signed in: 1 - Performed conversation with two different contacts	Deleted one contact from signed account
FileManager	User Installed	Active	2 (.docx) 2 (.ppt) 2 (.xlsx)	1 (.docx) 1 (.ppt) 1 (.xlsx)
Temple Run	User Installed	Active	Played once	-

3.7 Summary

The chapter has explained the importance of this research and has given the purpose of establishing test results for a commercial mobile forensic tool. The chapter has also clarified the methodology adopted for the forensic investigation of iDevice. Each step of forensic investigation methodology has been thoroughly explained. Moreover, various setups and executed actions associated with the application of methodology are appropriately documented.

Chapter 4

Test Results for Mobile Device Acquisition Tool:

Micro Systemation XRY v6.7

4.1 Introduction

This chapter validates the appropriateness of Micro Systemation XRY v6.7 according to Computer Forensics Tool Testing (CFTT) Program. The chapter documents the result summary and irregularities that came across when various tests were performed. Moreover, the chapter describes the mobile device which was selected for testing the tool, environment for performing the tests and data objects that were used to populate mobile device internal memory as well as associated media (i.e.UICC). The chapter also provides the results of selected test cases. However, the assertions and other details associated with each selected test case have been written/recorded on the DVD (which is attached at the end of this thesis).

4.2 Test Results for Mobile Device Data Acquisition Tool

Tool Tested:	XRY
Version:	6.7
Run Environment:	Windows 7 Enterprise 32-bit (6.1, Build 7601) Service Pack 1
Supplier:	Micro Systemation Inc
Visiting Address:	Hornsbruksgatan 28, SE-117 34 Stockholm, Sweden
Mailing Address:	Box 17111, SE-104 62 Stockholm, Sweden
Tel:	+46 8 739 02 70
Fax:	+46 8 730 01 70
WWW:	http://www.msab.com

4.3 Results Summary

The XRY is capable of extracting data from a wide range of mobile devices for example, GPS navigation units, smartphones, portable music players, 3G modems and the tablet processors (e.g. iPad) and Universal Integrated Circuit Card (UICC). The tool has been verified for its proficiency to acquire live and deleted data from the internal memory

of mobile device and universal integrated circuit card. The tool has acquired all the supported data objects correctly for all devices tested with the exception of the following anomalies.

Subscriber related data:

- Subscriber related information (i.e., MSISDN, IMSI) was not acquired after a successful mobile device internal memory acquisition. (iPad1 3G)

MSISDN:

- MSISDN was not presented in a useable format after a successful universal integrated circuit card memory acquisition. (iPad1 3G)

Modified device case data:

- When the case file or individual data objects were modified via third party means, the tool failed to notify the user that the universal integrated circuit card case data had been modified. (iPad1 3G)

For additional details see sections 4.5.1 – 4.5.2

4.4 Mobile Devices

The mobile device used for testing XRY v 6.7 is listed in the following table.

Table 4.1: Mobile Devices

Make	Model	OS	Firmware	Network
Apple iPad 3G	iPad 1 - MC497LL	iOS v5.1.1 (9B206)	07.11.01	GSM (Ufone, Telenor)

4.5 Testing Environment

The tests were performed in the forensic lab. This section explains the selected test execution environment and the data objects used to populate the internal memory of mobile device and universal integrated circuit cards (UICCs).

4.5.1 Execution Environment

One computer was used to run the tool (Micro Systemation XRY version 6.7): **MJ**

MJ has the following configuration:

Windows 7

Phoenix ROM BIOS PLUS Version 1.10 A09

Intel(R) Pentium(R) M processor 1.60GHz, ~1.6GHz

2.50 GB RAM

Intel integrated Media Accelerator 900 graphics card

TSSTcorp DVD+-RW TS-L632D ATA Device

Dell 1470 Internal Wireless 802.11a/b/g

3 USB 2.0

VGA out

Modem RJ-11

Ethernet RJ-45

Audio line-out (for speaker's headphones)

External microphone port

ExpressCard 34 slot

4.5.2 Internal Memory Data Objects

In order to measure Micro Systemation's XRY, the acquired data from the internal memory of pre-populated mobile device was analyzed. Table 4.2 shows the data objects and elements populated on the mobile device.

Table 4.2: Internal Memory Data Objects (from [13])

Data Objects	Data Elements
Address Book Entries	
	Regular Length
	Maximum Length
	Special Character
	Blank Name
	Regular Length, email
	Regular Length, graphic
	Regular Length, address
	Deleted Entry
	Non-ASCII Entry
PIM Data	
Datebook/Calendar	*Regular Length*
Memos	*Maximum Length*
	Deleted Entry
	Special Character

	Blank Entry
Stand-alone data files	
	Audio
	Graphic
	Video
	Audio –Deleted
	Graphic –Deleted
	Video –Deleted
Application Data	
	Device Specific App Data
Internet Data	
	Visited Sites
	Bookmarks
Location Data	
	GPS Coordinates

4.5.3 UICC Data Objects

The data elements populated on Universal Integrated Circuit Cards (UICCs) are presented in the Table 4.3

Table 4.3: UICC Data Objects

Data Objects	Data Elements
Abbreviated Dialing Numbers (ADN)	
	Maximum Length
	Special Character
	Blank Name
	Non-ASCII Entry
	Regular Length -Deleted Number
Call Logs	
	Last Numbers Dialed (LND)
Text Messages	
	Incoming SMS –Read
	Incoming SMS –Unread
	Non-ASCII SMS
	Incoming SMS –Deleted
	Non-ASCII EMS
	Incoming EMS -Deleted

4.6 Test Results

The test cases results stated by the tool are given in this section. Section 4.6.1 and section 4.6.2 cover the mobile device and universal integrated circuit card used respectively for testing Micro Systemation's XRY.

The *Test Cases* column (internal memory acquisition/UICC) in sections 4.6.1 – 4.6.2 contains two sub-columns that describe a specific test category and individual sub-

categories. These sub-categories are verified within each test case when acquiring the internal memory for supported mobile device and UICC. The results for tested mobile device/UICC are shown in each individual sub-category row. The results are described below.

As Expected: Expected test results were returned by the mobile forensic application - Data from the mobile device/UICC was successfully acquired and reported by the tool.

Partial: Some of data from the mobile device/UICC was returned by the mobile forensic application

Not As Expected: Expected test results were not returned by the mobile forensic application – Data from the mobile device/UICC was not successfully acquired and reported by the tool.

NA: Not Applicable – the mobile forensic application is incapable to carry out/execute the test; or the support for the acquisition of a particular data element is not provided by the tool

4.6.1 Mobile Device

Micro Sytemation's XRY v 6.7 was used for acquiring and analyzing the internal memory contents for iPad.

With the exception of the test case mentioned below, all other test cases related to the acquisition of iPad were successful

Acquisition of Subscriber Related Data

In test case: *equipment data,* subscriber related information (i.e., MSISDN, IMSI) was not reported for the iPad1 3G after a successful internal memory acquisition

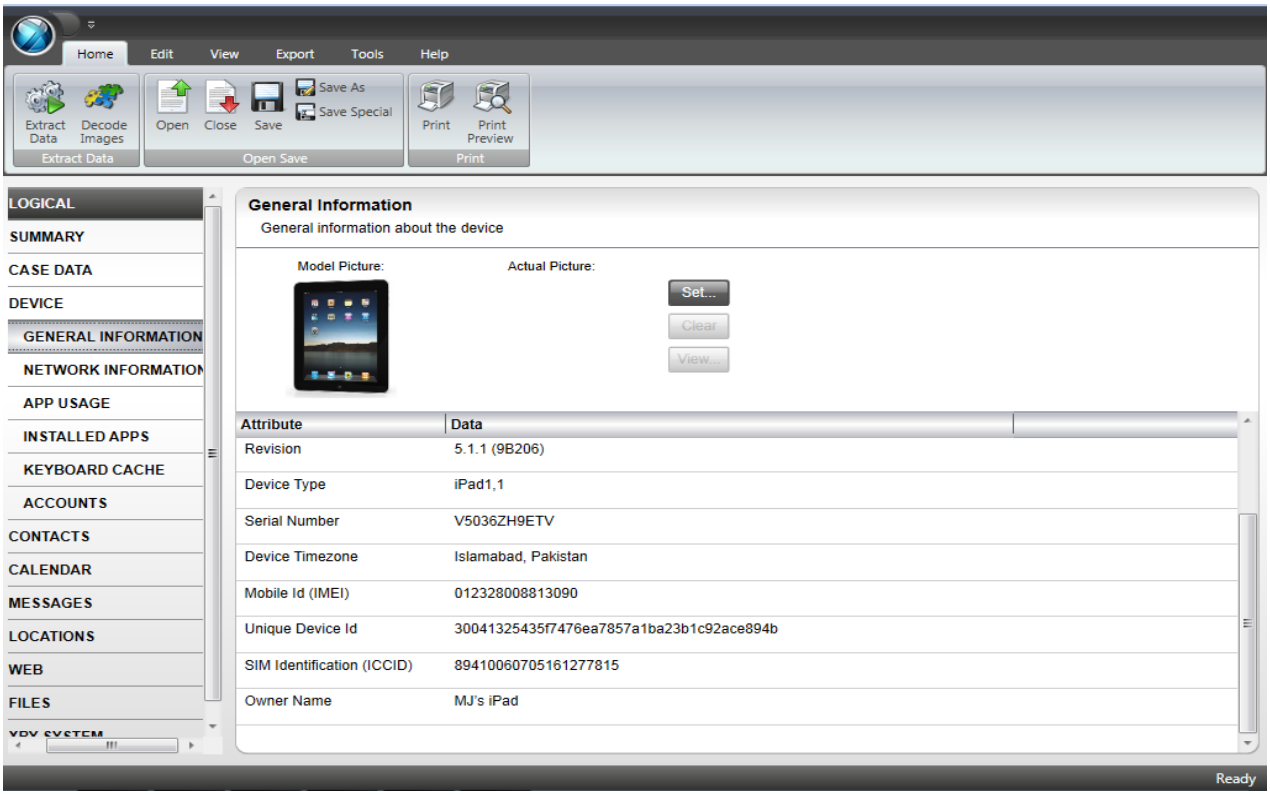


Figure 4.1: MSISDN was not Stated (Test case: Equipment Data)

See Table 4.4 below for more details.

Table 4.4: iPad

XRY v6.7		
Test Cases – Internal Memory Acquisition		*iPad 1*
Connectivity	Non Disrupted	*As Expected*
	Disrupted	*As Expected*
Reporting	Preview Pane	*As Expected*
	Generated Reports	*As Expected*
Equipment/ User Data	IMEI	*As Expected*
	MEID/ESN	*As Expected*
	MSISDN	***Not As Expected***
PIM Data	Contacts	*As Expected*
	Calendar	*As Expected*
	To-Do List/Tasks	*As Expected*
	Memos	*As Expected*

Stand-alone Files	Graphic	*As Expected*
	Audio	*As Expected*
	Video	*As Expected*
Application Data	Documents	*As Expected*
	Spreadsheets	*As Expected*
	Presentations	*As Expected*
Internet Data	Bookmarks	*As Expected*
	History	*As Expected*
Acquisition	Acquire All	*As Expected*
	Selected All	*As Expected*
	Select Individual	*As Expected*
Case File Data Protection	Modify Case Data	*As Expected*
Physical Acquisition	Readability	*As Expected*
	Deleted File Recovery	*As Expected*
	PUK attempts reported	*As Expected*
Non-ASCII Character	Reported in native format	*As Expected*
Hashing	Hashes reported for acquired data objects	*As Expected*
GPS Data	Coordinates (Long/Lat)	*As Expected*

4.6.2 Universal Integrated Circuit Cards (UICCs)

Micro Sytemation's XRY v 6.7 was used for acquiring and analyzing the internal memory contents for Universal Integrated Circuit Cards (UICCs).

With the exception of test cases mentioned below, all other test cases related to the acquisition of UICCs were successful

Acquisition of MSISDN

In test case: *equipment data*, subscriber related information i.e. MSISDN was not presented in a useable format after a successful UICC internal memory acquisition.

XRY case file reported MSISDN under unrecognized file category. And MSISDN file was not launched due to unknown file type/extension. To check whether the file contains useable data, MSISDN file was opened with a hex editor. However, nothing was found comprehensible.

