2-2019

Overcoming Forensic Implications with Enhancing Security in iOS

Mounika Reddy Gangula
mrgangula@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

Chapter Page

List of Figures

Figure Page

Figure Page

Figure Page

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.

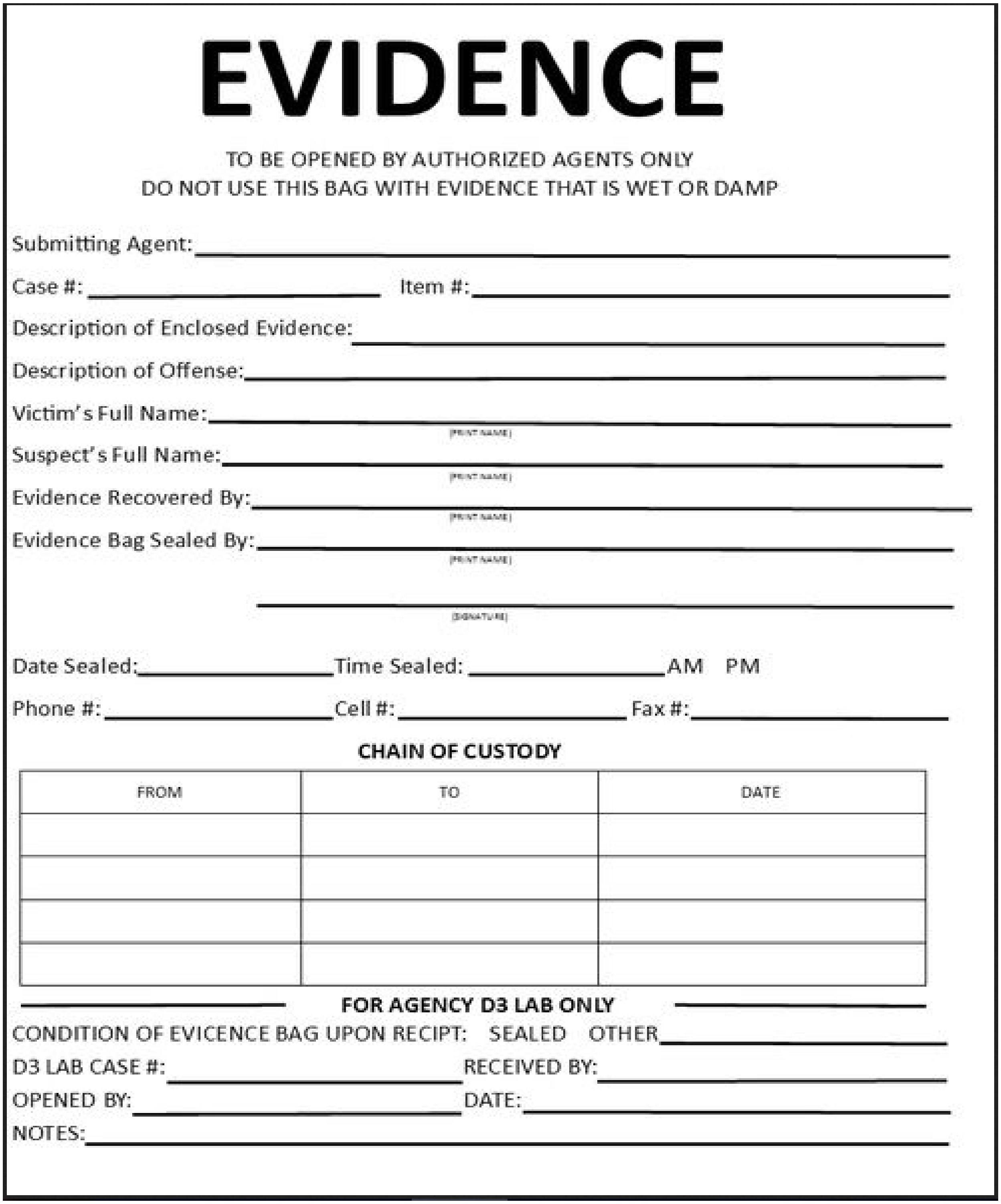
Background Related to Problem

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.



EVIDENCE

TO BE OPENED BY AUTHORIZED AGENTS ONLY
DO NOT USE THIS BAG WITH EVIDENCE THAT IS WET OR DAMP

Submitting Agent:____________________

Case #: ____________ Item #:____________

Description of Enclosed Evidence: ____________

Description of Offense:____________

Victim's Full Name:____________
(PRINT NAME)

Suspect's Full Name:____________
(PRINT NAME)

Evidence Recovered By:____________
(PRINT NAME)

Evidence Bag Sealed By:____________
(PRINT NAME)

____
(SIGNATURE)

Date Sealed:____________Time Sealed: ____________AM PM

Phone #:____________Cell #:____________ Fax #:____________

CHAIN OF CUSTODY

FROM	TO	DATE

FOR AGENCY D3 LAB ONLY

CONDITION OF EVICENCE BAG UPON RECIPT: SEALED OTHER____________

D3 LAB CASE #:____________RECEIVED BY:____________

OPENED BY:____________DATE:____________

NOTES:____________

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).

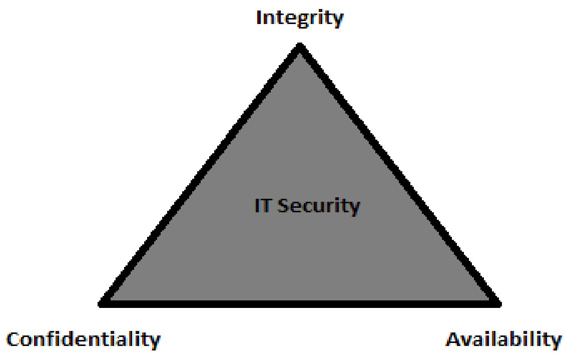


Figure 2: IT security principle

Like IT security, Digital forensics investigation also has a fundamental principle which includes:

1. Reconnaissance
2. Reliability
3. Relevance

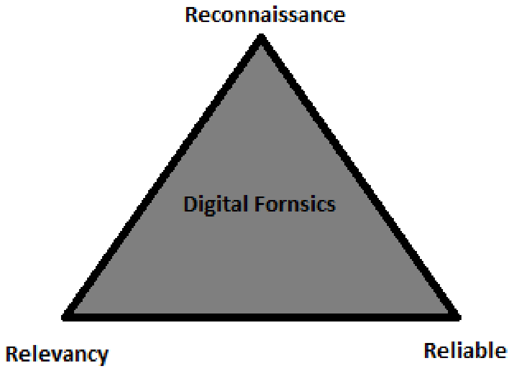


Figure 3: Digital forensic principle

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.).

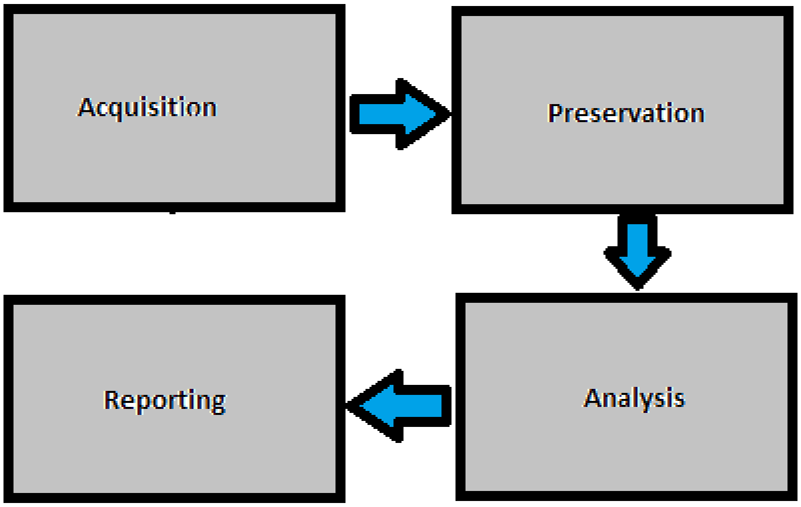


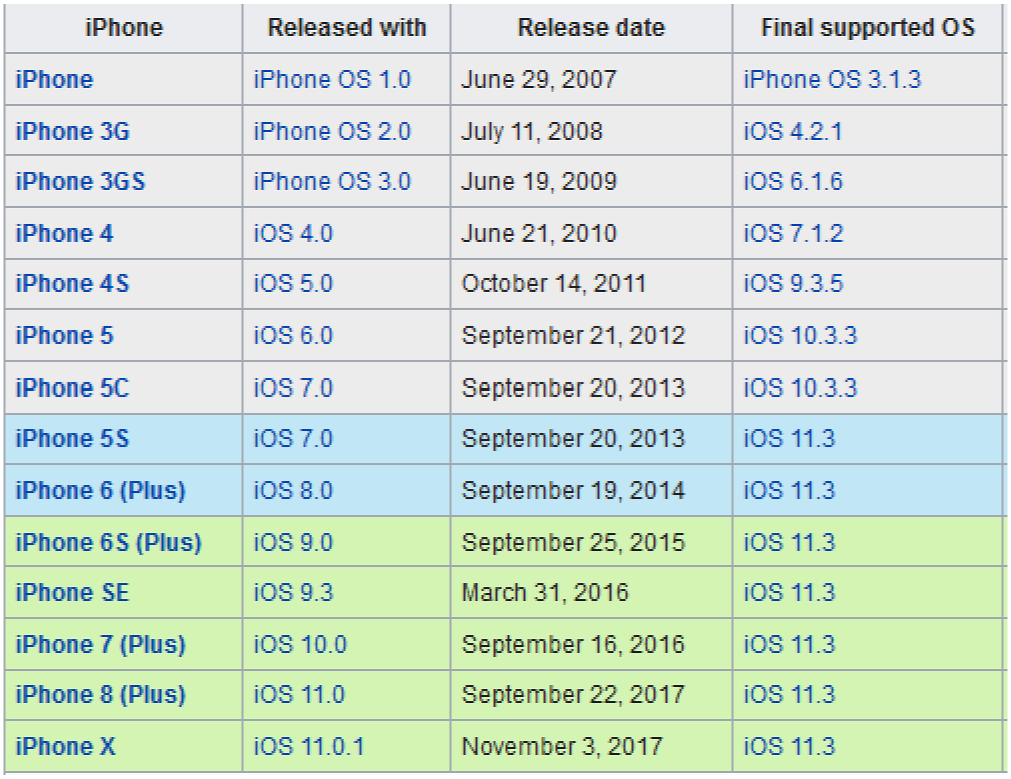
Figure 4: Digital forensics process

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)



