Overcoming Forensic Implications with Enhancing Security in iOS

Mounika Reddy Gangula
mrgangula@stcloudstate.edu

Follow this and additional works at: https://repository.stcloudstate.edu/msia_etds

Recommended Citation
https://repository.stcloudstate.edu/msia_etds/77

This Starred Paper is brought to you for free and open access by the Department of Information Systems at theRepository at St. Cloud State. It has been accepted for inclusion in Culminating Projects in Information Assurance by an authorized administrator of theRepository at St. Cloud State. For more information, please contact rsweelbaum@stcloudstate.edu.
Overcoming Forensic Implications with Enhancing Security in iOS

by

Mounika Reddy Gangula

A Starred Paper
Submitted to the Graduate Faculty of
St. Cloud State University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Science in
Information Assurance

March, 2019

Starred Paper Committee:
Mark Schmidt, Chairperson
Dennis Guster
Sneh Kalia
Abstract

As the decades passed, smartphones have come to their greatest inventions. But their history has more than 2500 years starting from a basic thing of strings and beads, i.e. from the Abacus to the latest of our present iPhone. With every special invention in this area brought people together socially over the internet. This, in turn, raised the alarm for having secured communication. With these devices getting popular, development in the technology to enhance the security features in those devices has also been increasing. These advancements have brought Apple operating system (IOS) into light. These devices are one step ahead of all other smartphones regarding storage by having space for storing emails, GPS data and many more. This feature of storage has a major advantage in conducting forensics for investigation purposes. In this research, I performed data acquisition on iPhones with two different OS versions using various forensic tools and then compare the forensic implications with variant security features. I analyzed the forensic implications with enhancements in security and iPhone operating systems over the years. I also used to software to break the iPhone passcode which is the major forensic implication caused.
# Table of Contents

<table>
<thead>
<tr>
<th>List of Figures</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

**Chapter**

I. Introduction ................................................................................................................................. 8
   - Introduction ............................................................................................................................... 8
   - Problem Statement ...................................................................................................................... 8
   - Nature and Significance of the Problem ................................................................................... 9
   - Objective of Study ..................................................................................................................... 9
   - Study Questions ....................................................................................................................... 9
   - Definition of Terms .................................................................................................................. 10
   - Summary .................................................................................................................................. 10

II. Background and Literature Review .............................................................................................. 11
   - Introduction .............................................................................................................................. 11
   - Background Related to Problem ............................................................................................... 11
   - Literature Related to Problem ................................................................................................. 11
   - Literature Review Related to the Methodology ........................................................................ 22
   - Security vs Forests .................................................................................................................. 30

III. Methodology ................................................................................................................................ 33
   - Introduction .............................................................................................................................. 33
   - Design of Study ......................................................................................................................... 33
   - Tools and Techniques ............................................................................................................... 33
   - Hardware and Software Requirements ..................................................................................... 33
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV. Data presentation and Analysis</td>
<td>35</td>
</tr>
<tr>
<td>Introduction</td>
<td>35</td>
</tr>
<tr>
<td>Data Presentation</td>
<td>35</td>
</tr>
<tr>
<td>Data Analysis</td>
<td>43</td>
</tr>
<tr>
<td>Summary</td>
<td>64</td>
</tr>
<tr>
<td>V. Results, Conclusion and Future Works</td>
<td>65</td>
</tr>
<tr>
<td>Introduction</td>
<td>65</td>
</tr>
<tr>
<td>Results</td>
<td>65</td>
</tr>
<tr>
<td>Conclusion</td>
<td>69</td>
</tr>
<tr>
<td>Future Works</td>
<td>69</td>
</tr>
<tr>
<td>References</td>
<td>71</td>
</tr>
</tbody>
</table>
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Evidence and chain of custody</td>
<td>13</td>
</tr>
<tr>
<td>2.</td>
<td>IT security principle</td>
<td>14</td>
</tr>
<tr>
<td>3.</td>
<td>Digital forensic principle</td>
<td>15</td>
</tr>
<tr>
<td>4.</td>
<td>Digital forensics process</td>
<td>16</td>
</tr>
<tr>
<td>5.</td>
<td>iPhone models</td>
<td>18</td>
</tr>
<tr>
<td>6.</td>
<td>iOS architecture</td>
<td>19</td>
</tr>
<tr>
<td>7.</td>
<td>Levels of abstraction</td>
<td>19</td>
</tr>
<tr>
<td>8.</td>
<td>Property list types and their various representations</td>
<td>20</td>
</tr>
<tr>
<td>9.</td>
<td>iOS security model</td>
<td>21</td>
</tr>
<tr>
<td>10.</td>
<td>iPhone in normal mode</td>
<td>24</td>
</tr>
<tr>
<td>11.</td>
<td>iPhone in recovery mode</td>
<td>25</td>
</tr>
<tr>
<td>12.</td>
<td>iPhone in DFU mode</td>
<td>26</td>
</tr>
<tr>
<td>13.</td>
<td>iPhone backup extractor</td>
<td>27</td>
</tr>
<tr>
<td>14.</td>
<td>iPhone analyzer</td>
<td>28</td>
</tr>
<tr>
<td>15.</td>
<td>iPhone explorer</td>
<td>29</td>
</tr>
<tr>
<td>16.</td>
<td>Passcode feature in iPhone 4s</td>
<td>30</td>
</tr>
<tr>
<td>17.</td>
<td>Passcode in iPhone 7plus</td>
<td>31</td>
</tr>
<tr>
<td>18.</td>
<td>Establishing connection in iPhone 4s and iPhone 7plus</td>
<td>32</td>
</tr>
<tr>
<td>19.</td>
<td>Installation of iMazing(a)</td>
<td>36</td>
</tr>
<tr>
<td>20.</td>
<td>Installation of iMazing(b)</td>
<td>36</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>21.</td>
<td>Installation of iMazing(c)</td>
<td>37</td>
</tr>
<tr>
<td>22.</td>
<td>Installation of Imazing(d)</td>
<td>37</td>
</tr>
<tr>
<td>23.</td>
<td>Analyzing iMazing against backup data</td>
<td>38</td>
</tr>
<tr>
<td>24.</td>
<td>Installation of iExplorer</td>
<td>38</td>
</tr>
<tr>
<td>25.</td>
<td>Analyzing iExplorer against iPhone 7plus</td>
<td>39</td>
</tr>
<tr>
<td>26.</td>
<td>Analyzing iExplorer against iPhone 6plus</td>
<td>39</td>
</tr>
<tr>
<td>27.</td>
<td>Analyzing backups of iPhone 6 plus</td>
<td>40</td>
</tr>
<tr>
<td>28.</td>
<td>Analyzing Safari in iExplorer of iPhone 6plus</td>
<td>40</td>
</tr>
<tr>
<td>29.</td>
<td>Analyzing notes in iExplorer of iPhone 6plus</td>
<td>41</td>
</tr>
<tr>
<td>30.</td>
<td>Analyzing photos in iExplorer of iPhone 6plus</td>
<td>41</td>
</tr>
<tr>
<td>31.</td>
<td>Analyzing calendar in iExplorer of iPhone 6plus</td>
<td>42</td>
</tr>
<tr>
<td>32.</td>
<td>Installation of Elcomsoft phone breaker</td>
<td>42</td>
</tr>
<tr>
<td>33.</td>
<td>Failed passcode attempts count</td>
<td>43</td>
</tr>
<tr>
<td>34.</td>
<td>Erase data option in iPhone 7plus</td>
<td>44</td>
</tr>
<tr>
<td>35.</td>
<td>Adding passcode enables data protection</td>
<td>45</td>
</tr>
<tr>
<td>36.</td>
<td>Deleting passcode disables data protection</td>
<td>46</td>
</tr>
<tr>
<td>37.</td>
<td>Failed brute force attack on stronger password</td>
<td>47</td>
</tr>
<tr>
<td>38.</td>
<td>iSumsoft iTunes password refixer</td>
<td>48</td>
</tr>
<tr>
<td>39.</td>
<td>Initializing iSumsoft iTunes password refixer</td>
<td>49</td>
</tr>
<tr>
<td>40.</td>
<td>Setting the range</td>
<td>49</td>
</tr>
<tr>
<td>41.</td>
<td>Setting the length</td>
<td>50</td>
</tr>
<tr>
<td>42.</td>
<td>Setting the logfile location</td>
<td>50</td>
</tr>
<tr>
<td>Figure</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>43. Processing the refixer</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>44. Extracting backup data using iMazing</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>45. Securing the user’s secrets in a keychain</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>46. Loading data for password recovery(a)</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>47. Loading data for password recovery(b)</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>48. Attacks for password recovery</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>49. Processing dictionary attack(a)</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>50. Processing dictionary attack(b)</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>51. Processing brute force attack</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>52. Failed brute force attack onto iPhone 7plus</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>53. Successful brute force attack on iPhone 7plus</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>54. Tools in Elcomsoft phone breaker</td>
<td>58</td>
<td></td>
</tr>
<tr>
<td>55. Exploring keychains</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>56. Exploring Wifi passwords</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>57. Failed password recovery on unencrypted data</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>58. Verifying password on PhoneRescue</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>59. Analyzing files on Phone Rescue</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>60. Completion of PhoneRescue scan</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>61. Analyzing recovered data</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>62. Acquiring deleted contacts</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td>63. Acquiring deleted call history</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td>64. Acquiring deleted messages</td>
<td>64</td>
<td></td>
</tr>
</tbody>
</table>
Chapter I: Introduction