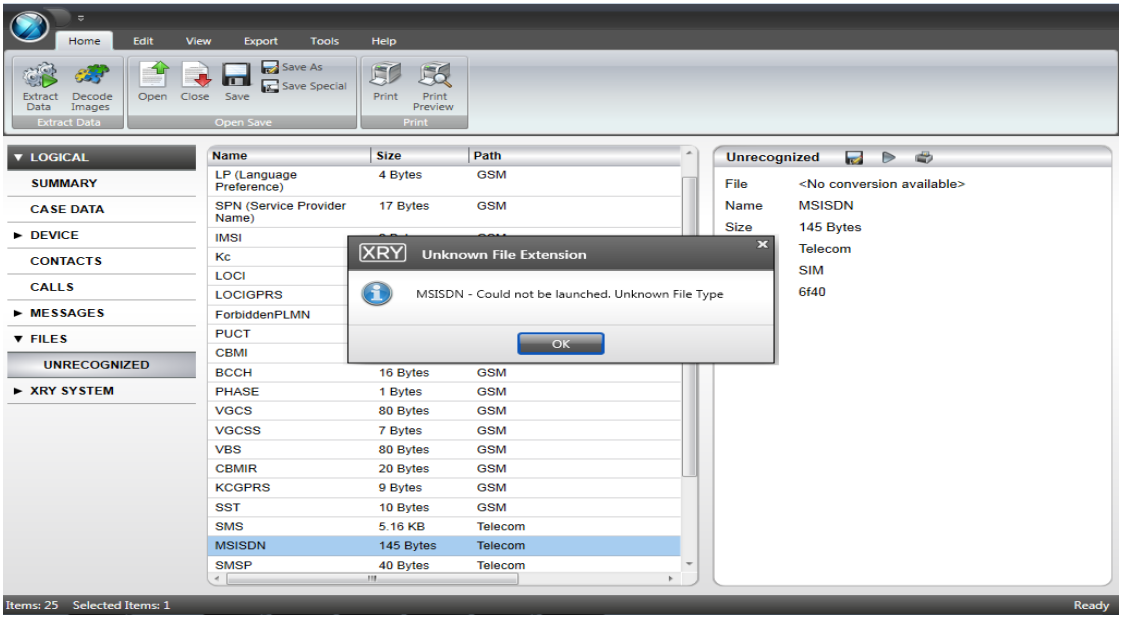


Figure 4.2: MSISDN was not Launched (Test case: Equipment Data)

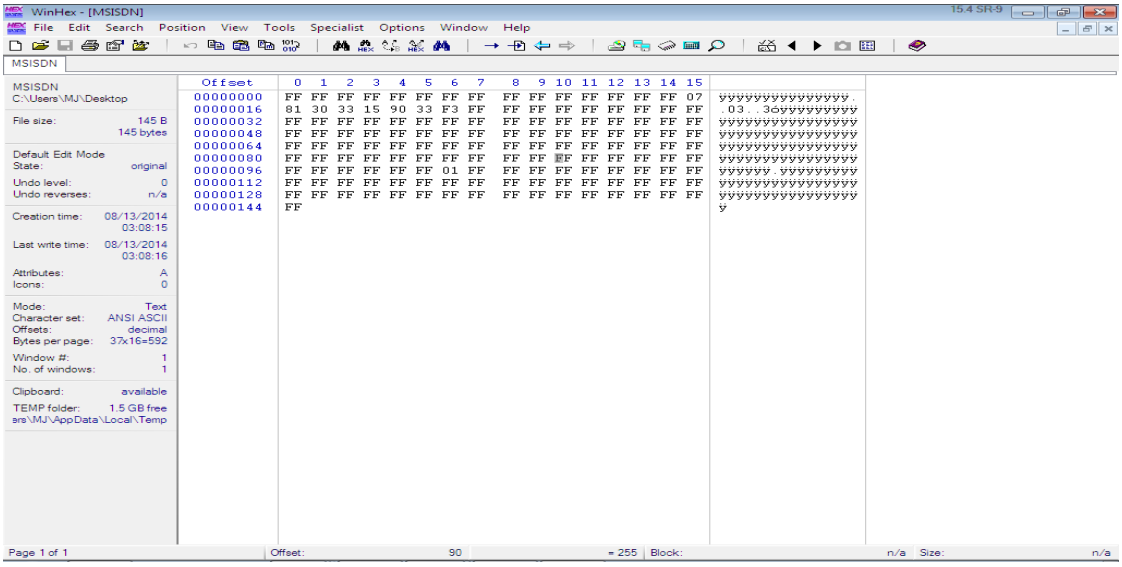


Figure 4.3: MSISDN File Opened in Hex Editor

Notification of modified device case data

In test case: *case file data protection*: Notification of modified UICC case data was not successful for Universal Integrated Circuit Cards. The saved case file was modified with a hex editor. Modified file was re-opened with the mobile device tool. Tool failed to notify that the case file has been altered.

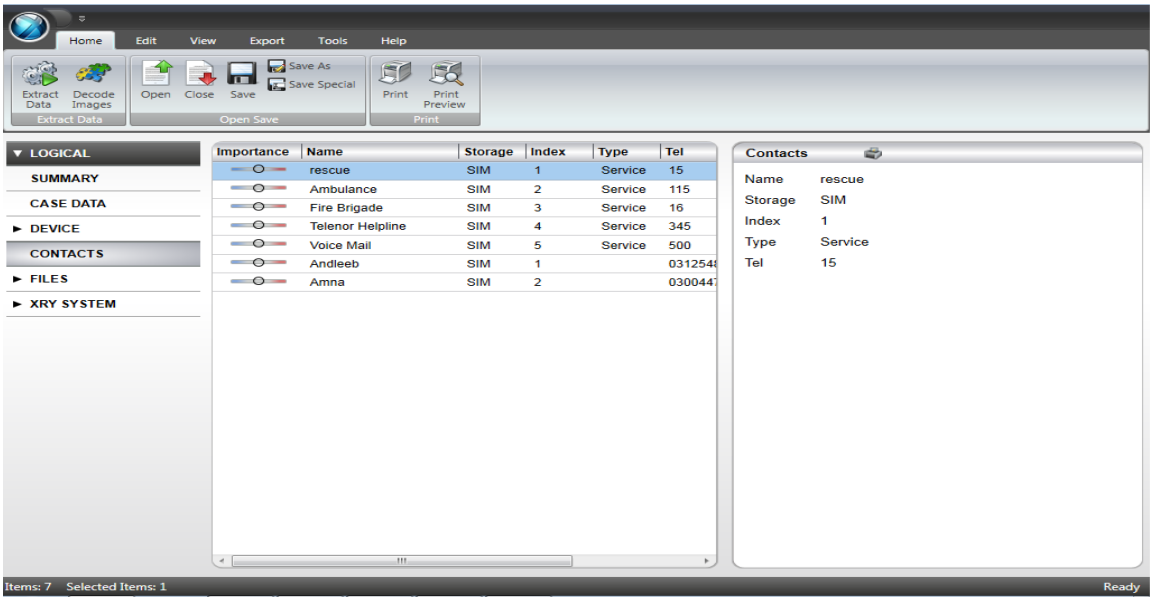


Figure 4.4: Name *police* Replaced by *rescue* (Test case: Case File Data Protection)

See Table 4.5 below for more details.

Table 4.5: Universal Integrated Circuit Cards

XRY v6.7		
Test Cases – UICC Acquisition		*Universal Integrated Circuit Card*
Connectivity	Non Disrupted	*As Expected*
	Disrupted	*As Expected*
Equipment/ User Data	Service Provider Name (SPN)	*As Expected*
	ICCID	*As Expected*
	IMSI	*As Expected*
	MSISDN	***Not As Expected***
PIM Data	Abbreviated Dialing Numbers (ADNs)	*As Expected*

	Last Numbers Dialed (LNDs)	*As Expected*
	SMS Messages	*As Expected*
	EMS Messages	*As Expected*
Location Related Data	LOCI	*As Expected*
	GPRSLOCI	*As Expected*
Acquisition	Acquire All	*As Expected*
	Selected All	*As Expected*
	Select Individual	*As Expected*
Case File Data Protection	Modify Case Data	***Not As Expected***
Password Protected SIM Acquire	Acquisition of Protected SIM	*As Expected*
PIN/PUK Attempts	PIN attempts reported	*As Expected*
	PUK attempts reported	*As Expected*
Non-ASCII Character	Non-ASCII characters	*As Expected*
Hashing	Hashes reported for acquired data objects	*As Expected*

4.7 Summary

The chapter has illustrated that mostly all the expected results for the executed tests using iPad1 and UICC were achieved. However, few anomalies were also observed and properly documented in this chapter. This chapter concludes that keeping in view the mentioned anomalies, XRY v 6.7 can be used for the forensic investigations where the evidences (target devices) are iPad1 and UICC.

Chapter 5

iPad Forensics Using Commercial Tool

5.1 Introduction

The chapter describes the various steps and ways in which artifacts of iPad have been acquired using a commercial tool. The various ways are single logical extraction, single physical extraction, followed by consecutive logical and consecutive physical extractions using XRY Complete. Moreover, the chapter discusses the detail of acquired XRY files and the artifacts associated with/residing in each file.

5.2 Acquisition

XRY Complete is a commercial hardware/software based tool manufactured by Micro Systemation (MSAB). It recovers live and deleted data from mobile devices in a forensically secure manner [16, 17]. XRY logical and XRY physical collectively make XRY Complete.

5.2.1 XRY Logical and XRY Physical

XRY logical retrieves live data whereas XRY physical recovers deleted data from a mobile device. For this, the iPad and XRY was mounted to a Windows 7 machine installed with XRY Complete. Logical and physical extraction was performed respectively via XRY. Steps to carry out each extraction are given in Table 5.1. The tool provides XRY logical and XRY physical files (.xry) containing numerous artifacts. Details of the artifacts are discussed in section 5.3.

Table 5.1: Data Acquisition Steps

Steps	**Description**
1.	Open XRY interface
2.	Click on *Extract data* button
3.	Select device (i.e. iPad)
4.	Click on *logical* or *physical* extraction button according to the requirement
5.	Create file name and set path where file will be saved.
6.	Turn off iPad by pressing power button on the top.
7.	Press start and power button simultaneously.

8.	Release power button as screen appears black.
9.	Keep pressing home button till XRY logo appears on the screen of iPad.
10.	XRY logo indicates that extraction has been started.
11.	After the completion of acquisition process, the iPad displays home screen.

Moreover, five repeated logical and then physical extractions were performed on an iPad using XRY Complete. Each created XRY file (.xry) was separately logged. Details related to the generated XRY files are discussed in section 5.3.

5.3 Examination and Analysis

Examination: The file created by either XRY logical or XRY physical have same format i.e., .xry. Each created .xry file is opened with and readable in XRY reader/software.

Analysis: XRY software shows that each created file (.xry) contains various segments. These segments are *Summary, Case Data, Device, Contacts, Calendar, Messages, Locations, Web, Files and XRY System*. All these segments are further subdivided into several sections. Sections contain artifacts related to that particular section. Each artifact can be studied and printed. However, files/artifacts associated with each section (like *Pictures, Audio, Videos, Documents, Archives, Databases and Unrecognized)* of *File* Segment have an option to print, save on the workstation and launch it in XRY software.

XRY Logical

Three out of four application documents were found in XRY logical extraction. Hash values for these three documents were computed and recorded. The application documents acquired in logical extraction were .doc, .ppt and .xlx files. And the application document that was not acquired in logical extraction was .pdf file as shown in figure 5.1.