iPhone	Released with	Release date	Final supported OS
iPhone	iPhone OS 1.0	June 29, 2007	iPhone OS 3.1.3
iPhone 3G	iPhone OS 2.0	July 11, 2008	iOS 4.2.1
iPhone 3GS	iPhone OS 3.0	June 19, 2009	iOS 6.1.6
iPhone 4	iOS 4.0	June 21, 2010	iOS 7.1.2
iPhone 4S	iOS 5.0	October 14, 2011	iOS 9.3.5
iPhone 5	iOS 6.0	September 21, 2012	iOS 10.3.3
iPhone 5C	iOS 7.0	September 20, 2013	iOS 10.3.3
iPhone 5S	iOS 7.0	September 20, 2013	iOS 11.3
iPhone 6 (Plus)	iOS 8.0	September 19, 2014	iOS 11.3
iPhone 6S (Plus)	iOS 9.0	September 25, 2015	iOS 11.3
iPhone SE	iOS 9.3	March 31, 2016	iOS 11.3
iPhone 7 (Plus)	iOS 10.0	September 16, 2016	iOS 11.3
iPhone 8 (Plus)	iOS 11.0	September 22, 2017	iOS 11.3
iPhone X	iOS 11.0.1	November 3, 2017	iOS 11.3

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).

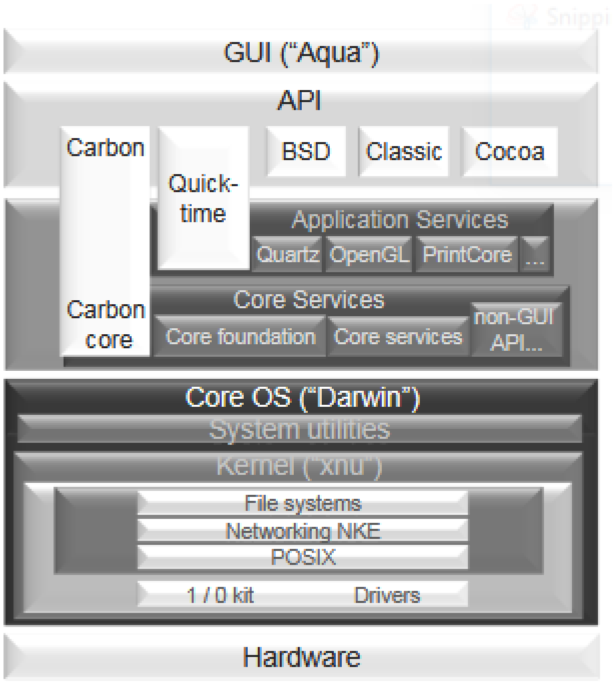


Figure 6: iOS architecture (iOS architecture, n.d.)

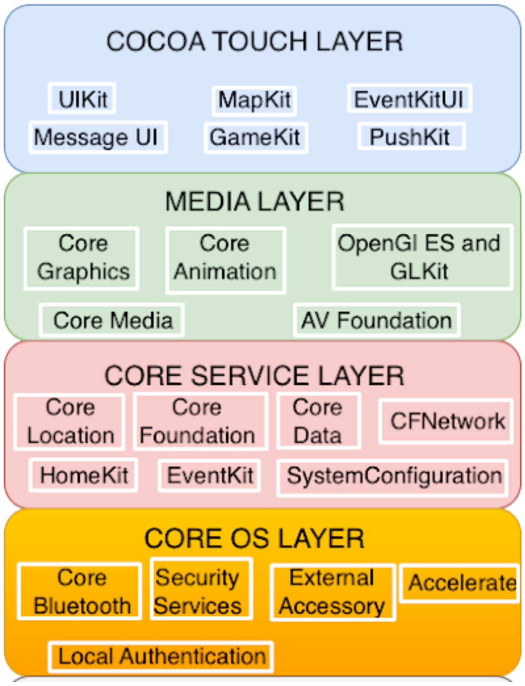
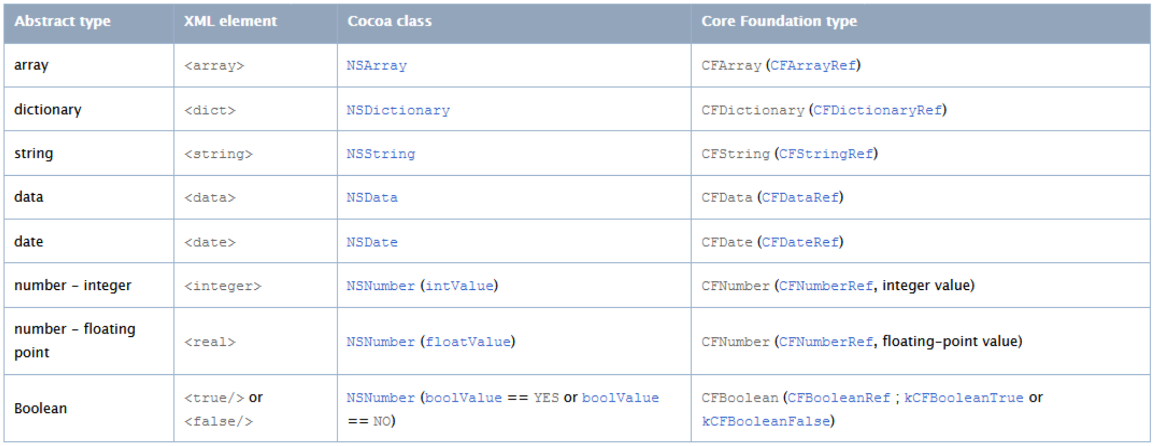


Figure 7: Levels of abstraction (Layered architecture, n.d.)

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.).



Abstract type	XML element	Cocoa class	Core Foundation type
array	<array>	NSArray	CFArray (CFArrayRef)
dictionary	<dict>	NSDictionary	CFDictionary (CFDictionaryRef)
string	<string>	NSString	CFString (CFStringRef)
data	<data>	NSData	CFData (CFDataRef)
date	<date>	NSDate	CFDate (CFDateRef)
number – integer	<integer>	NSNumber (intValue)	CFNumber (CFNumberRef, integer value)
number – floating point	<real>	NSNumber (floatValue)	CFNumber (CFNumberRef, floating-point value)
Boolean	<true/> or <false/>	NSNumber (boolValue == YES or boolValue == NO)	CFBoolean (CFBooleanRef ; kCFBooleanTrue or kCFBooleanFalse)

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:

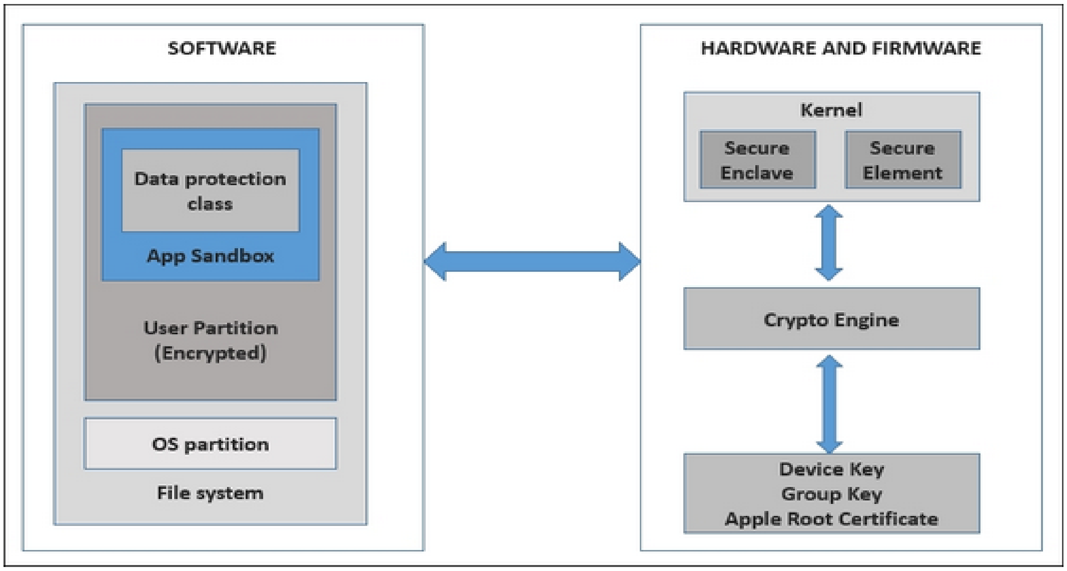


Figure 9: iOS security model (Velu, n.d.)

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).