Introduction

Digital forensics is the division of forensic science focusing on recovering and investigating data stored digitally or electronically. This digital forensics is like computer forensics with an extended feature of investigating all devices capable of storing data digitally. Mobile forensics is part of digital forensics which is related to the recovery of data on mobile devices. Technological innovations and internet have created a positive as well as negative impact on the society. The number of people using the technology has also increased by the accessibility of these through the internet.

As known, the technology can be used for legitimate as well as illegitimate purposes. Phone have become a widely used device for all ages. Starting from the time Apple Inc. introduced the iPhone until today, people are overwhelmed by seeing the advancements of the features in each version and the enhancements related to security. Nowadays, the number of iPhone users outnumber the other smartphone users. The increased use of phones led people to explore it more than usual making them commit various crimes believing they would never be caught. The data on the iPhone is encrypted, and the Apple operating system on the iPhone prevents us from running any applications that are not authorized by Apple to extract data.

With every release of new version of operating system, a new set of problems come into existence making mobile forensics a never-ending battle.

Problem Statement

Digital forensics relies on computer forensic investigations where digital and electronic media is used by the investigators to solve the cases. With the number of people using iPhones is increasing, few users started using it for committing crimes due to its high-end security,
storage space and its encrypted method of storing data. With security enhancements in each new release of iOS version, it is making hard for digital forensics investigators to extract data from the phone. It was always hard to extract any data from an iPhone without bypassing the passcode. In other words, it is hard to do a full data acquisition without unlocking the iPhone.

**Nature and Significance of the Problem**

Nowadays, new versions of iPhone have various features to ensure that the data is protected. The investigators are facing problems to extract data from highly secured phone and even if they crack in the code, it is impossible to extract deleted files from the phone. Hence few crimes have been hard to solve using digital forensic tools which failed to extract the deleted data. the possibility of hiding the data on iPhone and the possibility of making the iPhone unusable makes it hard to investigate. These forensic implications must be concentrated to solve cases with an ease in cases involving an iPhone as an evidence.

**Objective of Study**

The main objective of this project is to identify the forensic implications with changing security features and determine the forensic results of various forensic tools applied on the iPhone.

**Study Questions**

1. How can the forensic analysis be performed?
2. How are security features in iOS changing over years?
3. What are the forensic implications with the security?
4. What are the ways to bypass security?
5. What are Forensic tools used?
Definition of Terms

iOS: iOS stands for iPhone operating system. It is a mobile operating system developed by Apple Inc. There are number of versions being released every year. The current version of the operating system is iOS 11.

iPhone: This is the first product launched by Apple Inc. with iPhone operating system. There are many generations of iPhone with different operating system version. Each new release has new set of features.

Mobile Forensics: According to (Mobile Device Forensics, n.d.) “It is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions.”

Extraction: Data extraction is a process of retrieving data from the sources. In this case the source is an iPhone. There are various methods to in use to extract data. There are some legal clearances to extract data.

Jail break: It is an attempt to go deep into the root of the operating system. In case of an iPhone, jailbreaking removes all the software restrictions imposed by Apple on iOS.