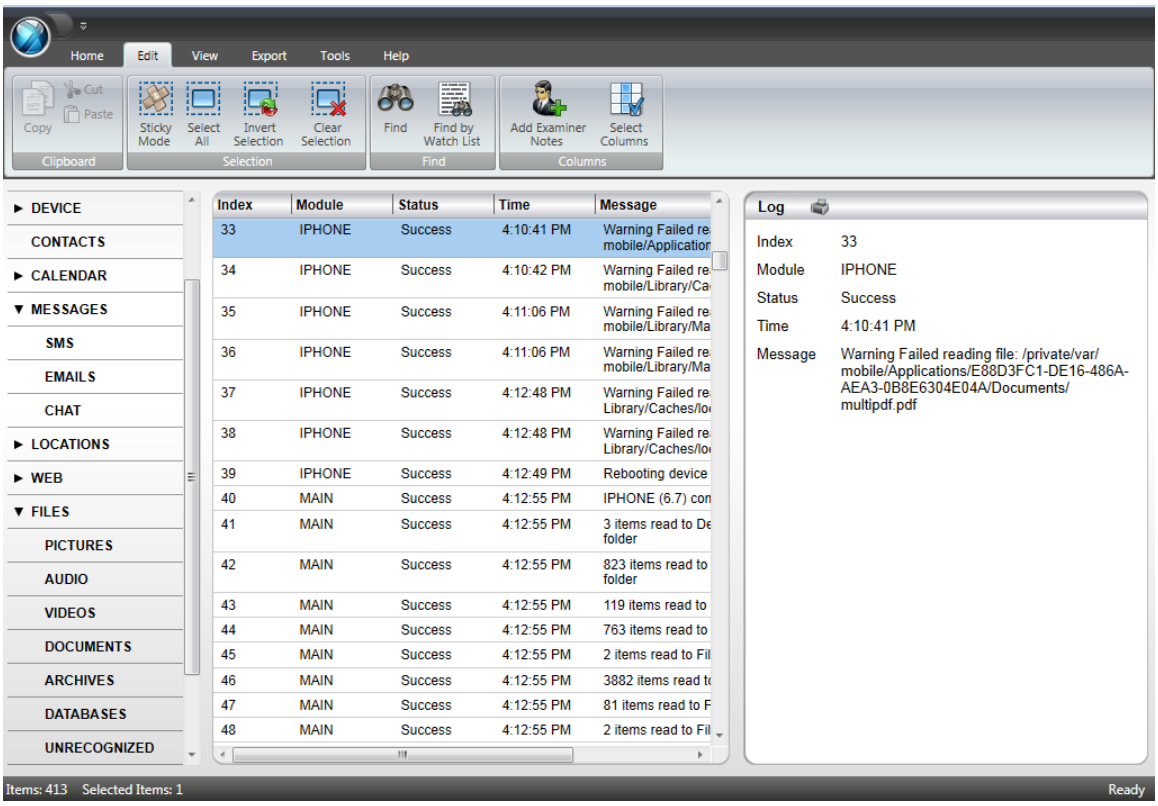


Figure 5.1: XRY Logical Failed to Read .pdf File

Consecutive XRY Logical or XRY Physical

In consecutive extractions, it was noticed that each XRY file varied in size (bytes) from another. Size of first XRY file varied from next file either by increase or decrease of bytes as shown in figure 5.2.

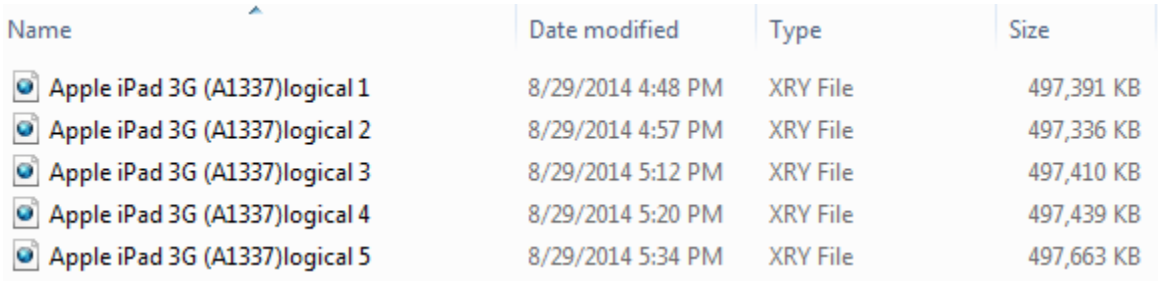


Figure 5.2: File Size Variation in Consecutive XRY Logical Extractions

To explore the differences, data of each XRY file was compared by opening the files in XRY software. In comparison, some variations were seen in terms of size, created time, modified time or accessed time of files in a particular XRY file. These changes

compelled authors to calculate hash values of modified files. Hash values were found to differ as per the anticipation. Table 5.2 shows the files which were altered and have different hash values in XRY logical or physical acquisition process.

Table 5.2: Modified Files in XRY Acquisition Process

File Name	Logical Acquisition File Path	Physical Acquisition File path
fseventsd-uuid	/private/var/tmp/	Data/tmp
Csidata	/private/var/wireless/Library/Preferences/	Data/wireless/Library/Preferences
restore.log	/private/var/MobileSoftwareUpdate/	Data/MobileSoftwareUpdate
backup_keys_cache.db	/private/var/keybags/	Data/keybags
general.log	/private/var/logs/AppleSupport/	Data/logs/AppleSupport
keybagd.log	/private/var/logs/	Data/logs
lockdownd.log	/private/var/logs	Data/logs
config.xml	/private/var/mobile/Applications/A5185C57-F396-4E70-8289-3A9802F4E0AA/Library/Application Support/Skype/live#3aperson_abc/	Data/mobile/Applications/ A5185C57-F396-4E70-8289-3A9802F4E0AA /Library/Application Support/Skype/live#3aperson_abc
shared.xml	/private/var/mobile/Applications/A5185C57-F396-4E70-8289-3A9802F4E0AA/Library/Application Support/Skype/	Data/mobile/Applications/A5185C57-F396-4E70-8289-3A9802F4E0AA/Library/Application Support/Skype
com.apple.timed.plist	/private/var/mobile/Library/Cache/	Data/mobile/Library/Caches
Cache.db	/private/var/mobile/Applications/A5185C57-F396-4E70-8289-3A9802F4E0AA /Library/Caches/com.skype.SkypeForiPad/	Data/mobile/Applications/A5185C57-F396-4E70-8289-3A9802F4E0AA /Library/Caches/com.skype.SkypeForiPad
AddressBook.sqlitedb	/private/var/mobile/Library/AddressBook/	Data/mobile/Library/AddressBook
ADDataStore.sqlitedb	/private/var/mobile/Library/AggregateDictionary/	Data/mobile/Library/AggregateDictionary
com.apple.AutoWake.plist	/private/var/preferences/SystemConfiguration	Data/preferences/SystemConfiguration
com.skype.SkypeForiPad.plist	/private/var/mobile/Applications/A5185C57-F396-4E70-8289-3A9802F4E0AA/Library/Preferences/	Data/mobile/Applications /A5185C57-F396-4E70-8289-3A9802F4E0AA /Library/Preferences
Cache.db	/private/var/mobile/Library/Caches/com.apple.aosnotifyd/	Data/mobile/Library/Caches/com.apple.aosnotifyd
Cache.db	/private/var/mobile/Library/Caches/com.apple.dataaccess.dataaccessd/	Data/mobile/Library/Caches/com.apple.dataaccess.dataaccessd
store.db	/private/var/mobile/Library/Caches/com.apple.keyboards/	------
Cache.db	/private/var/mobile/Library/Caches/com.apple.springboard/	Data/mobile/Library/Caches/com.apple.springboard
Envelope Index	/private/var/mobile/Library/Mail/	Data/mobile/Library/Mail
sms.db-shm	/private/var/mobile/Library/SMS/	Data/mobile/Library/SMS
sms.db-wal	/private/var/mobile/Library/SMS/	Data/mobile/Library/SMS
downloads.28.sqlitedb	/private/var/mobile/Media/Downloads/	Data/mobile/Media/Downloads
Photos.sqlite-shm	/private/var/mobile/Media/PhotoData/	------
cache_encryptedA.db	-------	Data/root/Library/Caches/location
lockCache_encryptedA.db	-------	Data/root/Library/Caches/location
glgps_nvs.bin	-------	Data/root/Library/Caches/location

Moreover, each XRY file contained one additional file as compared from the previous extracted XRY file. However there was no such file found in first created XRY

file. This file is a *ResetCounter.plist* found at /private/var/logs/CrashReporter/ or Data/log s/CrashReporter. Difference in hash values was detected, which was the consequence of different string value assigned to *Incident Identifier* preset in *ResetCounter.plist* file. The ResetCounter.plist was created on a specific location each and every time the iPad was restarted after XRY extraction. For example figure 9 shows that *ResetCounter-2014-02-01-160422* was found in second logical extraction. This means that the file was created when the iPad was restarted after the completion of first XRY logical extraction. *2014-02-01* represents the creation date and *160422* is some random number assigned to the file.

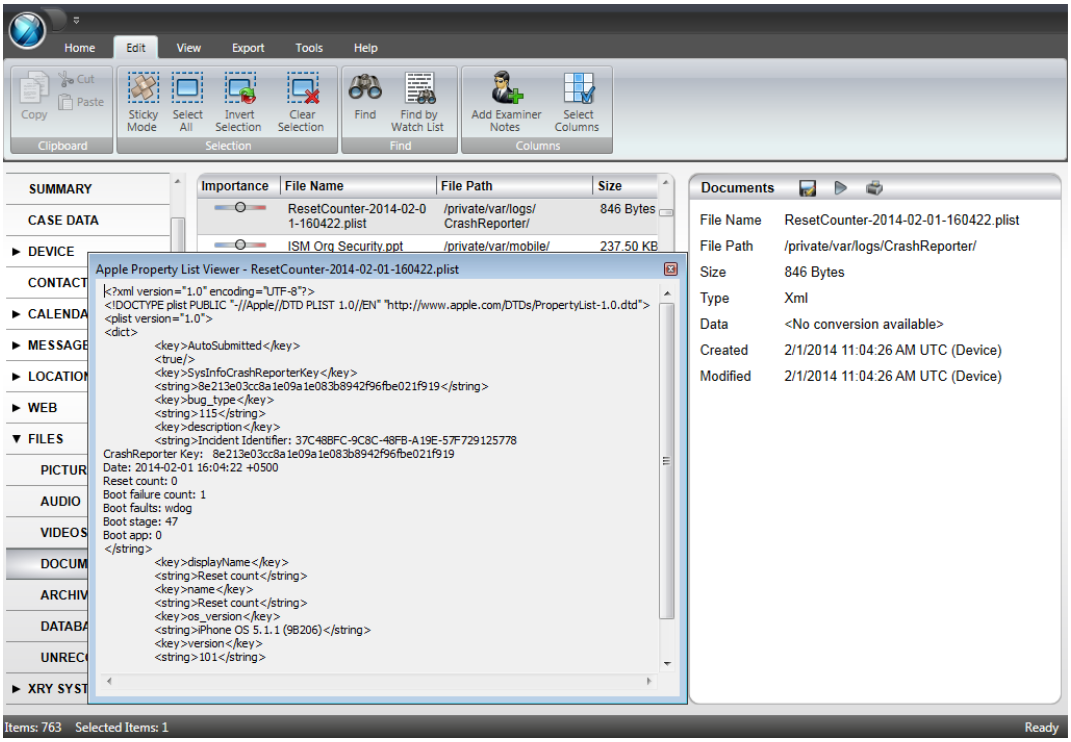


Figure 5.3: *ResetCounter.plist* found in second logical extraction

Another interesting fact was observed in consecutive logical and physical extractions i.e. in each successful or non-successful extraction *Skype* application and *Mail* application of iPad are being accessed by XRY Complete. Non successful extraction is one in which acquisition accidently stops either due to power failure or any other reason. It was observed in each XRY created file that access count for *com.skype.SkypeForiPad* and *com.apple.mobilemail* is increased by 1 value from the previous successful extraction. See figure 5.4.

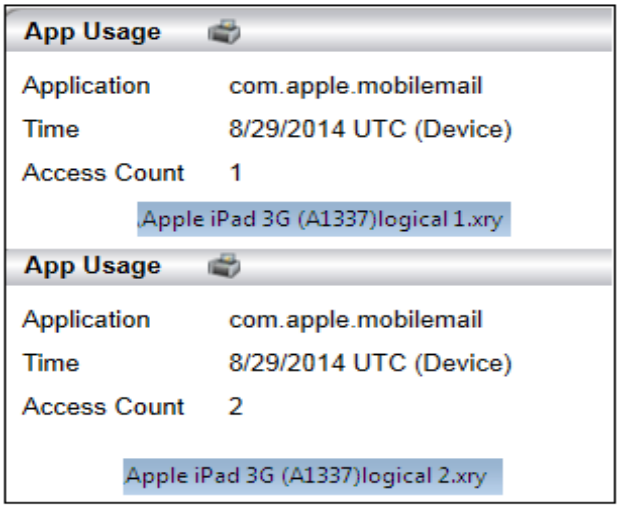


Figure 5.4: Access Count Incremented in Second Logical Extraction

Moreover, the analysis determined that additional files were found in some XRY files when consecutive logical/physical extractions were performed. Table 5.3 clearly shows additional files present in various logical extractions. Table also displays whether the particular file has same hash value in the residing XRY logical files.