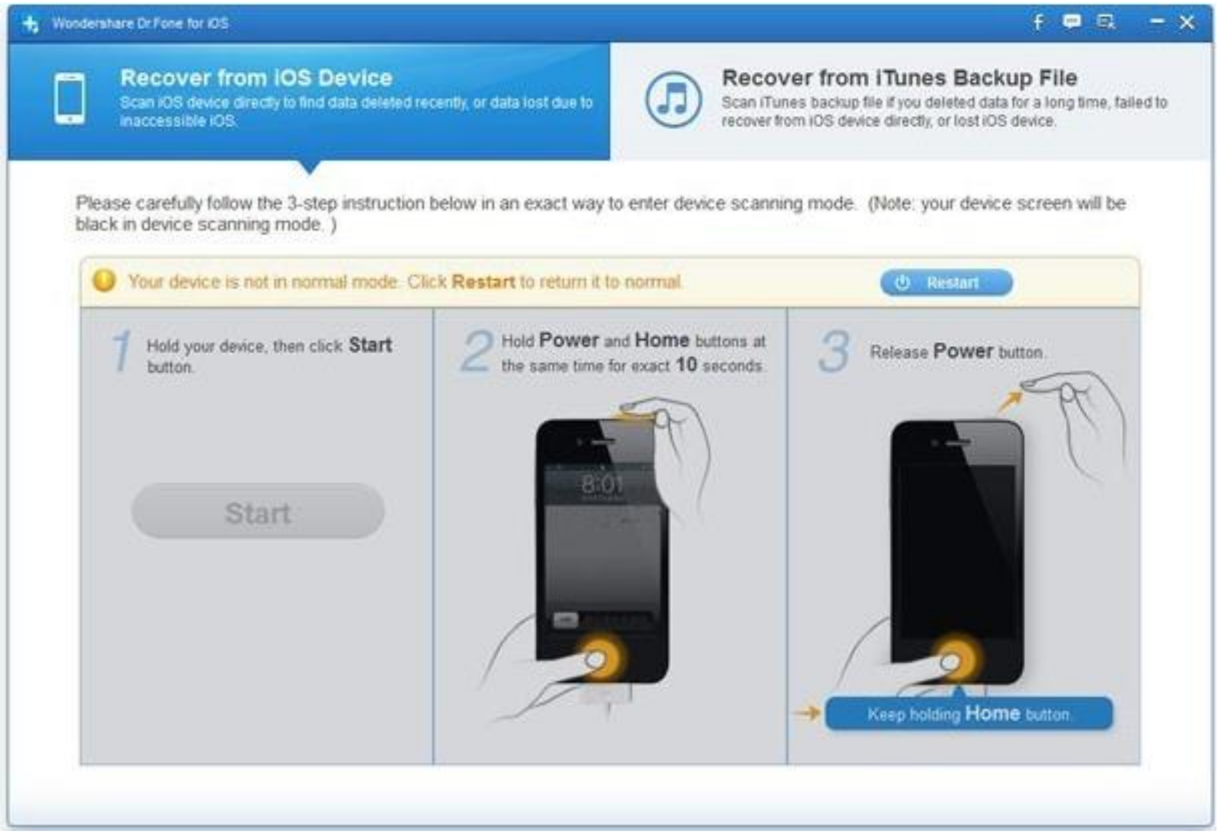
Backup or logical acquisition. The investigator will be able to extract or recover more information than that can be recovered using direct acquisition. This type of acquisition creates backup for the data without altering it. When it comes to backup or logical acquisition, it is important to understand 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).



Recover from iOS Device
Scan iOS device directly to find data deleted recently, or data lost due to inaccessible iOS.

Recover from iTunes Backup File
Scan iTunes backup file if you deleted data for a long time, failed to recover from iOS device directly, or lost iOS device.

Please carefully follow the 3-step instruction below in an exact way to enter device scanning mode. (Note: your device screen will be black in device scanning mode.)

Your device is not in normal mode. Click **Restart** to return it to normal.

1 Hold your device, then click **Start** button.

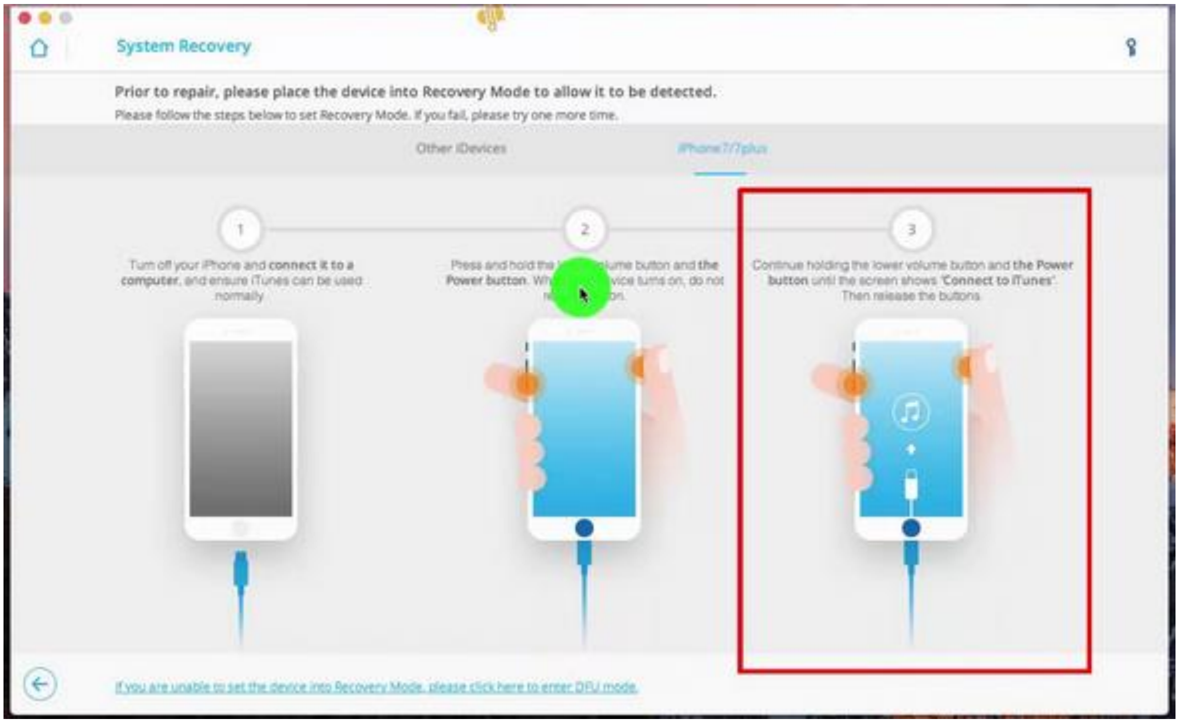
2 Hold **Power** and **Home** buttons at the same time for exact **10** seconds.

3 Release **Power** button.

Keep holding **Home** button.

Figure 10: iPhone in normal mode (Get iPad/ iPhone out of Recovery Mode, 2012)

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).



System Recovery

Prior to repair, please place the device into Recovery Mode to allow it to be detected.

Please follow the steps below to set Recovery Mode. If you fail, please try one more time.

1 Turn off your iPhone and **connect it to a computer**, and ensure iTunes can be used normally

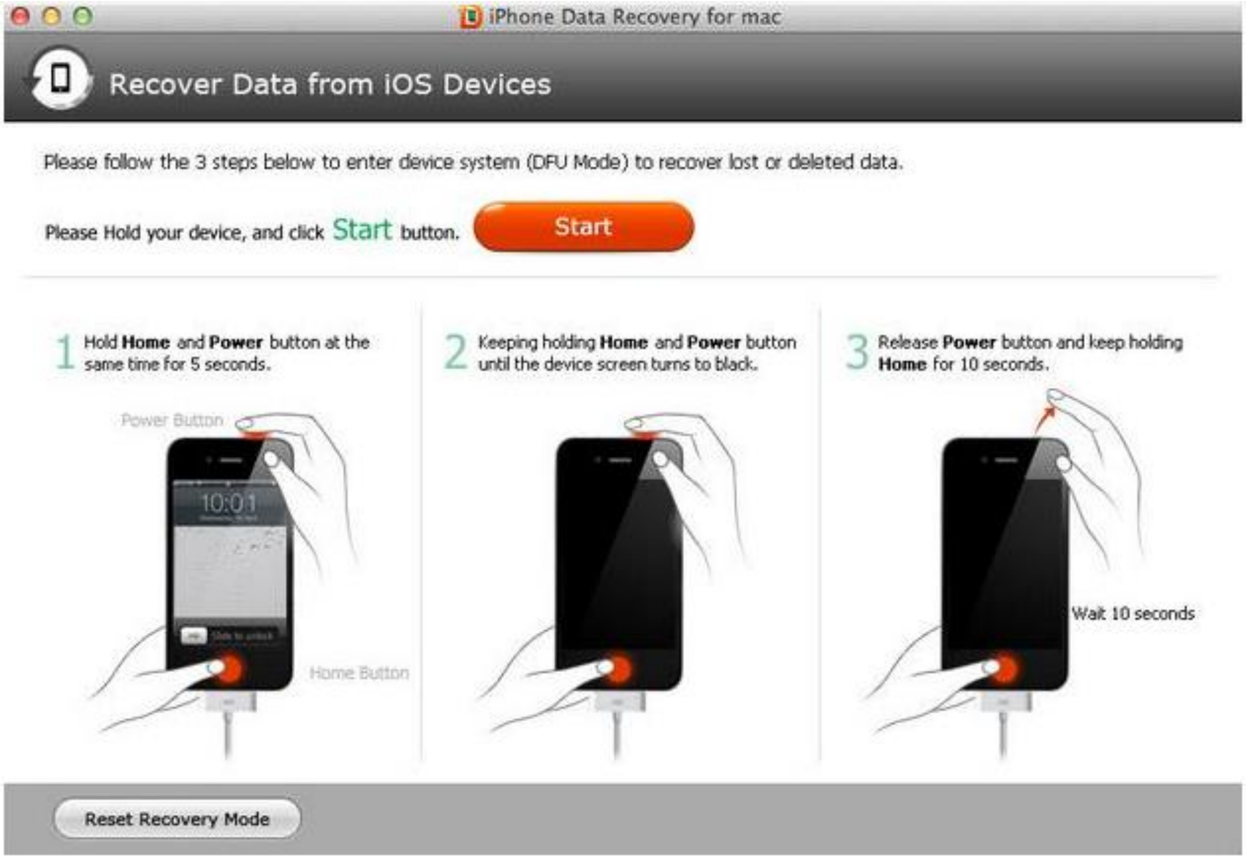
2 Press and hold the [illegible]lume button and **the Power button**. Wh[illegible]vice turns on, do not re[illegible]on.