Summary

In this chapter, we have learned what is the main motto of this research, what is digital forensics, what are the various problems faced by the forensic investigators with rapid increase in new releases of operating systems. We also learnt where the problem lies and how significant the problem of security persists in Forensics.
Chapter II: Background and Literature Review

Introduction

In this chapter, we will learn about forensics, digital forensics, the process of forensics, forensic implications with enhancing security. This section tells us about the literature required for the implementation of the experiment. I also discuss the fundamental principle of digital forensics and why is it related to conduct forensics.

Background Related to Problem

Over the years, Apple has been introducing various models of iPhones with each differing in the type of security features it incorporates. The iOS platform has its base as security being at its core. The new version of iOS will be built on entirely new platform architecture. To gain the utmost security with transparent interface, Apple combines software, hardware, and services to work together.

Literature Related to Problem

What is Forensics? According to (Wikipedia, n.d.) “Forensic science is the application of science to criminal and civil laws, mainly on the criminal side during the criminal investigation as governed by the legal standards of admissible evidence and criminal procedure.” In other words, forensics is a method of collecting and evaluating information or data about what has happened in a criminal case. Investigating the possible ways on how a crime could have happened. According to CSI (n.d.), the study of forensic science is drawn from number of other scientific branches, involving physics, chemistry, and biology, with its main objective set to recognize, identify, and evaluate the evidence. Forensics is not always about a software tool but
relies on the forensic scientist investigator. Investigators collect the evidence and report them using the chain of custody form.

The chain of custody is a document showing custody, control, transfer, seizure, analysis of the evidence. The main motto for having a chain of custody is to ensure that the data presented as evidence is as it is when originally acquired. The documentation must include everything about the evidence like the reason for collecting the evidence, duration of its custody, signatures of the people involved, and transfer custodians (EDRM, n.d.). There are many areas where forensics can be applied. We concentrate on forensics science applied on digital evidence which is termed as digital forensics.
Figure 1: Evidence and chain of custody (Chain of Custody, n.d.)
**Digital forensics.** According to Stephens’ (n.d.) article, digital forensics is “the science of identifying, preserving, recovering, analyzing and presenting facts about digital evidence found on computers or digital storage media devices.” Digital evidence is data put away or transmitted in binary form that might be relied upon on in court. It is normally connected with electronic crime, or e-crime, for example, a missing case or a credit card extortion. This is currently used to indict a wide range of crimes, not simply e-crime. For instance, suspects’ email or cell phone records like messages which shows if there is any association with other suspects in the crime, browsing history or gallery which shows any searches related to how to commit the crime and may also contain basic confirmation about their aim (NIJ, 2016). In the year 2013, there was a missing case of two teens registered in Anoka county of Minnesota. The investigators took the digital evidences from their iPods, iPhones. They have used forensics on these devices to identify the suspects. They succeeded in finding the victims and the suspect (Prather, 2014).

**Digital forensic principle.** As we all know IT security has one core principle to which all the technological aspects are linked or related. That one core principle revolves around-Confidentiality, Integrity, and Availability (Leong, 2006).

![Figure 2: IT security principle](image-url)
Like IT security, Digital forensics investigation also has a fundamental principle which includes:

1. Reconnaissance
2. Reliability
3. Relevance

![Diagram showing digital forensic principles]

**Figure 3**: Digital forensic principle

**Reconnaissance**: A forensic investigator must use different methods and tools to recover, discover, decode, analyze data and transform into readable evidence. They should be able to retrieve data irrespective of the place the data is stored and type of operating system the device has (Leong, 2006).

**Reliability**: The evidence found should be reliable enough to be admissible for the court. The chain of evidence must be preserved and be prevented from any modification (Leong, 2006).

**Relevance**: Even with evidence being admissible, the evidence must be relevant with the case only then it’ll be valid (Leong, 2006).

**Digital forensic procedure.** The digital forensics process includes four steps:

1. Acquisition
2. Preservation
3. Analysis

4. Reporting

**Acquisition**: This is the first and foremost step a digital forensic investigator does when he collects the digital evidence. The digital media can easily be modified. Even accessing of files can change the media as it logs the access. Hence data acquisition must be done. It is achieved by making a bit-copy or more specifically an image of the evidence. They also have hash values that can be used for future evidence validation. Any forensic investigation will only be done on the copy of the evidence but not directly on the original to prevent any modifications. To make an image is not just by copying data from the evidence, they do it by using specific tools. One such tool is FTK imager (wikipedia, n.d.).

![Digital forensics process](image)

**Figure 4**: Digital forensics process

**Preservation**: This process is the second step in digital forensics process. It ensures the retention and protection of evidence from deletion. Forensically sound methods are applied to preserve the digital evidence (Data Preservation, n.d.).
**Analysis:** This is the important step in digital forensics process. It does user analysis, recovers deleted data and identify reasons, consequences of a security incident (Dennon, n.d.).

**Reporting:** This is the last step after the investigation is done. It involves documenting the observations of the evidence and all the results in form of a report that will be submitted before the judiciary for further procedure of the case (Dennon, n.d.).