Table 5.3: Additional Files in Consecutive XRY Logical Acquisition

File Name	File Size	File Path	Logical					Difference in Hash Values
			1	2	3	4	5	
000000000000206c	1.20 KB	/private/var/.fseventsd/		✓	✓	✓	✓	✓
0000000000001ea4	1.05 KB	/private/var/.fseventsd/			✓	✓	✓	✓
0000000000002201	1.16 KB	/private/var/.fseventsd/			✓	✓	✓	✓
00000000000020f8	1.13 KB	/private/var/.fseventsd/				✓	✓	✓
00000000000022fb	1.10 KB	/private/var/.fseventsd/					✓	
3845961891	28.00 KB	/private/var/mobile/Library/ Caches/com.apple.keyboards /images/		✓	✓	✓	✓	✓
0000000000002a9d	0 Bytes	/private/var/tmp/	✓					
000000000000206d	0 Bytes	/private/var/tmp/		✓				
0000000000001ea5	0 Bytes	/private/var/tmp/			✓			
00000000000020f9	0 Bytes	/private/var/tmp/				✓		
00000000000022fc	0 Bytes	/private/var/tmp/					✓	
Changes	4 KB	/private/var/mobile /Media/PhotoData/	✓					
changes-wal	84.52 KB	/private/var/mobile /Media/PhotoData/	✓					
shaders.data	24.00 KB (1) , 12.00 KB (3), 12.00 KB (4), 12.00 KB (5)	/private/var/mobile/ Library/Caches/com.apple. springboard/com.apple.opengl/	✓		✓	✓	✓	✓
shaders.maps	2.00 KB (1) , 1.00 KB (3), 1.00 KB (4), 1.50 KB (5)	/private/var/mobile/ Library/Caches/com.apple. springboard/com.apple.opengl/	✓		✓	✓	✓	✓

Similarly, Table 5.4 displays additional files present in various physical extractions. Table also displays whether the particular file has same hash value in the residing XRY physical files.

Table 5.4: Additional Files in Consecutive XRY Physical Acquisition

File Name	File Path	File Size	Physical					Difference in Hash Values
			1	2	3	4	5	
shaders.data	Data/mobile/Library/Caches/ com.apple.springboard/com.apple.opengl	12KB	✓	✓	✓	✓		✓
shaders.maps	Data/mobile/Library/Caches/ com.apple.springboard/com.apple.opengl	1.00 KB	✓	✓	✓	✓		✓
queue.lock	Data/mobile/Applications/ A5185C57-F396-4E70-8289-3A9802F4E0AA/Library/Application Support/Skype/shared_httpfe	0 Bytes					✓	
0000000000001fea	Data/tmp	0 Bytes	✓					
0000000000001dba	Data/tmp	0 Bytes		✓				
0000000000001d6d	Data/tmp	0 Bytes			✓			
0000000000001ebc	Data/tmp	0 Bytes				✓		
0000000000001fd7	Data/tmp	0 Bytes					✓	
lockdownd.log.1	Data/logs	128.04 KB				✓	✓	
0000000000001db9	Data/.fseventsd	1.13 KB		✓	✓	✓	✓	
0000000000002089	Data/.fseventsd	1.16 KB		✓	✓	✓	✓	
00000000000018cc	Data/.fseventsd	1.02 KB			✓	✓	✓	
0000000000001d6c	Data/.fseventsd	1.13 KB			✓	✓	✓	
0000000000027f1	Data/.fseventsd	1.12 KB			✓	✓	✓	
0000000000001ebb	Data/.fseventsd	1.10 KB				✓	✓	
0000000000001fce	Data/.fseventsd	1.11 KB				✓	✓	
0000000000002014	Data/.fseventsd	1.12 KB				✓	✓	
0000000000001fd6	Data/.fseventsd	1.12 KB					✓	
log-bb-2014-08-29-stats.txt	Data/wireless/Library/Logs/ Baseband	180 Bytes		✓	✓	✓	✓	
log-aggregated-2014-08-29-000000_MJ's iPad.plist	Data/mobile/Library/Logs/ CrashReporter	6.20 KB			✓	✓	✓	

5.4 Summary

The chapter has explained the data acquisition from iPad using a commercial tool. The chapter has also discussed the artifacts of iPad acquired via single XRY logical and physical acquisition. Moreover, various changes observed in consecutive XRY logical and physical extractions are thoroughly listed in this chapter.

Chapter 6

iPad Forensics Using OS Utilities and Freeware

6.1 Introduction

The chapter explains how data of iPad has been acquired using few freely available techniques. These techniques are various OS utilities (windows 7 and Ubuntu), a freeware (libimobiledevice) and a jailbreak method. The artifacts of iPad attained via each technique are properly logged in this chapter. Furthermore, the chapter examines and analyses the acquired results in detail.

6.2 Acquisition

Data was acquired from iPad using following different tools and techniques.

6.2.1 OS Utilities

Windows 7: It is an operating system developed by Microsoft**.** In this investigation, iPad was first attached to Microsoft Windows 7 machine. It was recognized as a portable device.

Ubuntu: It is a Debian-based Linux operating system, made-up of numerous software packages. Most of the packages are freeware. Till date many Ubuntu versions have been released [18]. The iPad was mounted in a default option of read/write mode to Ubuntu 12.04.3 LTS operating system.

6.2.2 Freeware

libimobiledevice is a free software library which communicates to Apple devices natively and accesses file system without jail breaking a device [19]. libimobiledevice is an open source tool present in Santoku which is used for live data acquisition from iPad. Santoku is an open source platform, based on Linux environment and includes features like development tools, Penetration testing, Wireless analyzers, Device forensics and Reverse engineering [20].

To get live data using libimobiledevice on Santuko, iPad was first connected to Santoku. Then the connectivity between iPad and Santuko was checked; backup of device was created and the backup file was extracted (unback) in order to make it

browse-able. These three steps were performed by running commands in terminal window of libimobiledevice [21].

6.2.3 Jailbreak

To get full access/image, the iPad was jailbroken using RedSn0w [22, 23]. Table 6.1 illustrates the steps required to jailbreak the iPad.

Table 6.1: Steps for Jailbreaking iPad

Steps	Description
1.	Download Redsn0w [24] on workstation
2.	Open Redsn0w
3.	Click *Jailbreak* button
4.	Plug iPad to workstation and make sure it's off
5.	Click *next* button
6.	Follow the steps given on the screen of RedSn0w to enter DFU mode
7.	After performing those steps iPad will reboot
8.	Then jailbreak data will be prepared by RedSn0w. Select *Cydia* and click *Next*
9.	iPad will be rebooted again. And RedSn0w will start uploading the new RAM Disk and Kernel.
10.	Once uploading is completed, you will be informed that RedSn0w is done. iPad will be jailbroken with Cydia on the SpringBoard when iPad finishes rebooting.

After jailbreaking iPad, the device was imaged using numerous steps mentioned in Table 6.2.

Table 6.2: Steps for Imaging iPad

Steps	Description
1.	Open *Cydia* on iPad
2.	Check if SSH port already exists
3.	If SSH port doesn't exist, then enable Wi-Fi and install SSH port
4.	Now connect iPad to linux installed workstation and forensics USB Bridge. See figure 6.1 and figure 6.2 for details. (The iPad was connected to forensic bridge for forensically secure imaging)
5.	Make sure that workstation is connected to WiFi
6.	Open command prompt and run the following command: ssh root@[iPad ip] dd if=/dev/rdisk0 bs=1M | dd of=ios-root.img This command will create an image of iPad

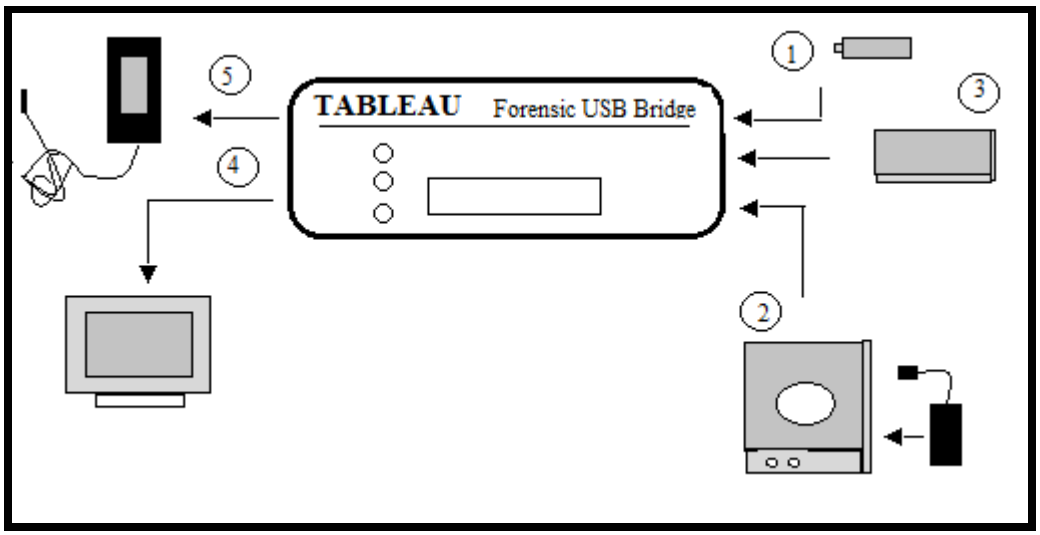


Figure 6.1: Device Connection Diagram

1. USB Mass Storage Device
Device can be directly connected to T8-R2 USB 1.1/2.0 connector

2. External USB Disk Drive
Use the appropriate cable for the USB drive that will be imaged

3. Media Cards
- Connect appropriate media reader to T8-R2
- USB 1.1/2.0 connector Insert media/flash cards into media reader

4. Host Connection
TC7-6-6 FireWire cable
TC8 USB cable

5. Power (DC In)
TP2 cable
(5-pin DIN)

Figure 6.2: Connection Recommendations

However few shortcomings were encountered while imaging the iPad. Firstly, the Forensic USB Bridge (write blocker) available in the lab did not support iPad. Though, it did provide support to iPod as shown in figure 6.3 and figure 6.4. Make and Model of the write blocker are mentioned in Table 6.3

Table 6.3: Specifics of Forensic USB Bridge

Device	Details
Forensic USB Bridge	Make: TABLEAU Model: T8-R2 S/N: 1208A01D 1413

Figure 6.3: Device Detect LED of Forensic USB Bridge does not Give Steady Illumination when Connected to iPad.

Figure 6.4: Device Detect LED of Forensic USB Bridge Gives Steady Illumination when Connected to iPod.

Secondly imaging a 64 gb device using dd command is a slow process and hence requires time. In order to take complete image of iPad, continuous power supply and internet connection were needed. However due to electricity breakdown in our country, imaging of 64 gb iPad was not possible.

So, to overcome these issues related to imaging, below mentioned technique was used to get full access of iPad's folders in short period of time.

6.2.4 iBrowse

iBrowse is a simple application that allows the workstation to access file system of an iOS device. Various steps to install iBrowse and utilize iPad's folders are mentioned in Table 6.4.

Table 6.4: Steps to Acquire iPad's Folder via iBrowse

Steps	Description
1.	Download *iBrowse* from the particular website [25] on the workstation.
2.	Run and install *iBrowse*
3.	Make sure iTunes is installed on the workstation and the iPad is jailbroken inorder to get access to all folders
4.	Connect iPad to the workstation and then open *iBrowse*
5.	Now you can access iPad's app, media and root folders

6.3 Examination and Analysis

6.3.1 Windows 7

Only the DCIM folder was visible to the examiner at Windows platform. DCIM folder contains pictures stored in the iPad. These pictures were acquired and hash values of each picture were recorded.

6.3.2 Ubuntu

At Ubuntu platform two different volumes were displayed: first volume was 'MJ's iPad' and second volume was 'Documents on MJ's iPad'. In actual practice data resides in various iPad's directories. One such directory which holds user data is /var/mobile/Media. Another directory which contains application documents is /var/mobile/Applications/{Identifier}/Documents. Artifacts associated with both these directories were found when iPad was mounted to Ubuntu machine. User's Video's, Podcast's, Book's, Download's, Photo's, iTunes Data, Purchase's and Music exists in

/var/mobile/Media directory. Documents residing in applications like Adobe Reader and FileManager applications resides in /mobile/Applications/{Identifier}/Documents. All these artifacts are a valuable source of evidence for forensic examination.

Ubuntu gave access to many folders, populated with various files. Figure 6.5 shows the volume named MJ's iPad, which contains 12 folders. Out of these 12 folders, 6 folders: Airfair, Books, DCIM, iTunes_Control, PhotoData and PhotoStreamsData, are further subdivided. All folders are populated with files of different types. Figure 6.6 shows another volume named "Documents on MJ's iPad". This contains several applications. Each application has a subfolder containing documents of different types.