3 Continue holding the lower volume button and **the Power button** until the screen shows '**Connect to iTunes**'. Then release the buttons

If you are unable to set the device into Recovery Mode, please click here to enter DFU mode.

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.).



Recover Data from iOS Devices

Please follow the 3 steps below to enter device system (DFU Mode) to recover lost or deleted data.

Please Hold your device, and click Start button.

1 Hold **Home** and **Power** button at the same time for 5 seconds.

2 Keeping holding **Home** and **Power** button until the device screen turns to black.

3 Release **Power** button and keep holding **Home** for 10 seconds.

Figure 12: iPhone in DFU mode (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.

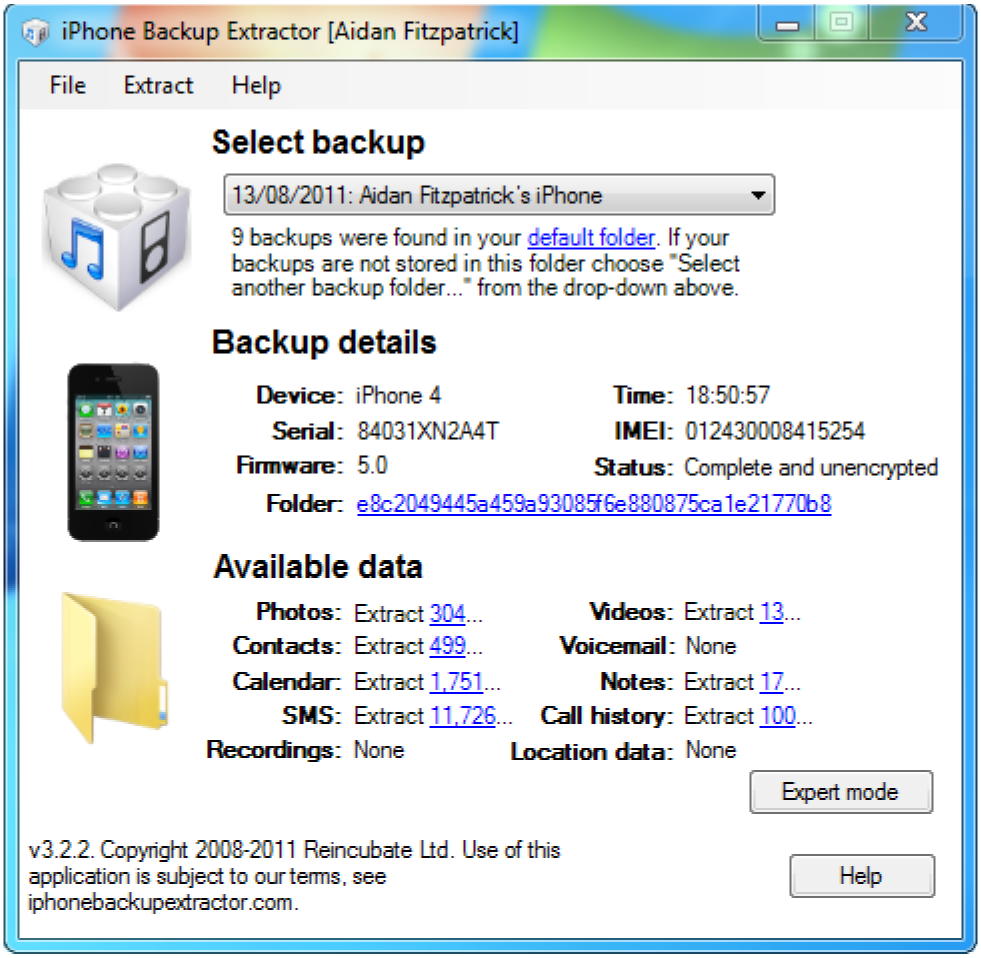
iPhone backup extractor. This is an open source tool, which can extract data from the device as well as iCloud backup (iPhone Backup Extractor, n.d.)

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.



Select backup

13/08/2011: Aidan Fitzpatrick's iPhone

9 backups were found in your default folder. If your backups are not stored in this folder choose "Select another backup folder..." from the drop-down above.

Backup details

Device:	iPhone 4	Time:	18:50:57
Serial:	84031XN2A4T	IMEI:	012430008415254
Firmware:	5.0	Status:	Complete and unencrypted
Folder:	e8c2049445a459a93085f6e880875ca1e21770b8		

Available data

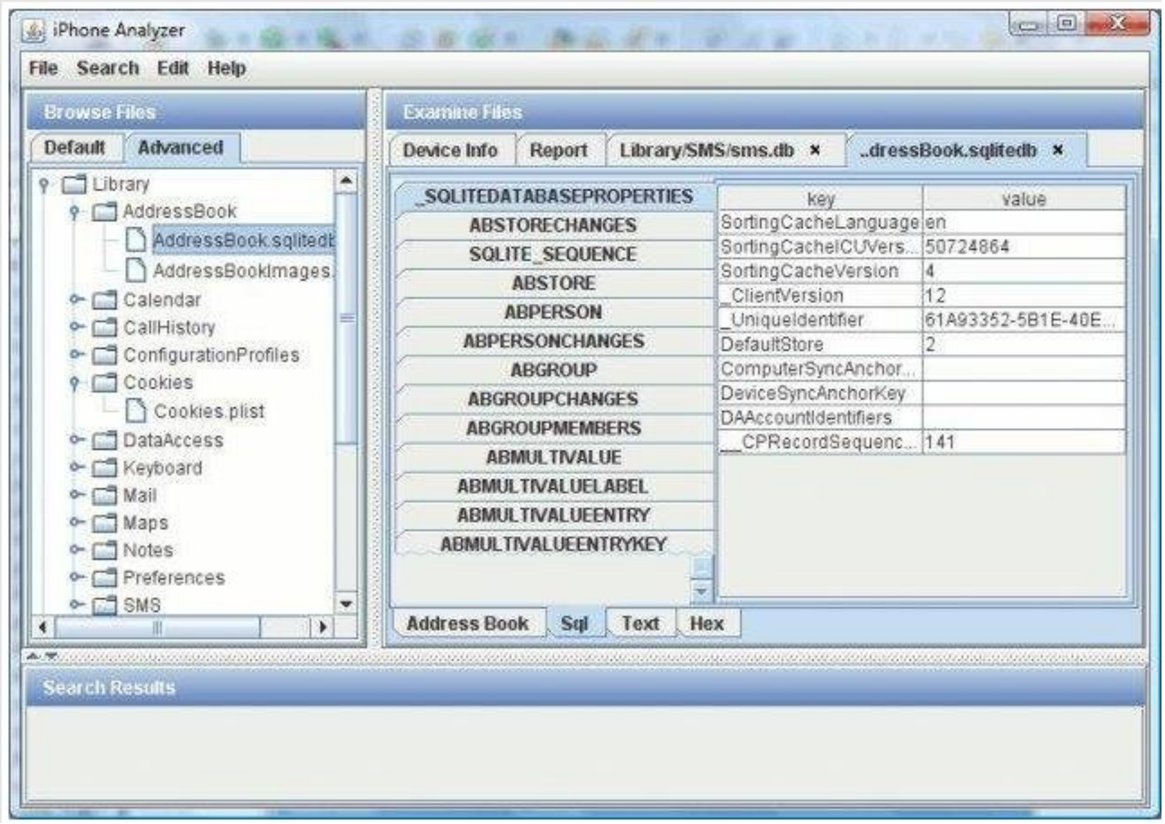
Photos:	Extract 304...	Videos:	Extract 13...
Contacts:	Extract 499...	Voicemail:	None
Calendar:	Extract 1,751...	Notes:	Extract 17...
SMS:	Extract 11,726...	Call history:	Extract 100...
Recordings:	None	Location data:	None

v3.2.2. Copyright 2008-2011 Reincubate Ltd. Use of this application is subject to our terms, see iphonebackupextractor.com.

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.”