**iPhone.** iPhone was first released in June 2007 by Apple, Inc. The current iPhone model is iPhone X. Each model arrives with its own firmware version that can be found by going into Settings>General>About>Version. With each new release the version of operating system is also changing. Each model has enhanced set of security and storage features. With increase in its popularity, iPhone has become one of the main focusing object for many forensic investigators. This also raised an alert for having an active hacking community yielding various research and investigation tools to support forensic investigations. There are basic tools that allow investigator to understand file system and data contents, such as Jailbreaking but it is not forensically sound method (Hoog & Strzempka, 2011)
<table>
<thead>
<tr>
<th>iPhone</th>
<th>Released with</th>
<th>Release date</th>
<th>Final supported OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone</td>
<td>iPhone OS 1.0</td>
<td>June 29, 2007</td>
<td>iPhone OS 3.1.3</td>
</tr>
<tr>
<td>iPhone 3G</td>
<td>iPhone OS 2.0</td>
<td>July 11, 2008</td>
<td>iOS 4.2.1</td>
</tr>
<tr>
<td>iPhone 3GS</td>
<td>iPhone OS 3.0</td>
<td>June 19, 2009</td>
<td>iOS 6.1.6</td>
</tr>
<tr>
<td>iPhone 4</td>
<td>iOS 4.0</td>
<td>June 21, 2010</td>
<td>iOS 7.1.2</td>
</tr>
<tr>
<td>iPhone 4S</td>
<td>iOS 5.0</td>
<td>October 14, 2011</td>
<td>iOS 9.3.5</td>
</tr>
<tr>
<td>iPhone 5</td>
<td>iOS 6.0</td>
<td>September 21, 2012</td>
<td>iOS 10.3.3</td>
</tr>
<tr>
<td>iPhone 5C</td>
<td>iOS 7.0</td>
<td>September 20, 2013</td>
<td>iOS 10.3.3</td>
</tr>
<tr>
<td>iPhone 5S</td>
<td>iOS 7.0</td>
<td>September 20, 2013</td>
<td>iOS 11.3</td>
</tr>
<tr>
<td>iPhone 6 (Plus)</td>
<td>iOS 8.0</td>
<td>September 19, 2014</td>
<td>iOS 11.3</td>
</tr>
<tr>
<td>iPhone 6S (Plus)</td>
<td>iOS 9.0</td>
<td>September 25, 2015</td>
<td>iOS 11.3</td>
</tr>
<tr>
<td>iPhone SE</td>
<td>iOS 9.3</td>
<td>March 31, 2016</td>
<td>iOS 11.3</td>
</tr>
<tr>
<td>iPhone 7 (Plus)</td>
<td>iOS 10.0</td>
<td>September 16, 2016</td>
<td>iOS 11.3</td>
</tr>
<tr>
<td>iPhone 8 (Plus)</td>
<td>iOS 11.0</td>
<td>September 22, 2017</td>
<td>iOS 11.3</td>
</tr>
<tr>
<td>iPhone X</td>
<td>iOS 11.0.1</td>
<td>November 3, 2017</td>
<td>iOS 11.3</td>
</tr>
</tbody>
</table>

**Figure 5:** iPhone models (iPhone, n.d.)

**iOS operating system.** iOS is an operating system is a derivative of BSD Unix with a Mach Kernel XNU based on Darwin OS. The figure represents an overview of iPhone architecture. The iPhone has an ARM processor with core OS including the XNU kernel. It has four levels of abstraction namely Core OS, Core Services, Media, Cocoa touch (Hoog & Strzempka, 2011).
Figure 6: iOS architecture (iOS architecture, n.d.)

Figure 7: Levels of abstraction (Layered architecture, n.d.)
**Data storage.** The data storage on iOS depends on how much data we want to store. The data on iOS is stored on two partitions, OS partition and User partition. The OS partition contains the system data and whereas the user partition contains the user data. The user data that is stored here is encrypted. The most widely used local storage implementation in iOS are (TBI Infotech, 2015):

- **SQLite:** This storage method is used by various platforms especially for low-level relational database work. To operate the data tables, it uses an API named SQL-centric.

- **Property List:** To express simple hierarchies of data, the property lists depend on abstraction. The items of data in these lists are limited to primitive types and other for container of values. The containers are arrays, dictionaries, indexed collections of values. The primitive types can be strings, numbers, binary data, and Boolean values. Using this kind of storage is only limited to small blocks of binary data primarily containing strings and numbers (Property List Programming Guide, n.d.).

<table>
<thead>
<tr>
<th>Abstract type</th>
<th>XML element</th>
<th>Cocoa class</th>
<th>Core Foundation type</th>
</tr>
</thead>
<tbody>
<tr>
<td>array</td>
<td>&lt;array&gt;</td>
<td>NSMutableArray</td>
<td>NSArray (CFArrayRef)</td>
</tr>
<tr>
<td>dictionary</td>
<td>&lt;dict&gt;</td>
<td>NSDictionary</td>
<td>NSDictionary (CFDictionaryRef)</td>
</tr>
<tr>
<td>string</td>
<td>&lt;string&gt;</td>
<td>NSString</td>
<td>NSString (CFStringRef)</td>
</tr>
<tr>
<td>data</td>
<td>&lt;data&gt;</td>
<td>NSData</td>
<td>NSData (CFDataRef)</td>
</tr>
<tr>
<td>number – integer</td>
<td>&lt;integer&gt;</td>
<td>NSNumber (intValue)</td>
<td>NSNumber (CFNumberRef, integer value)</td>
</tr>
<tr>
<td>number – floating point</td>
<td>&lt;float&gt;</td>
<td>NSNumber (floatValue)</td>
<td>NSNumber (CFNumberRef, floating-point value)</td>
</tr>
<tr>
<td>Boolean</td>
<td>&lt;true/&gt; or &lt;false/&gt;</td>
<td>NSBool (boolValue == YES or boolValue == NO)</td>
<td>CFBoolean (CFBooleanRef; kCFBooleanTrue or kCFBooleanFalse)</td>
</tr>
</tbody>
</table>

**Figure 8:** Property list types and their various representations (Property List Programming Guide, n.d.)
• **Core Data**: The core data allows us in dealing with most common functionalities of an application. This core data using SQLite queries to store its data which eliminates the use of separate database.

• **NSUser Defaults**: This kind of storage saves in the logged state of the users within an application and saves user preferences.

• **Key Chain**: This is most secure and reliable method to store data. This is done by using simple wrapper classes using key chain method. The keychain secures data by encrypting them before storing them on the file system. The entire keychain can also be locked entirely needing the master password to decrypt (Keychain Services Programming Guide).

**Security.** The most important aspect of my project is the security. The only problem of full data acquisition is raised because of security enhancements with each release of the operating system. The following figure shows the iOS security model:

![iOS security model](image)

**Figure 9**: iOS security model (Velu, n.d.)
System Security: By designing the system security, the hardware and software of every iOS devices are secured. The tightly coupled integration of the hardware, software and the services ensures the validity of the system. Even the booting of the iOS device is secured. Each step must be cryptographically authorized by Apple hence assuring integrity and trust must be obtained.

The upgraded OS versions have security enclave in their kernel which protects the data by encrypting it. Even if the kernel is compromised by some external applications, the data is still protected by some keys. When the device is turned on, the Secure Enclave part in the kernel is encrypted by the generated ephemeral key associated with a unique ID. The security features like fingerprint, face ID are all processed by Secure Enclave.

Literature Review Related to the Methodology

Data extraction. Data extraction is synonymous to data acquisition. During the forensic investigation, the investigator first must identify the following five features of the evidence (iPhone). They are,

1. Which model is the evidence?
2. What is the iPhone operating system version?
3. What is the passcode?
   a. Is it locked or unlocked?
4. If locked is there any backup password?
5. Is the device jailbroken or not?
With all these in hand, the forensic investigator must take through the next step in the process. The next step is data extraction or acquisition which can be done in following four techniques.