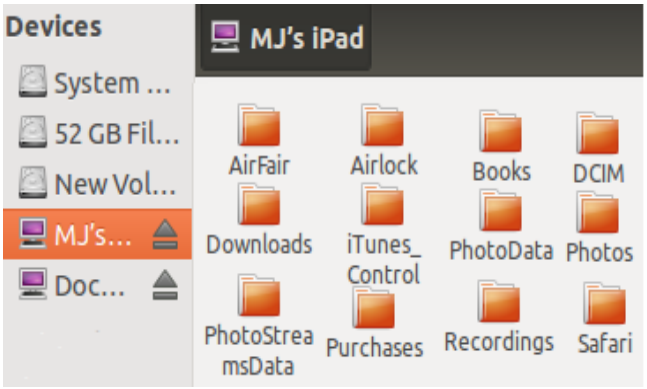


Figure 6.5: iPad's User Data Found via Ubuntu Machine

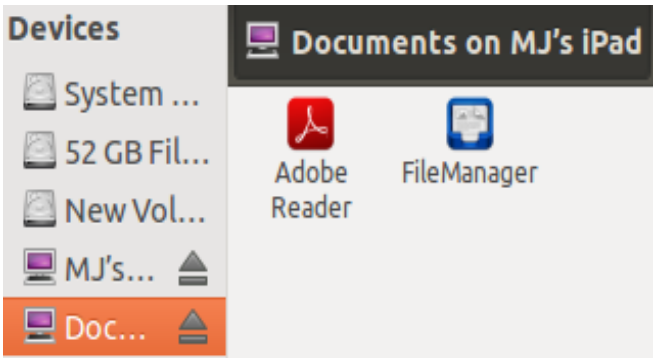


Figure 6.6: iPad's Application Documents Found via Ubuntu Machine

In this investigation, total 90 files were obtained from first volume and 4 documents were obtained from second volume. Table 6.4 shows the path of main folders and the different types of files residing in each relevant folder. In an effort to check data authenticity, hash values of each file were separately logged. The files with extensions like, Jpeg, Png, Tiff, Blob, Mp4, Mp3, Xml, Binary Plist, SQLite, SQLite Shared Memory,

SQLite Write-Ahead Log, pdf, .docx, .ppt, .xlsx. are forensically important. Files like property list (plist) and SQLite database were also found in Media folder. Plist are Xml manifests, stores valuable data related to iDevice applications such as Preferences, Accounts, Bookmarks, System Configuration, Web Clips along with history of Google maps and Safari. SQLite database file mainly stores user's data like voice mails, SMS and E-mail messages, calendar events, call history, notes, photos, address and Google maps data. [1].

Table 6.5: List of File Types Acquired from Ubuntu Platform

Path	**Type**
/var/mobile/Media/Books/	➢ SQLite
/var/mobile/Media/DCIM/	➢ Jpeg ➢ Png
/var/mobile/Media/Downloads/	➢ SQLite
/var/mobile/Media /iTunes_Control/	➢ Blob ➢ Jpeg ➢ Mp4 ➢ Mp3
/var/mobile/Media /PhotoData/	➢ Blob ➢ Xml ➢ Tiff ➢ Jpeg ➢ SQLite ➢ SQLite Shared Memory ➢ SQLite Write-Ahead Log
/var/mobile/Media/Photos/	➢ Binary PList
/var/mobile/Media/PhotoStreamsData/	➢ Xml ➢ Binary PList ➢ Png ➢ Jpeg
/var/mobile/Media/Safari/	➢ SQLite
/var/mobile/Applications/{Identifier}/DOcuments	➢ .pdf ➢ .docx ➢ .ppt ➢ .xlsx

6.3.3 libimobiledevice

When unback operation was executed, numerous folders named Keychains, Managed Preferences, Mobile, MobileDevice, Root and Wireless were obtained. Each folder contains various files. Hash values of 197 files were extracted and separately logged.

6.3.4 iBrowse

iBrowse gave access to *Apps, Media* and *Root* folder of iPad. These folders contain various subfolders and files. Data related to user installed applications is present in *App* folder. All user data resides in *Media* folder. System data and system settings exist in *Root* folder.

In this research, *Apps* folder contains 4 folders i.e. *Adobe Reader*, *FileManager*, *Skype* and *Temple Run.* All these folders depict user installed applications. These 4 folders contain several subfolders and files related to user installed applications. *Media* folder contains 8 folders i.e. *Books, DCIM, Downloads, HackStore, iTunes_Control, jb_install, PhotoData* and *Recordings*. *Root* folders includes 19 folders like *.fseventsd, .Trashes, Applications, bin, boot, cores, dev, Developer, etc, lib, Library, mnt, private, sbin, System, tmp, User, usr and var.* Out of these 19 folders, 7 folders has no data. These empty folders are *.Trashes, boot, cores, Developer, lib, mnt and var.*

Except for the empty folders mentioned above, all the above mentioned folders (of *Apps, Media* and *Root* Folders) contain numerous subfolders and files. Hash values of each file was calculated and recorded.

6.4 Summary

The chapter has stated several freely available techniques to acquire data from iPad. The chapter has also thoroughly illustrated the setup procedure for each data acquisition technique. Furthermore, the artifacts acquired using OS utilities, a freeware and the jail break technique have been precisely noted, explained and analyzed in this chapter.

Chapter 7

Comparison of Results and Discussion

7.1 Introduction

The chapter compares the artifacts acquired from open source forensic tools with the artifacts acquired from a commercial tool. The chapter also analyzes the changes/modifications for difference in hash values for same artifact acquired via different forensics techniques. Moreover the chapter advises which tool can be used in a specific circumstance while keeping in view the shortcomings of the tool.

7.2 Comparison

In this research iOS version 5.1.1 has been considered with the aim of discovering a reliable acquisition method for /var/mobile/Media directory files, /var/mobile/ Applications directory documents and folders like *Keychains, Mobile, Preferences, Root* and *Wireless*; these folders contain user data and application related information which is important for a forensic investigation. By recognizing particular directory and comprehending what it holds via the proposed methods, the practice of collecting artifacts can begin directly as we have verified the data authenticity by computing the hash values. Acquired artifacts and their hash values are recorded on DVD. Table 7.1 describes miscellaneous folders containing artifacts, obtained from various acquisition techniques. Table 7.2 shows hash values of some user data files acquired through various data acquisition techniques.

Table 7.1: Comparison of Folders Obtained from Various Acquisition Methods

Microsoft Windows 7	**Ubuntu 12.04.3 LTS**	**Libimobiledevice**	**iBrowse**
- DCIM	- AirFair - AirLock - Books - DCIM - Downloads - iTunes_Controls - PhotoData - Photos - PhotoStreamsData - Purchases - Recordings - Safari - Application Documents.	- Keychains -Managed Preferences - Mobile - MobileDevice - Root - wireless	- App - Media - Root

Table 7.2: Hash Values of User Files Obtained from Various Acquisition Methods

File Name	File Type	Acquisition Method	Hash Values	
			MD5	SHA256
IMG_0001	.PNG	Microsoft Windows 7	D30B23352CA86888 3C7677B290B2D8EA	18B32F812A81456BA78F8 2431275AC70EBF5CAA9B 1233F23A514B0ADC7F32178
		Ubuntu 12.04.3 LTS		
		Libimobiledevice		
		iBrowse		
		XRY Complete		
Contacts	.xlsx	Ubuntu 12.04.3 LTS	7671BC8B28D0744F 5715BC382F8349D7	48B32F836A81456C45AF4 B431273CB70EBF5CBB9C 7263F22A554A0ADC7F32027
		Libimobiledevice		
		iBrowse		
		XRY Complete		

Investigation determined that all iPad's artifacts acquired from MJ's iPad volume via Ubuntu platform have given same hash values when compared to the one extracted from XRY logical except from one file named *downloads.28.sqlite*. This particular database comprises of various known tables [26]. As shown in Table 7.3, *persistent_manager_kind* table was found to differ in each extraction process. Three fields that are *pid*, *manager_id* and *download_kind* reside within *persistent_manager_kind* table.

Analysis determined that integrity of *downloads.28.sqlite* file was compromised because of the changes in data entry of certain fields that are *pid* and *download_kind*. Table 7.3 shows that in every extraction two changes were observed. One is that a new *pid* was assigned against each *download_kind* data entry. Second, same thirteen data entries in *download_kind* field randomly changed position in each extraction process. It was thus concluded that whichever method is adopted, integrity of this file will certainly be compromised.

Table 7.3: Differences In *persistent_manager_kind* Table

Artifacts Acquired from Ubuntu Platform

Pid	manager_id	download_kind
-8697013296067968042	-3079926881866431783	videoPodcast
-7402569617997322243	-3079926881866431783	Book
-7329431502199691124	-3079926881866431783	Song
-6103358376161157882	-3079926881866431783	feature-movie
-1926500322170101766	-3079926881866431783	tv-episode
-843140266838312323	-3079926881866431783	Ebook
380133384971333366	6359578672334592279	Software
1965503006134192909	-3079926881866431783	Podcast
5210172721110099699	-3079926881866431783	Tone
5857462790415292211	-3079926881866431783	Ringtone
7441660511175830427	-3079926881866431783	Software
7875068394866816547	-3079926881866431783	music-video
7947198972459445051	-6895534963590278926	com.apple.MobileAsset

Artifacts Acquired from XRY

pid	manager_id	download_kind
-5096606683834414342	-3079926881866431783	tv-episode
-4519809471157545230	-3079926881866431783	videoPodcast
-4159226675442296094	-3079926881866431783	music-video
2396457548417753381	-3079926881866431783	Podcast
3765671117134938152	-3079926881866431783	feature-movie
3983873152646791978	-3079926881866431783	Software
5497865317862532018	6359578672334592279	Software
7155669364744334388	-3079926881866431783	Book
7514104786197330003	-3079926881866431783	Ringtone
7947198972459445051	-6895534963590278926	com.apple.MobileAsset
8304865426285548539	-3079926881866431783	Ebook
8884606758783125398	-3079926881866431783	Tone
9028490395618818294	-3079926881866431783	Song

Evaluating the results of libimobiledevice, 8 files out of 197 files have given different hash values from logical and physical XRY files. The 8 files are: com.apple.itunesstored.2.sqlitedb, sms.db, applicationstate.plist, com.apple.Accessibility. plist, com.apple.wifi.plist, clients.plist, com.apple.MobileSMS.plist, com.apple.spring board.plist. libimobiledevice compromised integrity of 3 files i.e. com.apple.itunesstored. 2.sqlitedb, sms.db and applicationstate.plist. However, XRY maintained integrity of these files. As all consecutive XRY extractions gave same hash values for these 3 files. Further, plists named com.apple.Accessibility, clients, cache, com.apple.wifi, com.apple.springboard, com.apple.atc.plist, com.apple.MobileSMS were found to give same hash values in every alternate extraction. This was observed for both, the freeware

and the commercial tool. Hence, concluding that integrity was not preserved for commercial tool as well as freeware.

Another significant thing was observed regarding the commercial tool. XRY logical failed to read the PDF document which was easily accessed from "Documents on MJ's iPad" volume via Ubuntu platform as shown in figure 7.1.

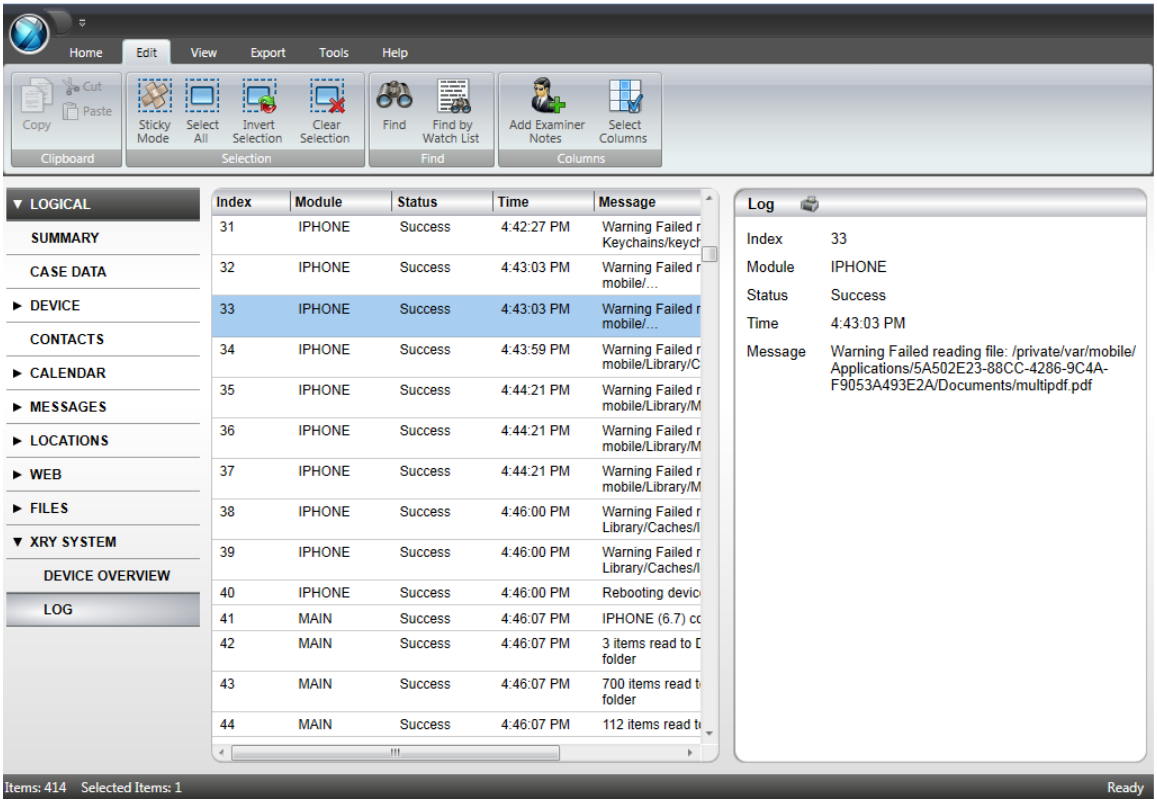


Figure 7.1: XRY Logical Failed to Retrieve Live .pdf Document from iPad

Moreover, analysis determined that all the artifacts attained from ibrowse method have given same hash values when compared to XRY logical. However, few changes were observed in *Media* and *Root* Folders achieved via ibrowse method. These changes were endless iteration and addition of few subfolders in *Media* and *Root* Folders. *Media* Folder contained few additional subfolders namely *HackStore* and *jb-install as shown in figure 7.2. Hackstore* contained 11 subfolders. Out of these 11 subfolders 4 subfolders were the same as present in *Media* Folder. These same subfolders were *DCIM, Downloads, PhotoData* and *PhotoStreamsData* as shown in figure 7.3. While, *jb-install* subfolder contained files related to jailbreaking as shown in figure 7.4.