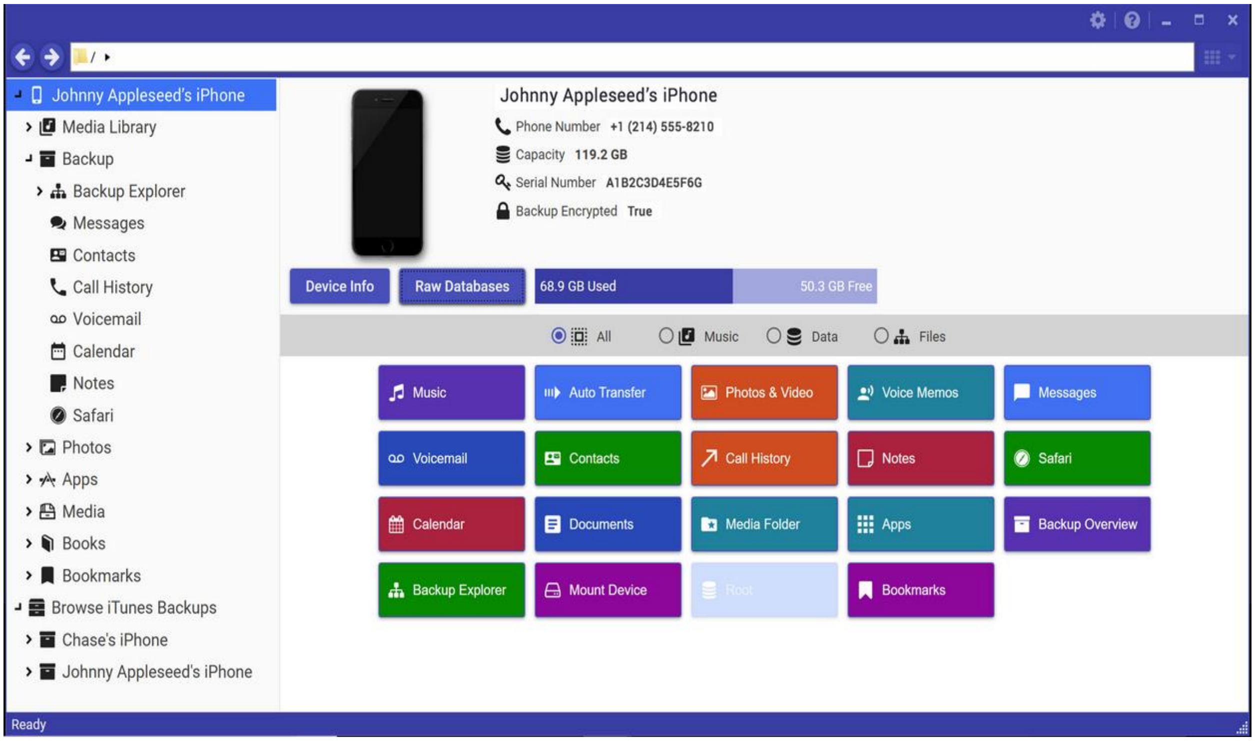
iPhone analyzer. It is a free tool built using java programming language for iOS backup developed by Crypticbit. This has a multi-platform for getting the data. Using this tool, the iOS file system can be viewed easily. The data here is retrieved using iTunes backup so there is no need to worry about 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).



key	value
SortingCacheLanguage	en
SortingCacheICUVers...	50724864
SortingCacheVersion	4
_ClientVersion	12
_UniqueIdentifier	61A93352-5B1E-40E...
DefaultStore	2
ComputerSyncAnchor...	
DeviceSyncAnchorKey	
DAAccountIdentifiers	
__CPRecordSequenc...	141

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.)



Johnny Appleseed's iPhone

Phone Number +1 (214) 555-8210

Capacity 119.2 GB

Serial Number A1B2C3D4E5F6G

Backup Encrypted True

68.9 GB Used

50.3 GB Free

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.

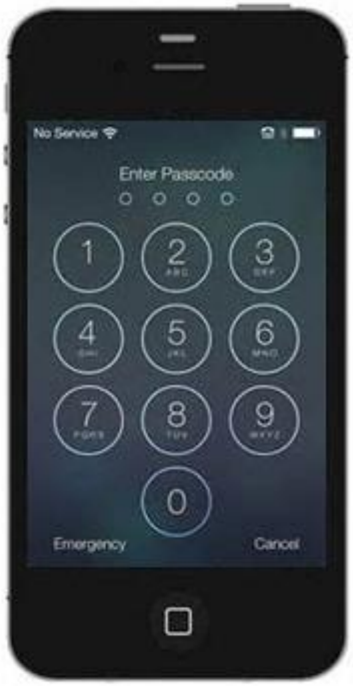


Figure 16*:* Passcode feature in iPhone 4s (iPhone 4S, n.d.)

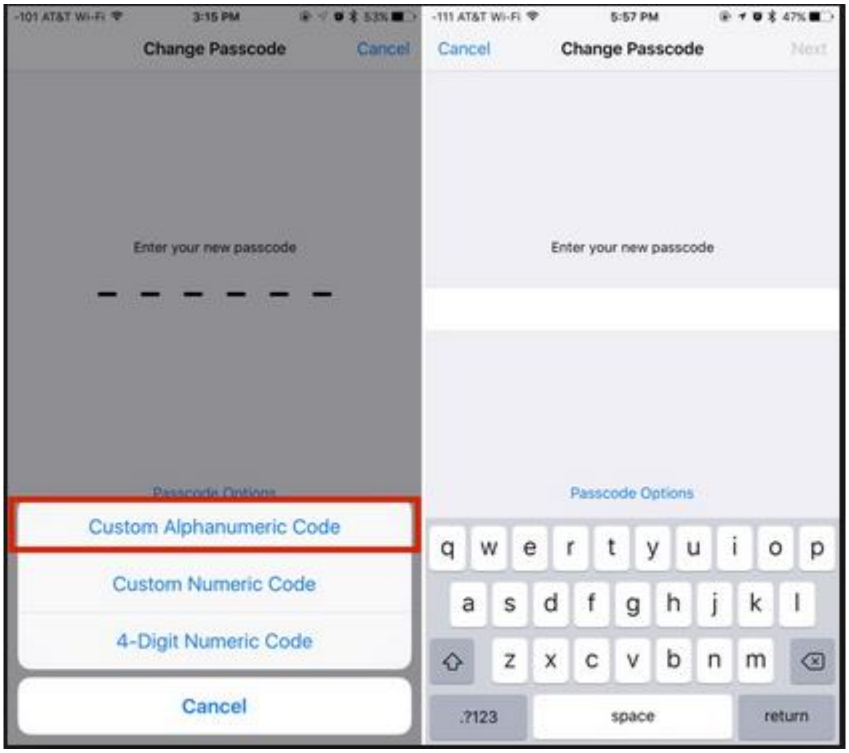
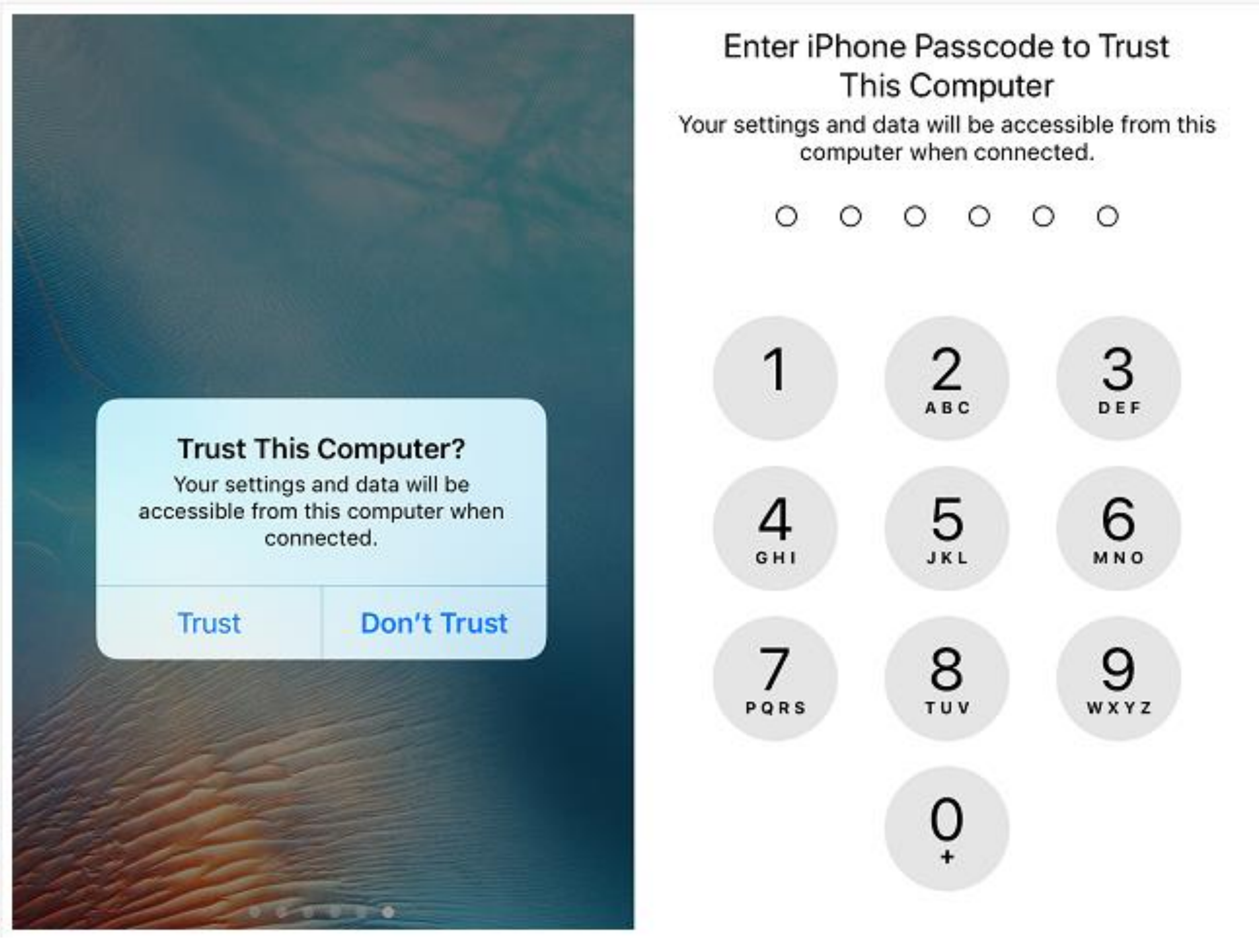


Figure 17: Passcode in iPhone 7plus (passcode on iPhone 7plus, n.d.)

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).



Trust This Computer?

Your settings and data will be accessible from this computer when connected.

Enter iPhone Passcode to Trust This Computer

Your settings and data will be accessible from this computer when connected.