1. Direct
2. Backup or logical acquisition
3. Physical

**Direct.** The direct acquisition method can be done on any iPhone irrespective of the iOS version it has. The iPhone must be unlocked in other words the iPhone must be not protected by a passcode. The tools used for doing this type of acquisition are iFunBox, iMazing, iExplorer (Epifani & Stirparo, 2015).

**Backup or logical acquisition.** The investigator will be able to extract or recover more information than that can be recovered using direct acquisition. This type of acquisition creates backup for the data without altering it. When it comes to backup or logical acquisition, it is important to understand the differences between the different operating modes. There are three modes for an iPhone which should be known by the forensic investigator while performing forensics.

   Normal Mode
   Recovery Mode
   DFU Mode

**Normal mode:** When an iPhone is powered on it should boot an operating system. This is referred to as a normal mode. When doing this there are three steps that takes place, the Low-Level Bootloader is loaded, it gets the iBook, Lastly, the iOS kernel system gets running (Hsamanoudy, 2017).
**Recovery mode:** This mode is used to determine the software version of the iPhone using *irecovery*. There are two most common ways of putting the iPhone in recovery mode- Power-Down Method and Force-Power Method. By setting the iPhone in the recovery mode, investigator can gain access to the device by using some specific tools (Zdziarski, iOS Forensic Investigative Methods, 2012).
**Figure 11:** iPhone in recovery mode (Recover mode image, n.d.)

**DFU mode:** DFU mode stands for Device Firmware Upgrade mode. This mode is used by most tools to bypass the internal security of the iPhone. This helps in setting up forensic imaging on the iPhone (Lorianne Actus branchees, n.d.).
Logical acquisition tools. Logical acquisition can be done using many tools. According to (Epifani & Stirparo, 2015), there are list of tools for logical acquisition like iTunes, Libimobiledevice, UFED Physical Analyzer/UFED 4PC/Ufed Touch, Oxygen Forensic Suite Standard/Analyst, Mobiledit Forensic, AccessData Mobile Phone Examiner Plus, Lantern, XRY, Paraben’s Device Seizure, SQLite Browser, iExplorer. Secure view 3, WaterBoard and iPhone backup extractor.

iPhone backup extractor. This is an open source tool, which can extract data from the device as well as iCloud backup (iPhone Backup Extractor, n.d.)
Functionality and features.

Converts extracted backup databases into CSV, VCard or ICAL formats.

Recover data from encrypted iPhone backup and iCloud backups.

Easy to use.

![iPhone Backup Extractor](image)

**Figure 13:** iPhone backup extractor (iPhone Backup Extractor, n.d.)

**Waterboard.** Waterboard is an open source forensic logical acquisition tool released by Jonathan Zdziarski for iOS devices. This tool performs advanced logical acquisition of iPhone using some extended services in Apple’s built-in lockdown services. This tool can bypass Apple’s mobile backup encryption and hence will be able to give a clear text copy of the file
system. According to (Zdziarski, Waterboard, 2013), “the Waterboard is an extremely useful tool for law enforcement and can provide important evidence in criminal case.”

**iPhone analyzer.** It is a free tool built using java programming language for iOS backup developed by Crypticbit. This has a multi-platform for getting the data. Using this tool, the iOS file system can be viewed easily. The data here is retrieved using iTunes backup so there is no need to worry about the data modification. There is also no human intervention when it is creating the backup. As we all know, there will be data stored in the iPhone as the binary files, to get them the iPhone analyzer has a feature “export all files”. Most of the backups of iTunes are encrypted. This is the problem for retrieving data. In my project, I will research and try to extract even the password encrypted files from the iPhone (Hsamandoudy, 2017).

![iPhone Analyzer](image)

**Figure 14:** iPhone analyzer (Hsamandoudy, 2017)
**iPhone explorer.** This application is developed by Macroplant. It is used to obtain logical data from the iPhone. This is the most common method used by the forensic investigators. This tool allows forensic investigators to extract data from the evidence (iPhone Explorer, n.d.)

![iPhone Explorer](image)

**Figure 15:** iPhone explorer (iPhone Explorer, n.d.)

**Physical acquisition.** Physical acquisition helps the investigator to extract most of the content from an iPhone. The analyst will get a copy of the memory and can access the file system. If the device is not protected by passcode then it is easy to obtain the physical image of the evidence. If the iPhone is protected with a passcode, we have to employ few more techniques to unlock the phone. There are many tools to perform physical acquisition namely, UFED Physical Analyzer, Elcomsoft iOS Forensic Toolkit, Lantern and AccessData MPE, and iXAM (Epifani & Stirparo, 2015).
Security vs Forensics

As we already have seen the updating OS versions in the previous sections, it is important to learn the forensic implications it can cause. Let us discuss about the current version iOS 11. The major forensic issue is the enhanced security feature on the iOS.

**Passcode:** In an iPhone 4s model the length of the passcode is just 4 digits whereas in iPhone 7plus the length of the passcode is 6. This passcode can also be alphanumeric making it hard for the forensic investigators to crack the code.

*Figure 16: Passcode feature in iPhone 4s (iPhone 4S, n.d.)*
Establishing trust: The current OS version requires passcode to establish connection with any other system. Earlier it just prompted “Trust this Computer”. If that is confirmed, the connection would be established. Obtaining the connection is important to perform logical acquisition. In the earlier versions it was much easy to acquire logical acquisition. But with the new version the pairing procedure requires device passcodes to establish trust between the device and the computer (Afonin, 2017).
Figure 18: Establishing connection in iPhone 4s and iPhone 7plus (Longenecker, 2017)

The **S.O.S. mode:** The updated OS version has an extra feature giving an intuitive way for the users to call emergency. They can do it by just pressing the power button five times in continuous succession. When this happen, the iPhone shows a screen prompting three options including the cancel button. This method disables the touch id temporarily and asks for the user’s passcode to unlock the iPhone. This can be a problem to an investigator when the user deliberately does this to disable the Touch ID (Afonin, 2017).
Chapter III: Methodology

Introduction

In this chapter, I focus on the things needed to perform forensics analysis to do data acquisition from the iPhone running on two different levels of iPhone operating systems. I also focus on things like what are the tools and techniques I’ll be using, what is the design of my research and what type of data I’ll collect during the analysis along with the time needed to conduct this entire process.