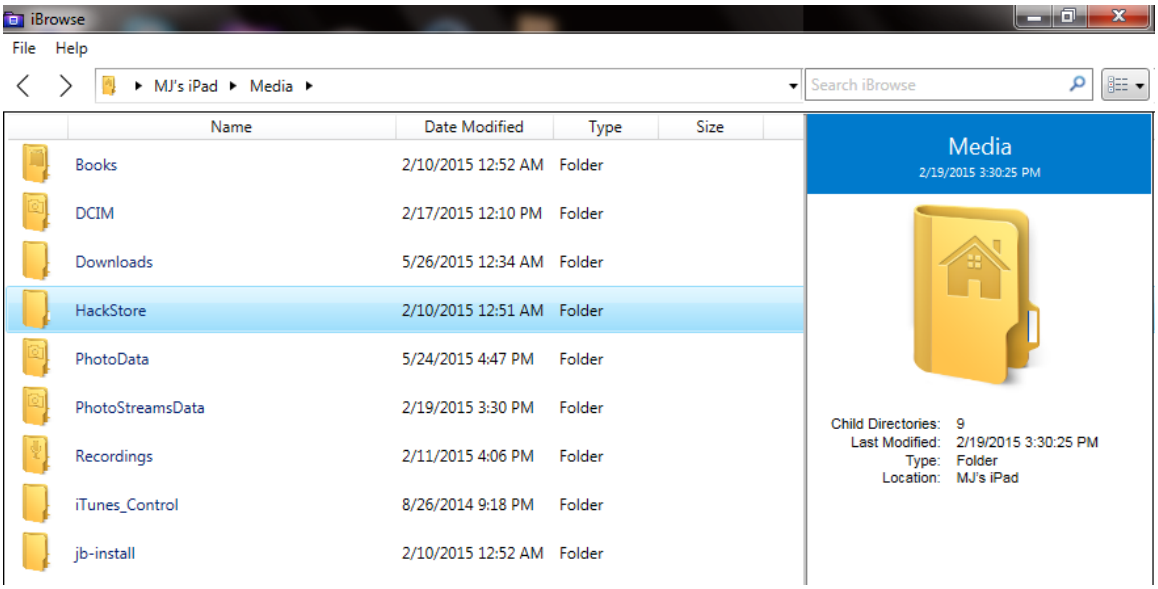


Figure 7.2: *Media* Folder Contained Few Additional Subfolders

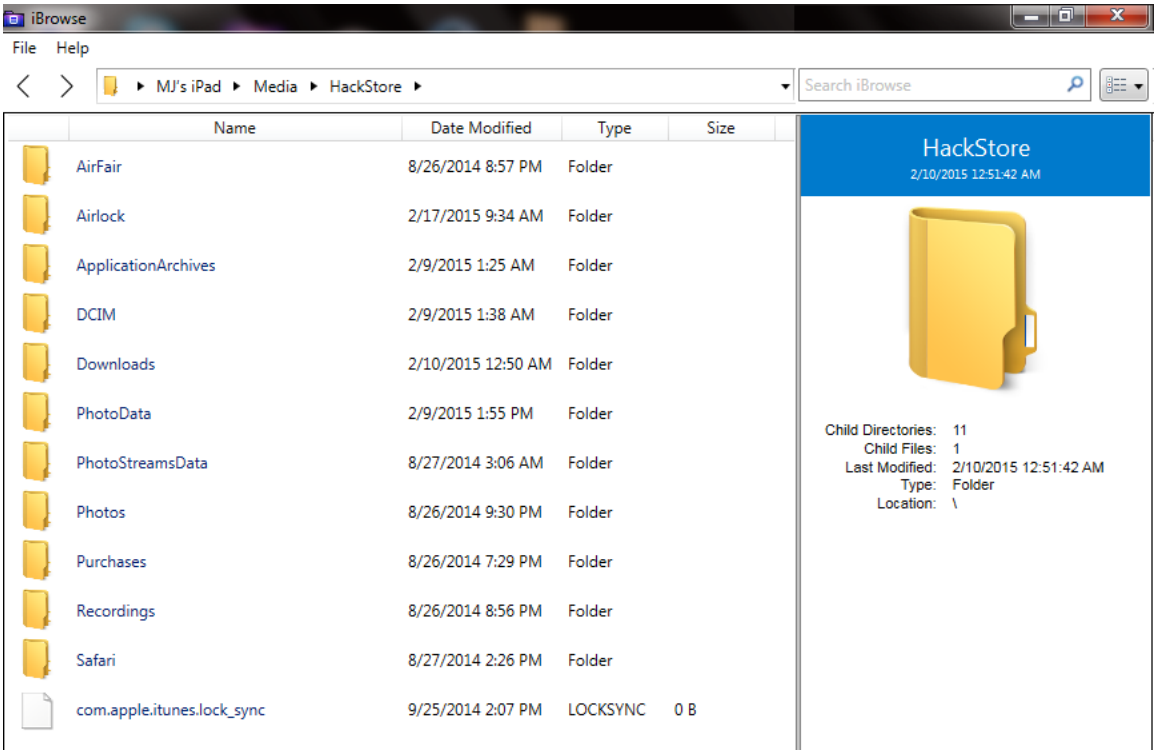


Figure 7.3: Hackstore Subfolder Comprised Few Similar Folders As Present in *Media* Folder

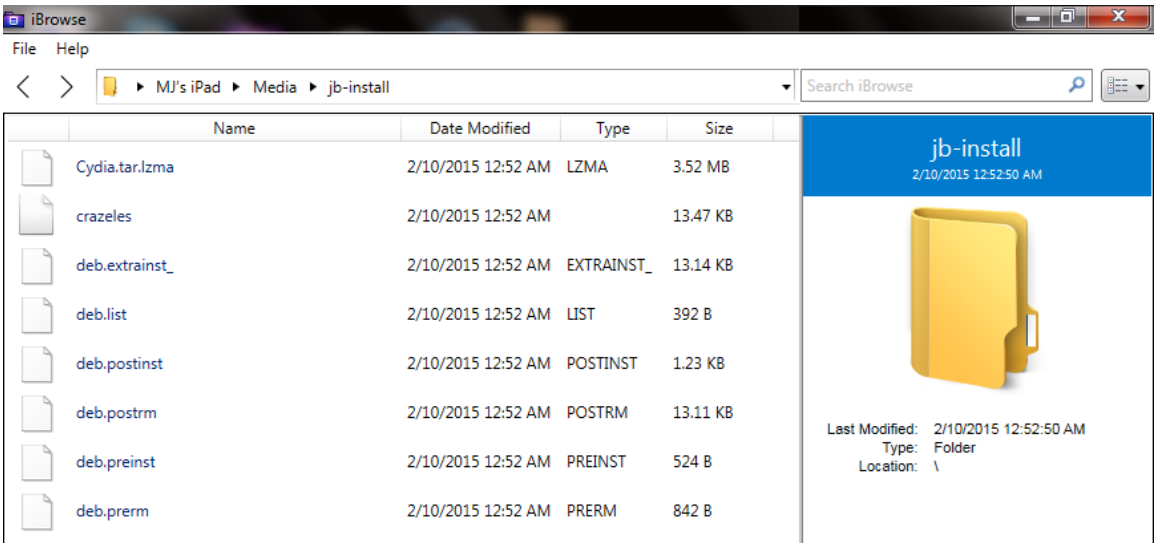


Figure 7.4: Various Files Related to Jailbreaking were Present in *jb-install*

Moreover, in *Media* folder endless iteration of *Books* subfolder was explored as shown in figure 7.5 and figure 7.6. *Books* subfolders contained various folders. Out of these numerous folders, *var* folder contains similar artifacts as present in *Media* folder.

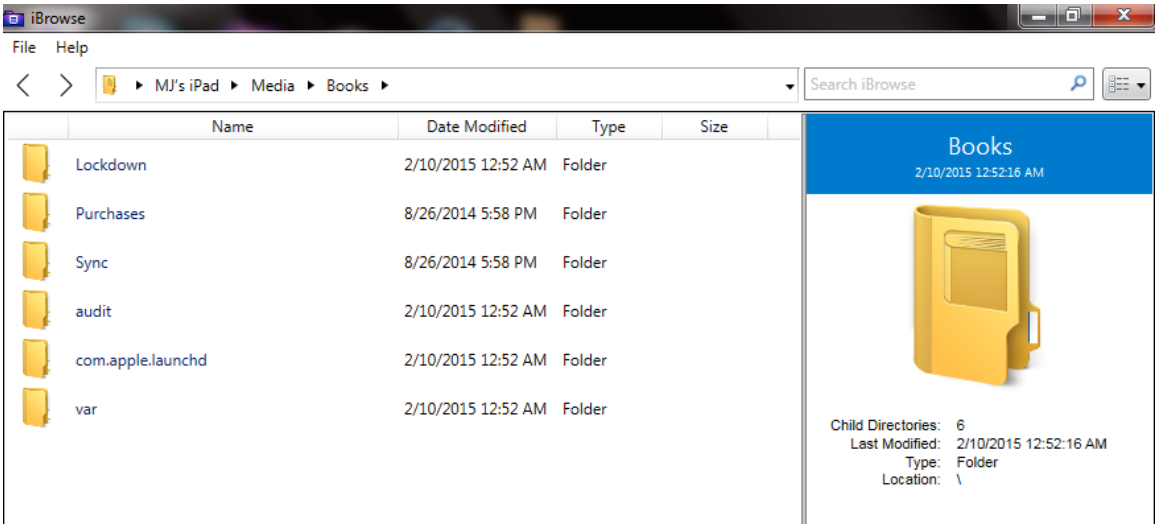


Figure 7.5: *Books* Subfolder Contained Various Folders

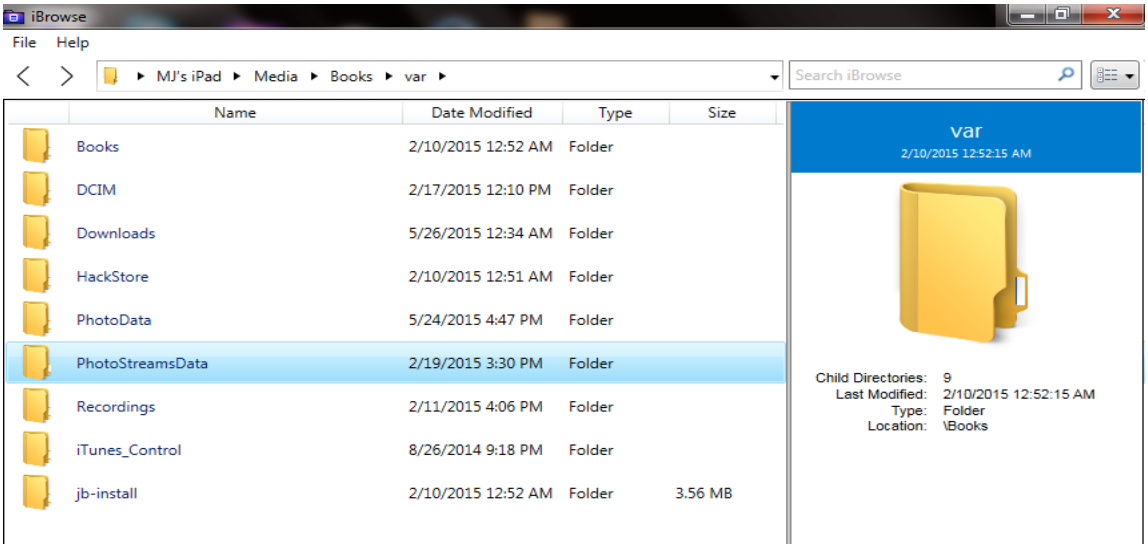


Figure 7.6: *var* Subfolder Contained Similar Artifacts as Associated with *Media* Folder and Artifacts of *Books* Subfolder were Infinitely Repeated.