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 7plus 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

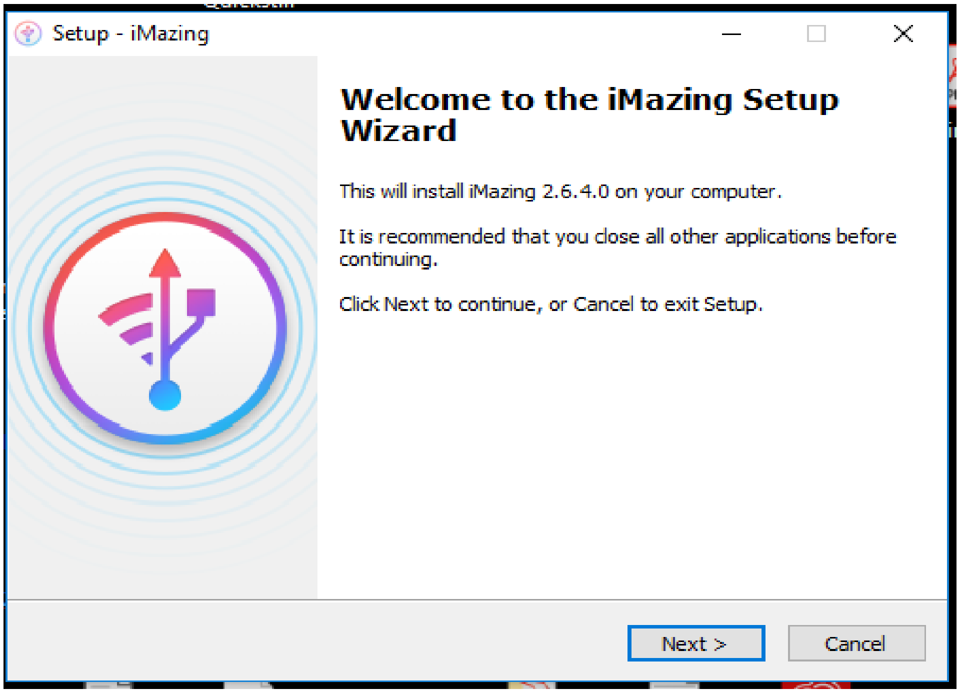
In this chapter, All the data collected as part of my experiment will be presented and analyzed.

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.



Setup - iMazing

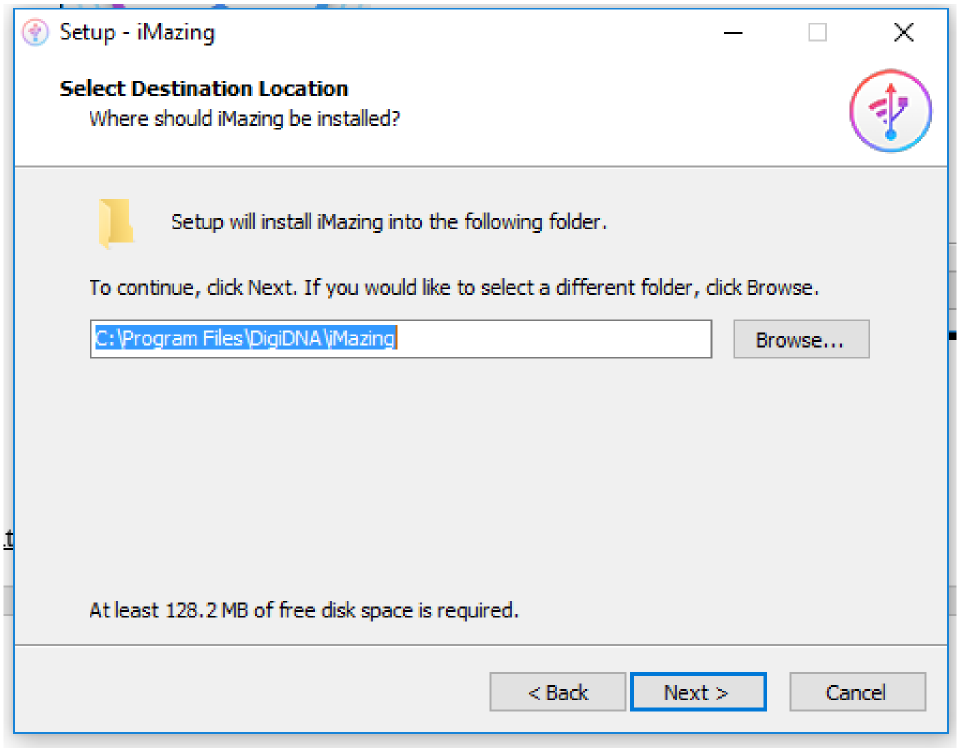
Welcome to the iMazing Setup Wizard

This will install iMazing 2.6.4.0 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 19: Installation of iMazing(a)



Setup - iMazing

Select Destination Location

Where should iMazing be installed?

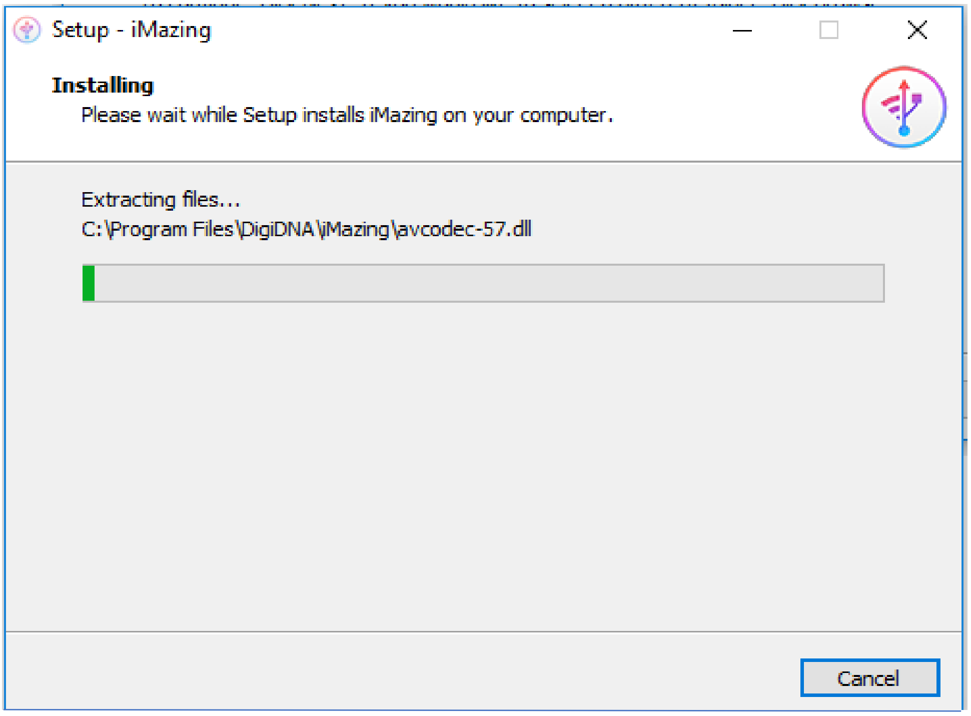
Setup will install iMazing into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\DigiDNA\iMazing

At least 128.2 MB of free disk space is required.

Figure 20: Installation of iMazing(b)

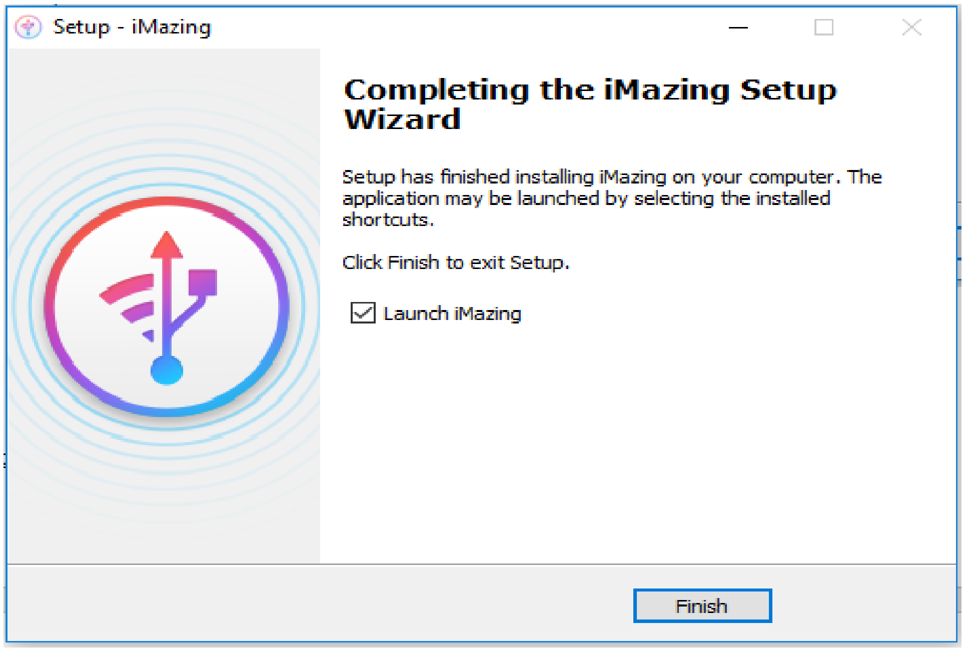


Installing

Please wait while Setup installs iMazing on your computer.