Design of Study

I will use quantitative approach and perform practical experiment on iPhone 6 plus and iPhone 7 plus both having different levels of operating system. I will use tools on both iPhone models. The results of the experiment will be analyzed and compared for the different security measures deployed on them. I will analyze and report which methodology can acquire full data from the evidence. To perform experiments, quantitative approach is best suited.

Tools and Techniques

The objective for my project is to perform full data acquisition. To carry out this, first things I need are an iPhone and a laptop. I will be using many experimental tools like FTK imager, iPhone backup extractor, iPhone backup browser. According to my research till now, these are the three main tools to acquire full data acquisition. I will also employ jail-breaking to see what happens when we use the above-mentioned tools on already jail-broken device.

Hardware and Software Requirements

I will use the following hardware and software to carry out my experiment:
Hardware requirements.

Item 1- iPhone

  Model 6s
  Released OS version 8.0
  Updated OS version 10.2.1
  Memory 32gb

Item 2- iPhone

  Model 7plus
  Released OS version 10.0
  Updated OS version 11.4.1

Item 3- Dell Laptop

  Model Inspiron 5555 Signature Edition
  Processor AMD A10-8700P Radeon R6, 10 Compute Cores 4C+6G 1.80 GHz
  RAM 8.00 GB
  System type 64-bit Operating System, x64-based processor

Software Requirements.

Forensic Tools: All types of acquisition tools will be used in this experiment. The following are the few tools which I researched that will be used:

  iPhone Backup Extractor/ iPhone Explorer
  Elcomsoft Phone Breaker
  iSumsoft iTunes Password Refixer
  PhoneRescue
Chapter IV: Data Presentation and Analysis

Introduction

In this chapter, All the data collected as part of my experiment will be presented and analyzed.

Data Presentation

To start with the experiment, in a forensic professional’s point of view, we must backup the evidence which is an iPhone in my case. The first and foremost step is to acquire the backup. I used iTunes to back up the phone’s data.

I have used iPhone back up extractor, iPhone back up explorer, iExplorer, Elcomsoft Phone Breaker, iSumsoft iTunes Password Refixer and PhoneResue software to carry out my experiment of finding the forensic apprehensions caused by the security provided by the device.

The installations of the same are as follows:

**iPhone backup extractor and iphone backup explorer.** These two softwares are now provided as a package called iMazing.
**Figure 19:** Installation of iMazing(a)

**Figure 20:** Installation of iMazing(b)
Figure 21: Installation of iMazing(c)

Figure 22: Installation of iMazing(d)
Figure 23: Analyzing iMazing against backup data

iExplorer.

Figure 24: Installation of iExplorer
Figure 25: Analyzing iExplorer against iPhone 7plus

Figure 26: Analyzing iExplorer against iPhone 6plus
Figure 27: Analyzing backups of iPhone 6 plus

Figure 28: Analyzing Safari in iExplorer of iPhone 6 plus
Figure 29: Analyzing notes in iExplorer of iPhone 6plus

Figure 30: Analyzing photos in iExplorer of iPhone 6plus
**Figure 31:** Analyzing calendar in iExplorer of iPhone 6plus

Elcomsoft phone breaker.

**Figure 32:** Installation of Elcomsoft phone breaker
Data Analysis

The first method I used to analyze the data is getting the views from an external person who have been closely associated with using iPhone.

**Bypassing iOS lock screen.** The major downfall for any forensic professional is that bypassing the iPhone Lock passcode. The iPhone must be unlocked to carry out any further forensic processes. With latest iOS updates, bypassing the lock screen has become next to impossible. Though with downgraded iOS versions we can still find ways to unlock the iPhone. One such method is to make iPhone vulnerable to password cracking algorithms like brute force attack. One problem which a forensic professional must be concerned about is the number of failed passcode attempts. Considering iPhone 7 plus, below are the screenshots of this feature. When navigated on to settings and then to Touch ID and Passcode. We must type in the passcode to view the further options in Touch ID & Passcode tab. Each failed attempt is counted.

![Failed passcode attempts count](image)

**Figure 33:** Failed passcode attempts count
The last option in the below screenshot is an option to erase data, this if enabled will wipe off the entire data. This version here wipes of the entire data if there are 10 failed attempts. Here in this phone the erase data option is not enabled.

![Erase data option in iPhone 7plus](image)

**Figure 34:** Erase data option in iPhone 7plus

**Forensic implication.** Brute Force attack takes years together to unlock the passcode. The length of the password is directly proportional to the time taken to decode the lock. Earlier iPhone models just had lock screen password security feature but now with latest updates in security, Touch ID and Face ID have been added to enhance the security. Adding of passcode enables data protection by default.
Figure 35: Adding passcode enables data protection

When the passcode is removed, the data protection will also be automatically disabled. If we carefully observe the below screenshot, the statement regarding the data protection is not there this is because the passcode option has been turned off.
**Figure 36:** Deleting passcode disables data protection

I used an encrypted backup of iOS 11.4.1 with known passcode but still attempting to decode it using Elcomsoft Phone Breaker’s brute force attack. The photograph below shows us the estimated time to decode the passcode (whose length is 14 characters) as 9 years, 47 weeks, 3 days, 1 hour. The average speed that this is iterating is 2 passwords per minute.
Figure 37: Failed brute force attack on stronger password

**Overcoming forensic implication.** In this project we use Elcomsoft Phone Breaker to decode the icloud passcode by performing Brute force and dictionary attacks. If the length of the passcode is less than 5 characters, then the passcode can be decoded sooner.

Disabling of erase data option in the phone can help when the passcode is unknown. There is one more software named iSumsoft iTunes Password Refixer, which performs attacks to decode the password. The great disadvantage is that the passcode decoding takes ample time and the passcode should be just 4 characters in length.
Figure 38: iSumsoft iTunes password refixer
Figure 39: Initializing iSumsoft iTunes password refixer

Figure 40: Setting the range
Unknown iCloud password. Now let us assume to not know the iCloud password.

When we usually backup our phone we can either choose backup to be protected with a password or not.

First of all, let us check what can the softwares that we are using are capable of doing. I present a series of screenshots regarding the features of the softwares. Let us start with iMazing tool, to see how the data is being extracted.
If we closely see the above screenshot, it has a dialog box prompting to type in the backup passcode. While we are backing up the iPhone, iTunes provides us with two options to choose from. We must either choose to encrypt backup or choose not to. With this feature provided, most of the people will choose to encrypt the backup. By doing this, the backup data will be protected from unauthorized access.