Moreover, similar endless iterations were observed in few subfolders of *Root* Folder. These subfolders were *usr*, *var*, *User*, and *private*. Artifacts associated with these folders were infinitely repeated as shown in figure 7.7, figure 7.8, figure 7.9 and figure 7.10.

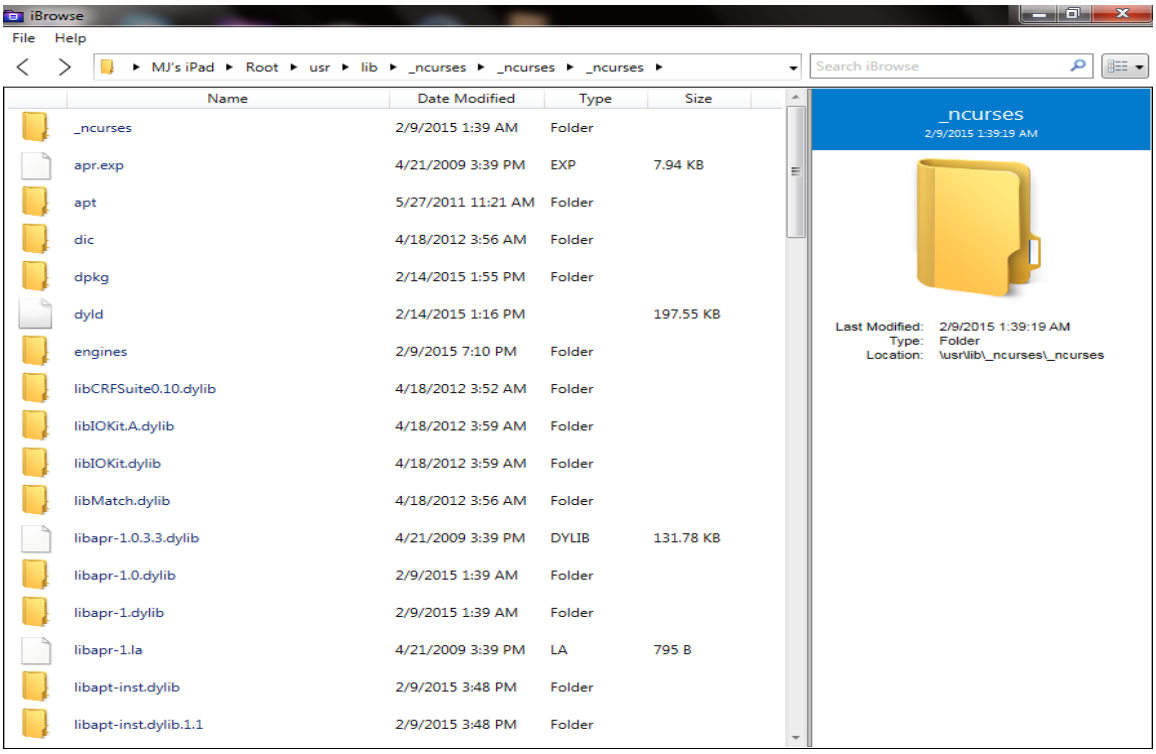


Figure 7.7: Endless Iteration of *_ncurses* Subfolder

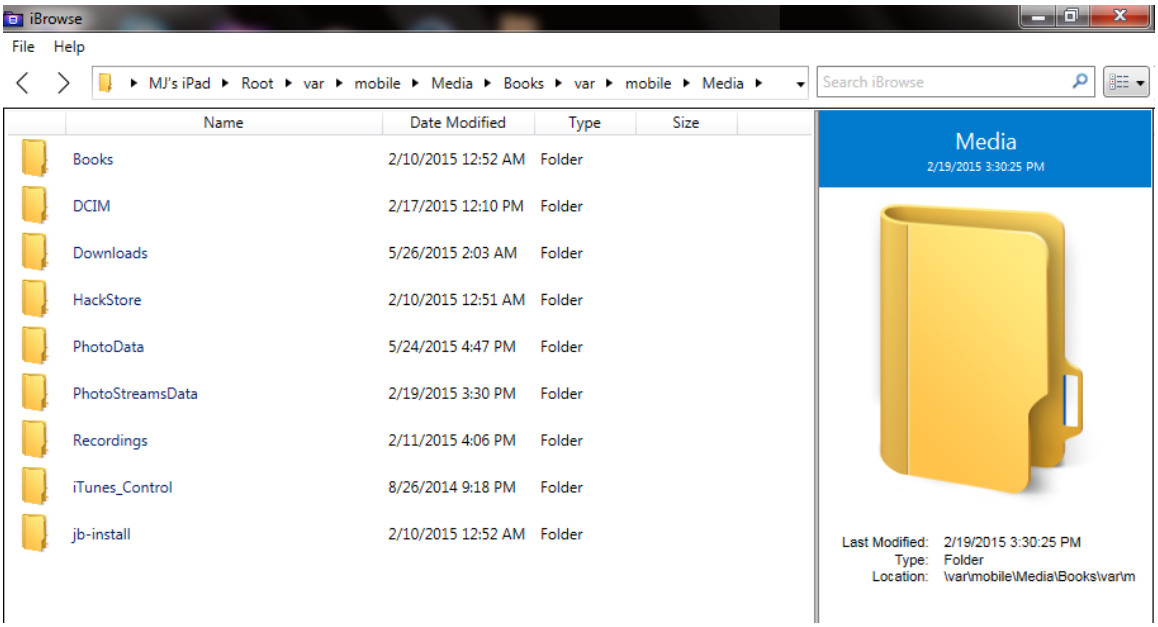


Figure 7.8: Endless Iteration of *mobile* Subfolder

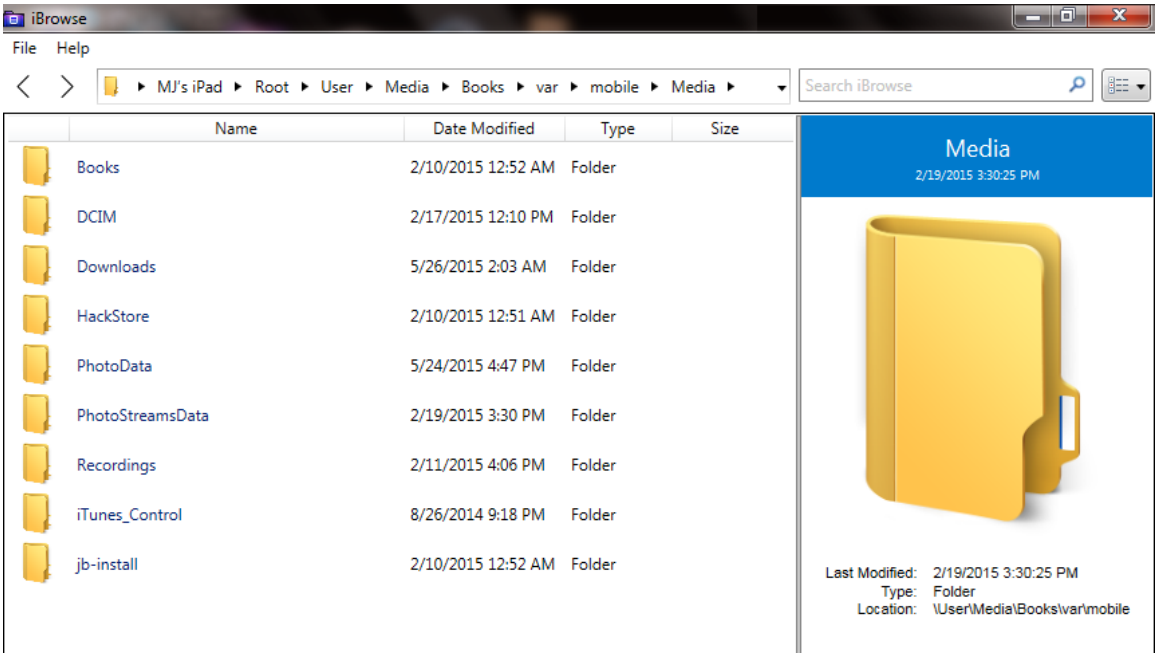


Figure 7.9: Endless Iteration of *Media* Subfolder

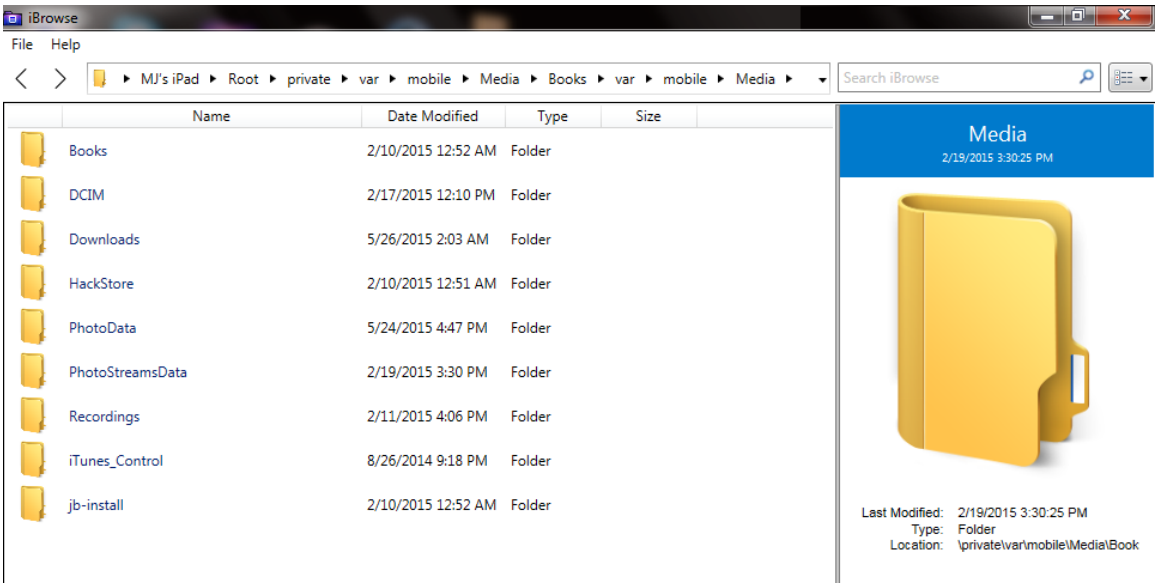


Figure 7.10: Endless Iteration of *var* Subfolder

The results show that hundred percent data integrity is not guaranteed whether free tool or commercial tool is used. However, depending on the need (files to be extracted) different extraction tools may be used.

The findings of our investigations suggest that investigator who is just interested in camera picture can simply use Windows 7 operating system utility. As Ubuntu platform and libimobiledevice methods provide subset of similar reliable results comparable to XRY logical, so these two free available tools can be used for live data extraction. However, if investigator is interested in recovery of deleted data, then XRY physical (or logical) can be utilized for better results.

7.3 Summary

The chapter has compared the artifacts attained from open source forensic tools with the artifacts attained from a commercial forensic tool. The artifacts acquired from various tools were compared in terms of difference in hash values. Moreover, several variations and added files/folders due to the use of specific forensic tool were properly shown and discussed. Moreover, the chapter has recommended specific forensic tools depending upon the requirement of an incident.

Chapter 8

Conclusion and Future Work

iDevices have achieved great success and gained widespread popularity in short period of time. These devices contain plenty of data which has forensic value. Preserving the integrity of data throughout the acquisition process is an important step in any digital forensic investigation.

This research has discussed simple techniques to attain same subset of iDevice's artifacts which we can acquire from a commercial tool. To assure authenticity of the proposed methods, hashes of related files acquired from different tools were calculated and compared. Furthermore, various files, which were altered in consecutive XRY extractions, have been identified and analyzed. The results can be used by a forensic examiner to choose the appropriate tool for data extraction keeping in view the requirements.

This research has also analyzed jail breaking procedure. It was interesting to perform a jail breaking acquisition technique on an iPad and comparing this with a commercial tool to determine what level of data integrity can be obtained via jail breaking technique.

As a continuation of current research work, following areas serve for future work.