Extracting files...
C:\Program Files\DigiDNA\iMazing\avcodec-57.dll

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



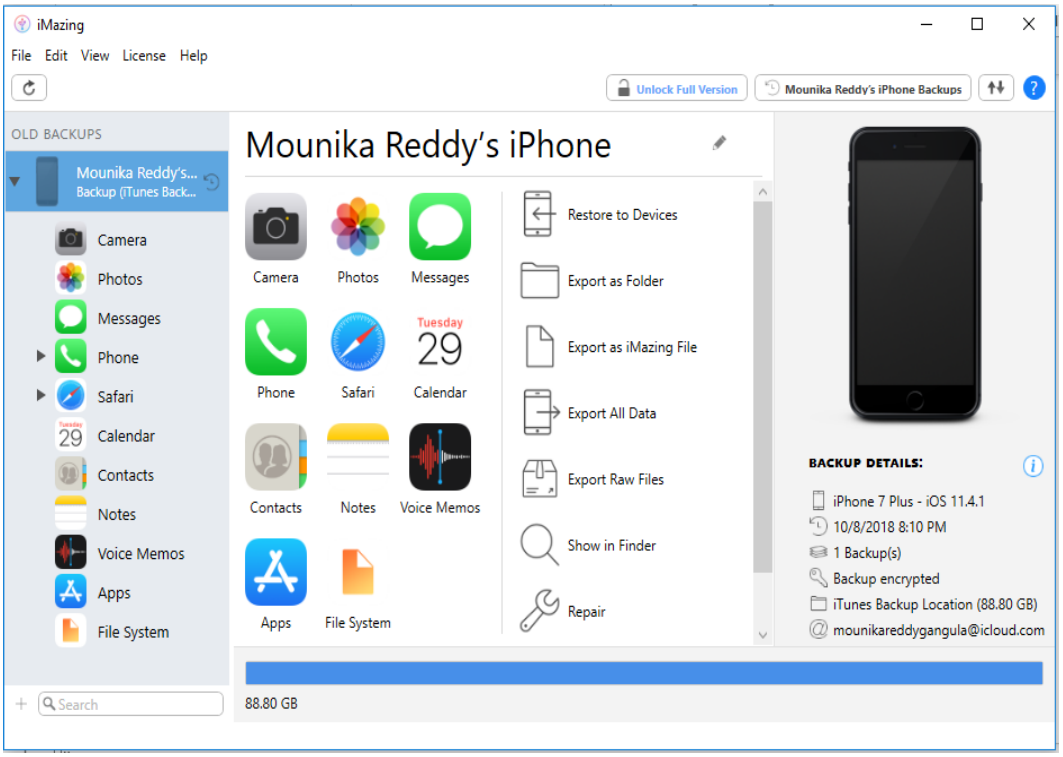
Completing the iMazing Setup Wizard

Setup has finished installing iMazing on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Launch iMazing

Figure 22*:* Installation of iMazing(d)



BACKUP DETAILS:

iPhone 7 Plus - iOS 11.4.1

10/8/2018 8:10 PM

1 Backup(s)

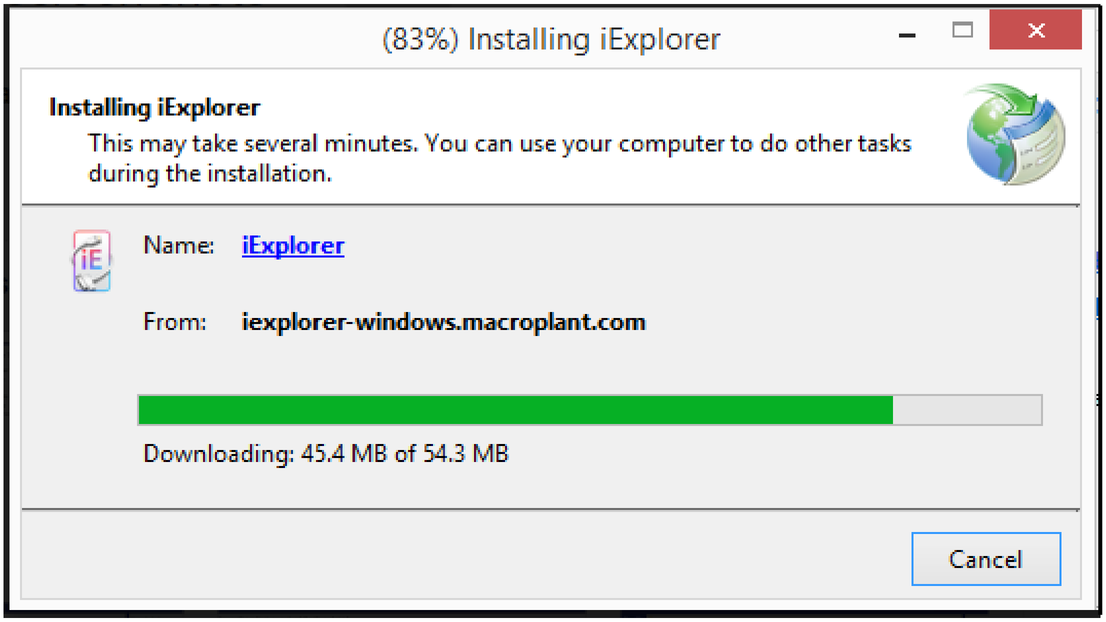
Backup encrypted

iTunes Backup Location (88.80 GB)

mounikareddygangula@icloud.com

Figure 23: Analyzing iMazing against backup data

iExplorer.



Installing iExplorer

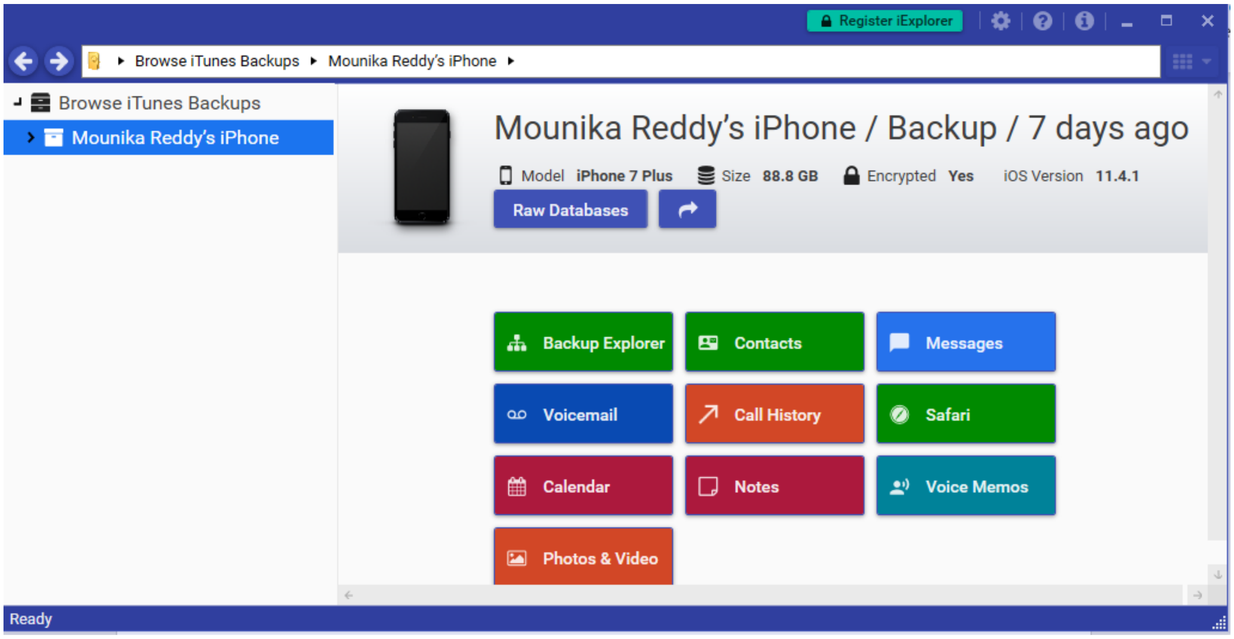
This may take several minutes. You can use your computer to do other tasks during the installation.