**Forensic implication.** The encrypted backup poses a bigger challenge in front of the forensic professional. They cannot analyze the backup data even with having the evidential backup with them. The increased security features in iOS makes all sorts of problematic situations to the forensic professional. One such feature is the encrypted backup. Let us now deduce more about encrypted backup and see how encryption is done.

**Figure 44:** Extracting backup data using iMazing
All the iOS devices have a AES-256 crypto engine dedicated for each which is built between the flash storage and main system memory which makes the encryption efficient (Apple Inc, n.d.).

**According to my study the encryption is done in following methods:**

**Method 1:** The user sets up a passcode to lock the device. Go to settings, then tap on general and then on passcode lock option. The passcode not only creates a lock on the phone but also plays pivot role in encrypting part of iPhone data. This creates a basic level of encryption for the data like iMessages, mail messages and attachments.

**Method 2:** The iOS also provides three application program interfaces through which encryption of the data is carried out.

1. **Keychain Services API:** This API provides the secure storage of passwords and keys in a specially encrypted file called keychain. The keychain can also store arbitrary data.

![Figure 45: Securing the user’s secrets in a keychain (Apple, Inc, n.d.)](image)
2. **Cryptographic Message Syntax:** This API enables the developer to add a digital signature to S/MIME messages.

3. **Certificate, Key, and Trust Services:** This API provides trust validation for cryptography and basic encryption capabilities.

**Overcoming forensic implication.** I have used Elcomsoft Phone Breaker to break the encrypted backup password. This software employs two attacks to decode the encrypted password. They are:

1. **Dictionary Attack:** Elcomsoft Phone Breaker performs dictionary attack to decrypt the encrypted backup password. This attack is performed by automated program to try a list of various words present in dictionary. Now a days having used this attack on latest iOS produces no results. I have performed this attack on the iPhones with various iOS versions, one is iPhone 7 plus with iOS version being the 11 series and then the next iPhone 6 plus with iOS version being the 9 series.

2. **Brute Force Attack** This attack is performed by systematically trying all sorts of combinations of alphabet, numbers and symbols. This best works with short passwords. This attack will find the password but the time it takes is the main concern.

Let us now see the set of screenshots of these two attacks on both of the iOS version backups.
**Figure 46:** Loading data for password recovery(a)

**Figure 47:** Loading data for password recovery(b)
**Figure 48:** Attacks for password recovery

**Figure 49:** Processing dictionary attack(a)
Figure 50: Processing dictionary attack(b)

Figure 51: Processing brute force attack
**Figure 52:** Failed brute force attack on iPhone 7plus (stronger password)

**Figure 53:** Successful brute force attack on iPhone 7plus (average password)
I used these methods on both the iOS versions and the iOS version with having iOS version less than 10 has been vulnerable to the brute force attack and the backup has been decrypted sooner than the later version. After decrypting I acquired various other passwords that will be needed for any forensic professional to check on the evidence.

I first explored the keychain to extract various passwords saved on the phone.

![Tools in Elcomsoft phone breaker](image)

**Figure 54:** Tools in Elcomsoft phone breaker
Figure 55: Exploring keychains

Figure 56: Exploring WiFi passwords
This tool cannot be used if the backup data is not encrypted. The other device which I am using doesn’t have its backup encrypted. Hence this software did not work. It prompted a dialog box saying the same.

![Password Recovery Wizard](image)

**Figure 57:** Failed password recovery on unencrypted data

**Acquisition of data.** I used PhoneRescue software to acquire the lost or deleted data. After decoding the password, I used the password in this software to decrypt the backup and acquire all the data from the backup especially the deleted data. Acquiring deleted data provides a major lead in any case.
Figure 58: Verifying password on PhoneRescue

It took 11 hours to acquire all the data after verifying the password. The time depends on the amount of data. In this software, we can choose what data to be acquired. I selected to acquire the entire data hence took me ample amount of time.

Figure 59: Analyzing files on PhoneRescue
I recovered 85982 deleted items from the backup.

Figure 60: Completion of PhoneRescue scan

Figure 61: Analyzing recovered data
In the below screenshot you can see the deleted contacts.

**Figure 62:** Acquiring deleted contacts

**Figure 63:** Acquiring deleted call history
Summary

In this chapter, I started off with presenting the installations of the softwares. I analyzed the features of them and noted down the findings. I also mentioned the possible Forensic implications and methods to overcome them with updating security. I deduced brute force attack to decode the password. I tried using iSumsoft iTunes Password Refixer to decode the password but I found that this software can only be used when the length of password is 4 characters. Elcomsoft Phone Breaker can apply these attacks only if the backup is encrypted. After decoding the password, I went ahead and decrypted the backup. The results from this approach is was used in another software known as PhoneRescue. Using this software, I performed logical acquisition. This helped us to recover the deleted data too.
Chapter V: Results, Conclusion and Future Works

Introduction

In this chapter I will discuss the results of various softwares used and how it’ll answer the problem statement. The overcoming of forensic implications will also be discussed here. With all these things, the updates in the security will also be mentioned.

Results

I used two iPhones running on different iOS version levels. One is iPhone 6 plus running on iOS version 9.2.1 and another iPhone 7 plus running on iOS version 11.4.1. I used 2 laptops with different OS versions one running windows 10 and other windows 8. The reason I used two different systems so that the backups and iTunes doesn’t messes up. I used brute force attack to bypass the passcode. This method succeeded when used on the encrypted backup with less than 10 characters of password. I used Elcomsoft Phone Breaker and iSumsoft iTunes Password Refixer for this process on both of the iPhone models. I listed the security features and their respective forensic implications with them. To be more precise and accurate about results, I will write answers the study questions.

1. How can the forensic analysis be performed?

The forensic analysis is performed by doing logical acquisition of the evidential device. In my case, iPhone 6 plus and iPhone 7 plus are backed up and the forensic tools are used against them. First, I used password cracking attacks to find the password.

2. How are security features in iOS changing over years?

iOS 1: iOS 1 did not have support for third party applications and it did not have an App store. Based on this there was not a whole lot of consciousness on security. But Apple did notice some vulnerabilities and did release three updates in the iOS version. The first kind of
vulnerability was cross-site scripting in Safari. For this they released a new update v1.0.