- Develop iDevice forensic tool based on the forensic techniques discussed in this research work.
- Compare data integrity of other interesting forensic tools in their latest versions.
- Make and modify jailbreaking laws from the useful information achieved from this research work

Appendix-I

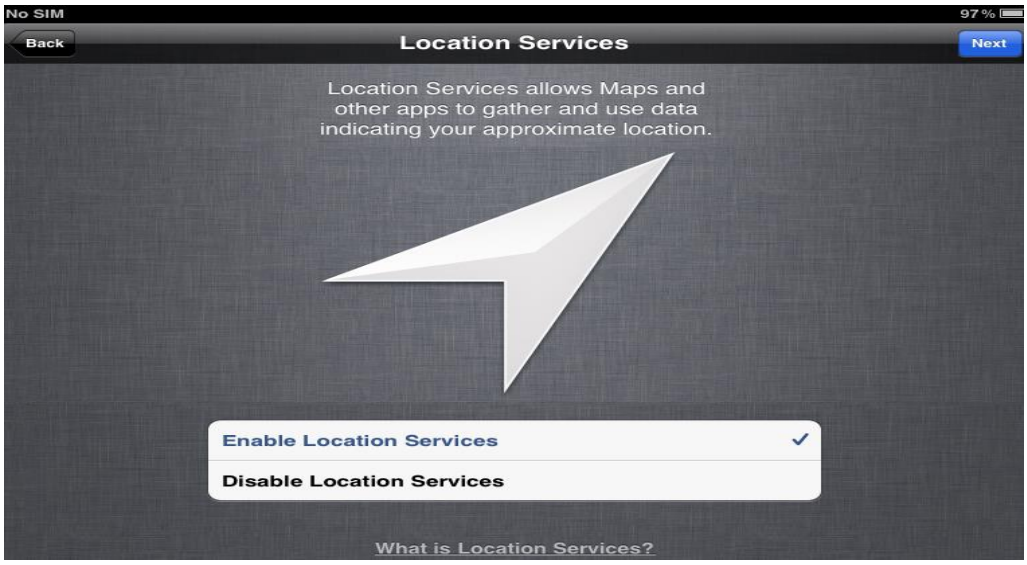
iPad Configuration

Step # 1: Slide to configure

Step # 2: Select language

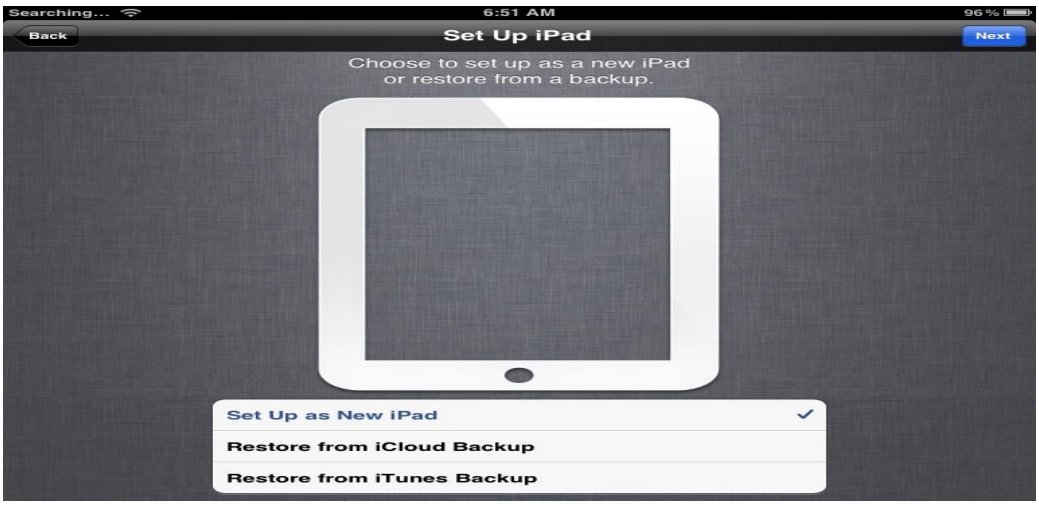
Step # 3: Choose Country

Step # 4: Select *Enable location services*



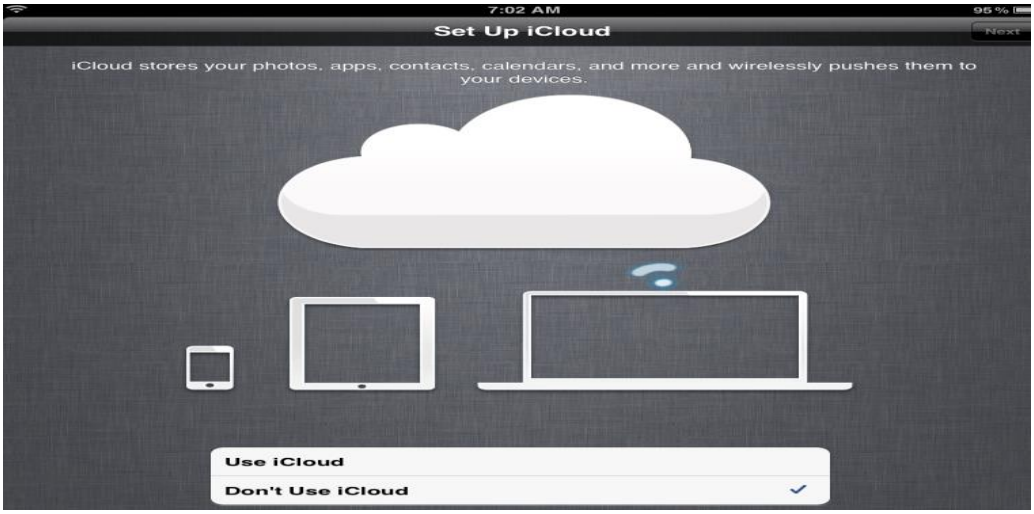
Step # 5: Enable Wi-fi Network

Step # 6: Select *Set Up as New iPad*



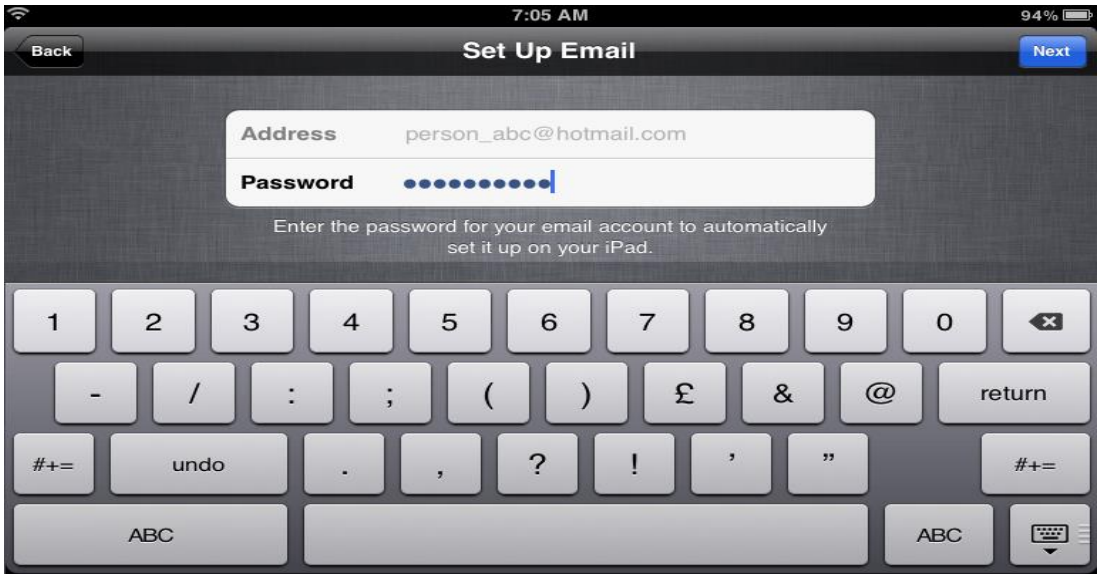
Step # 7: Create Apple ID

Step # 8: Select *Don't Use iCloud*



Step # 9: Select *Use Find My iPad*

Step # 10: Set up email on iPad



iPad is properly configured and ready for use.

BIBLIOGRAPHY

[1] B. Iqbal, A. Iqbal and H. A. Obaid "A Novel Method of iDevice (iPhone,iPad,iPod) Forensics without Jailbreaking," International Conference on Innovations in Information Technology (IIT), 2012

[2] L. Gomez and J. Arnedo, "Universal, fast method for iPad forensics imaging via USB adapter," Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011

[3] D. Abalenkovs et al., "Mobile Forensics: Comparison of extraction and analyzing methods of iOS and Android," 2012

[4] National Institute of Standards and Technology. Computer Forensics Tool Testing Program. [Online]. Available: http://www.cftt.nist.gov/

[5] National Institute of Standards and Technology. (2008, May). Test Results for Mobile Device Acquisition Tool: Micro Systemation .XRY 3.6. [Online]. Available: https://cyberfetch.org/sites/default/files/Mobile_Micro_Systemation_XRY_3_6_2008.pdf

[6] National Institute of Standards and Technology (2010, April). Smart Phone Tool Test Assertions and Test Plan. http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Test_Assertions_and_Test_Plan.pdf

[7] National Institute of Justice. [Online]. Available: http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/cftt.htm

[8] J. Zdziarski, iPhone Forensics: Recovering Evidence,Personal Data, and Corporate Assets.: O'Reilly, 2008.

[9] A. K. Kubi, S. Saleem, and O. Popov, "Evaluation of Some Tools for Extracting e-Evidence from Mobile Devices," 5th International Conference on Application of Information and Communication Technologies (AICT), Baku, 2011.

[10] J. Sigwald. iphone-dataprotection. [Online]. Available: http://code.google.com/p/iphone-dataprotection/wiki/README

[11] J. Sigwald. Automatic SSH ramdisk creation and loading. [Online]. Available: http://msftguy.blogspot.com

[12] National Institute of Standards and Technology. (2010, November). Test Results for Mobile Device Acquisition Tool: XRY 5.0.2. [Online]. Available: https://cyberfetch.org/sites/default/files/Mobile_Test_Results_for_Mobile_Device_Acquisition_Tool_XRY_5_0_2_Nov_201....pdf

[13] National Institute of Standards and Technology. (2013, February). Test Results for Mobile Device Acquisition Tool: Micro Systemation XRY v6.3.1. [Online]. Available: https://cyberfetch.org/sites/default/files/Mobile_Micro_Systemation_XRY_v6_3_1_2013.pdf

[14] National Institute of Standards and Technology Guidelines on Mobile Device Forensics. (2014, May). [Online]. Availabe: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

[15] B. D. Boer and A. Bosselaers "Collisions for the compression function of MD5, Advances in Cryptology," EUROCRYPT '93. LNCS 765; p. 293-304, 1994

[16] MicroSystemation. XRY COMPLETE. [Online]. Available: http://www.msab.com/xry/xry-complete

[17] MicroSystemation. USEFUL LINKS. [Online]. Available: http://www.msab.com/support/useful-links

[18] What is Ubuntu? [Online]. Available: https://help.ubuntu.com/12.04/ installation-guide/powerpc/what-is-ubuntu.html

[19] J. Auzu. How to Manage iPhone/iPod/iPad on Linux. [Online]. Available: http://www.junauza.com/2012/07/how-to-manage-iphoneipodipad-on-linux.html

[20] About Santoku. [Online]. Available: https://santoku-linux.com/about-santoku

[21] HOWTO create a logical iOS device backup using libimobiledevice on Santoku Linux. [Online]. Available: https://santoku-linux.com/howto/mobile-forensics/howto-create-a-logical-backup-of-an-ios-device-using-libimobiledevice-on-santoku-linux

[22] Dev-Team Blog. To find yourself, think for yourself © Socrates 469 BC. [Online]. Available: http://blog.iphone-dev.org/tagged/redsn0w

[23] iClarified. How to jailbreak Your iPad 1 Using RedSn0w (Windows) [5.1.1]. [Online]. Available: http://www.iclarified.com/entry/index.php?enid=21055

[24] iClarified. Where to Download RedSn0w From. [Online]. Available: http://www.iclarified.com/entry/index.php?enid=16424

[25] iBrowse by Macroplant. [Online]. Available: https://www.ibrowseapp.com/

[26] downloads.28.sqlitedb - SQLite Database Catalog. [Online]. Available: http:// www.filesig.co.uk/sqlitedatabasecatalog/downloads.28.sqlitedb%20SQLite%20Database%20%5b00001%5d.html

RELATED RESEARCH PUBLICATIONS

Conference Paper

M. J. Ahmed, U. Khalid, B. Aslam, “iDevice forensics - Data integrity,” 17th IEEE International Multi Topic Conference, 2014