Similarly, they faced man-in-the-middle attacks and passcode bypass issues.

**iOS 2:** iOS 2 had a major enhancement and added third-party applications which can be installed via App store. This update also included addition of VPN services which caused some vulnerabilities to show up and hence release security updates. The most common update was for the passcode bypass during emergency calls and third-party apps reading other apps information.

**iOS 3:** This version was the beginning of utilizing location services and find my iPhone feature. Based on this it was a potential threat as based on certain circumstances one could easily bypass the find my iPhone feature. This version also had the security vulnerability of passcode removal when the iPhone is restored via backup.

**iOS 4:** At this point of time Apple has realized its mistake of putting a 4 digit passcode as it was easily bypassed. So, it took additional measures and introduced a longer version of passcodes. It also took measures in controlling the privacy by making the user have control on the location services. It also made sure that the e-mail attachments are encrypted and also extended the same support to third party applications.

**iOS 5:** This version had a feature of a new kind of warning box called “Unsecured Call”. During that time all the major network phone calls were easily intercepted and Apple had its way to warn the user that their phone call is being intercepted by providing this warning. This was also the beginning of Find My Friends app and Apple took a whole lot of preciseness on the privacy of how the data should not be intruded. The common issues were bypassing passcode by using Siri on the lock screen and also slide to redial option.

**iOS 6:** This was the turning phase in update of iOS as it has added a special feature called privacy which lets users to limit access to their information for applications. It also added a
feature of limiting data sharing via Bluetooth. This version also had common bypassing of passcode.

**iOS 7:** This version added the Touch ID feature to unlock the phone along with the passcode. This version has added additional client-side verification of data to perform complete checks during the device activation. This also enforced the limit on failed passcode attempt limit. The accessing of foreground data has been addressed in this version update. Apple added “Trust this computer” feature which is prompted when the phone is connected to a system.

**iOS 8:** This version has added new feature of using random spoofed MAC address instead of the original MAC address to determine the phone’s location. Along with these each new update in the third-party application needs a touch ID to install even an update.

**iOS 9:** This version has the six-digit passcodes instead of having traditional four-digit passcode as the default. This increased the possible passcode combinations from 10,000 to one million. The two-factor authentication was added in this version. When you sign in to the iCloud account on any device for the first time, it asks for the passcode and a six-digit verification code that will be sent to your device.

**iOS 10:** This version did not have any special or key security features.

**iOS 11 & 12:** The major security update in this feature is that “establishment of trust”. Initially in prior version the device was plugged in to a new system, it prompted us to either trust the system or not but in this version along with these options, it also asks us to enter the passcode to trust even when the phone is unlocked. This has “Erase Data” option to erase data when the failed passcode attempts exceed an enforced limit. IOS 12 as today’s date has not seen any much security updates.
3. **What are the forensic implications with the security?**

   a. The stronger passcode length is one major forensic implication which makes it difficult to extract data from a locked device.
   
   b. Establishing the trust between the system and the device causes severe problem.
   
   c. The encrypted backup feature makes it difficult to extract the backup. This encryption is secured along with the addition of passcode.
   
   d. Erase data option makes it difficult to enforce algorithms that iterates over set of password combinations.

4. **What are the ways to bypass security?**

   Brute force attack and dictionary attack is used to iterate over the set of password combinations to unlock the password. In case of unlocking the phone’s, lock screen can also be done using brute force attack. Phones with four-digit passcode and six-digit passcode can be cracked by employing those attacks to iterate. Iterating of numeric combinations is comparatively easy to be iterating over alphanumeric password.

   The forensic tools are used to decrypt the backup which helps us in acquiring the data. The tools can also be employed to recover deleted data which is major bypass.

   The recent call history and messages can be easily found on the iPhone using voice commands or through Siri.

5. **What are Forensic tools used?**

   The list of Forensic tools used are:

   a. iMazing
   
   b. iExplorer
   
   c. Elcomsoft Phone Breaker
d. iSumsoft iTunes Password Refixer

e. PhoneRescue

**Conclusion**

The forensic implications caused by the security updates are to some extent bypassed. The password for the encrypted backup has been successfully decoded. However, we realized that this method of bypassing can only be done with password with shorter length. The result with iSumsoft iTunes Pasword Refixer is that it can only decode the code if the length is 4 characters long.

This experiment also showed us the possible time that will be taken to decode the password. The logical acquisition of the data is also performed by using the PhoneRescue software. The deleted data is also recovered using this software. This complete acquisition helps forensic professional to have a great lead in any case. The deleted data is the critical evidence that can be used to solve any digital crime.

Most of the forensic implications that were posed in earlier stage of this experiment have been solved. Elcomsoft Phone Breaker and PhoneRescue software have been stood among all the other software that have been used in this experiment. From this research, I analyzed two things, one, that forensic implications will persists if there are continuous security enhancements and newer operating system, iPhones are produced. Second, an iPhone can be jailbroken but with utmost care. A jail broken device can bypass all the security enhancements and is easy to dive in and acquire the required data.

**Future Works**
As long as Apple produces and updates the iOS versions, the need for this research is needed. The continuation of this experiment would be the research on overcoming the future forensic implications that are yet to be evolve with the updating security. Like the current iOS version 12 and the current iPhone model like iPhone XS, XR might have many forensic implications in the future which are to be studied and solved.
References


*Chain of Custody*. (n.d.). Retrieved from https://www.google.com/search?client=firefox-b-1-ab&biw=1366&bih=654&tbm=isch&sa=l&ei=3BPIWo28OuqjwTt4Z_IDw&q=chain+of+custody+form+images&oq=chain+of+custody+form+images&gs_l=psy-ab.3...0.0.0.10734.0.0.0.0.0.0.0.0.0.0.0.0.0.0...0...1c..64.psy-ab.3...0.0.0.10734.0.0.0.0.0.0.0.0.0.0.0..0...1c..64.psy-ab..0.0.0....0.6.


*iPhone 4S.* (n.d.). Retrieved from https://www.google.com/search?q=passcode+in+iPhone+4s&client=firefox-b-1-ab&amp;source=lnsms&amp;tbm=isch&amp;sa=X&amp;ved=0ahUKEwiZpqmqvLPaAhUCbKwKHXn-CkQ_AUICygC&amp;biw=1366&amp;bih=654#imgrc=pJCLEYci5mhPyM:.