Name: iExplorer

From: iexplorer-windows.macroplant.com

Downloading: 45.4 MB of 54.3 MB

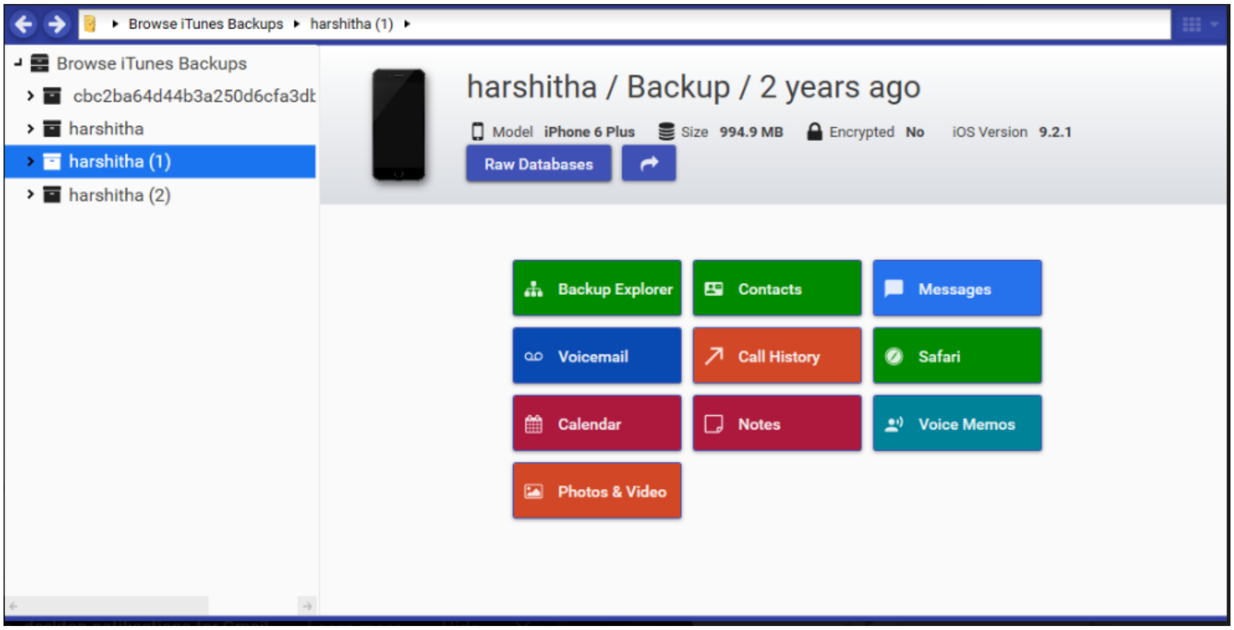
Figure 24: Installation of iExplorer



Mounika Reddy's iPhone / Backup / 7 days ago

Model iPhone 7 Plus Size 88.8 GB Encrypted Yes iOS Version 11.4.1

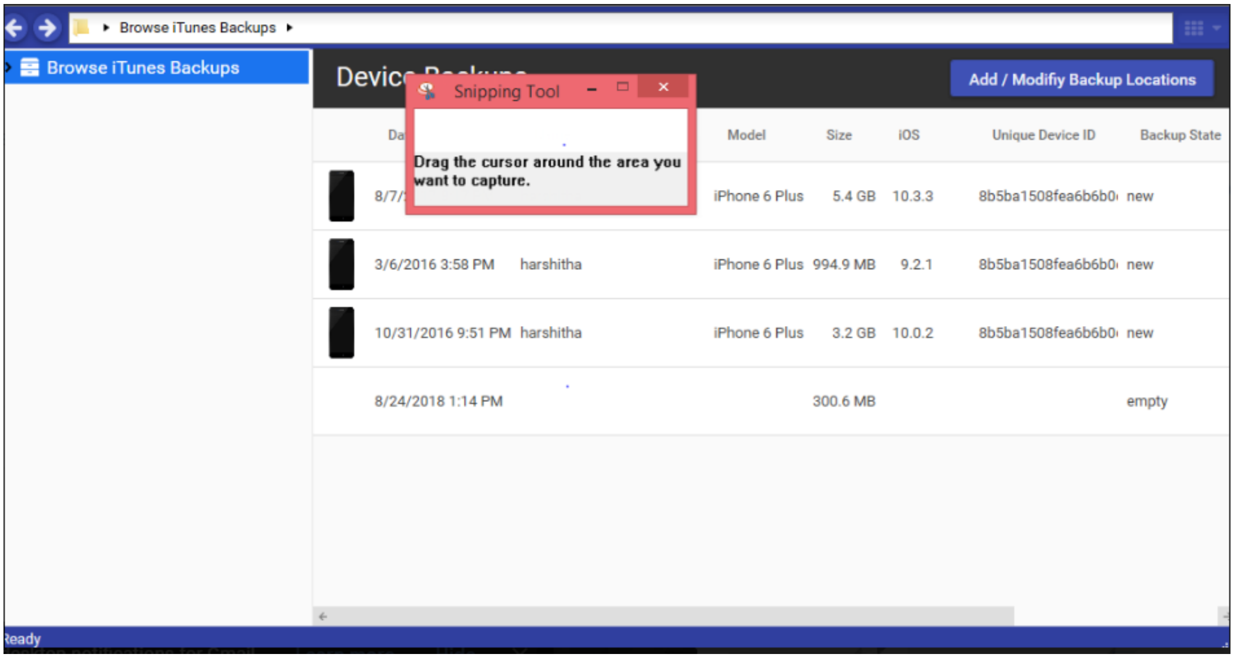
Figure 25: Analyzing iExplorer against iPhone 7plus



harshitha / Backup / 2 years ago

Model iPhone 6 Plus Size 994.9 MB Encrypted No iOS Version 9.2.1

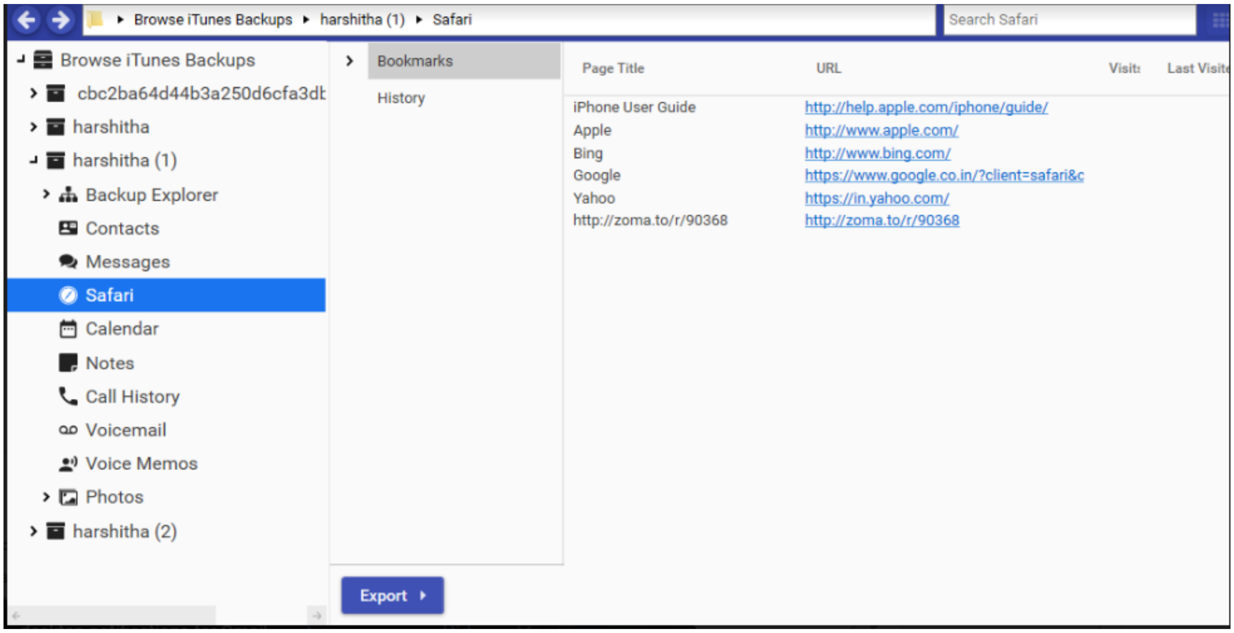
Figure 26: Analyzing iExplorer against iPhone 6plus



Drag the cursor around the area you want to capture.

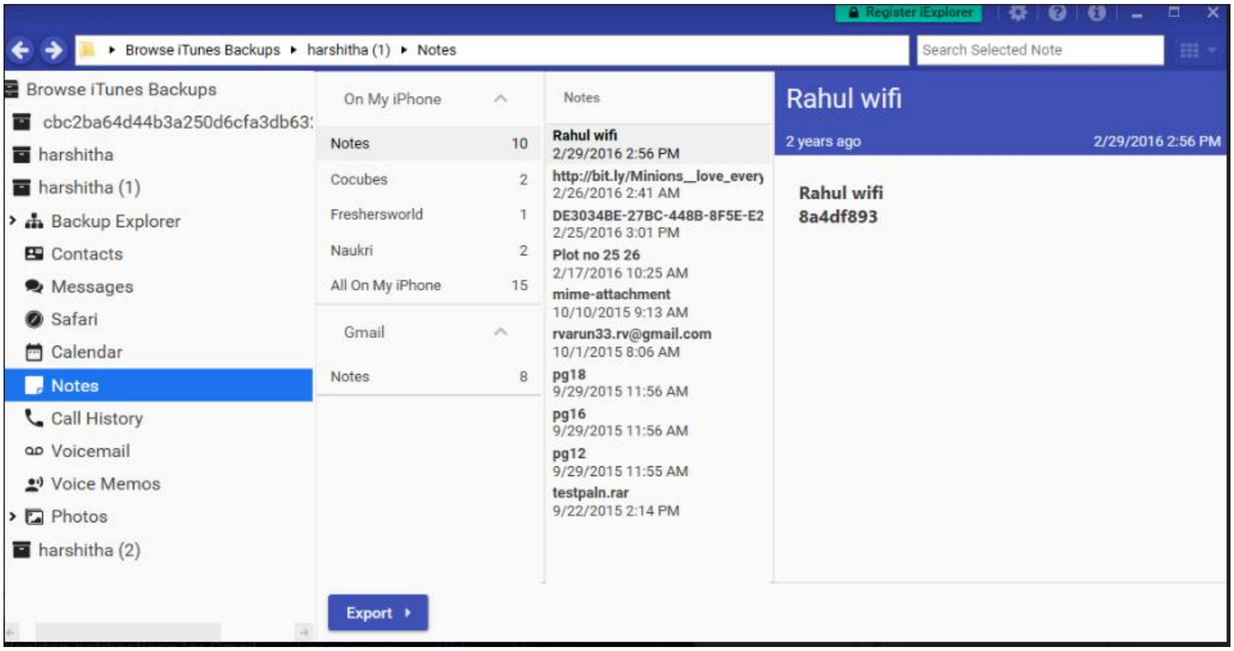
Da		Model	Size	iOS	Unique Device ID	Backup State
8/7/		iPhone 6 Plus	5.4 GB	10.3.3	8b5ba1508fea6b6b0	new
3/6/2016 3:58 PM	harshitha	iPhone 6 Plus	994.9 MB	9.2.1	8b5ba1508fea6b6b0	new
10/31/2016 9:51 PM	harshitha	iPhone 6 Plus	3.2 GB	10.0.2	8b5ba1508fea6b6b0	new
8/24/2018 1:14 PM			300.6 MB			empty

Figure 27: Analyzing backups of iPhone 6plus



Page Title	URL	Visit:	Last Visite
iPhone User Guide	http://help.apple.com/iphone/guide/		
Apple	http://www.apple.com/		
Bing	http://www.bing.com/		
Google	https://www.google.co.in/?client=safari&c		
Yahoo	https://in.yahoo.com/		
http://zoma.to/r/90368	http://zoma.to/r/90368		

Figure 28: Analyzing Safari in iExplorer of iPhone 6 plus



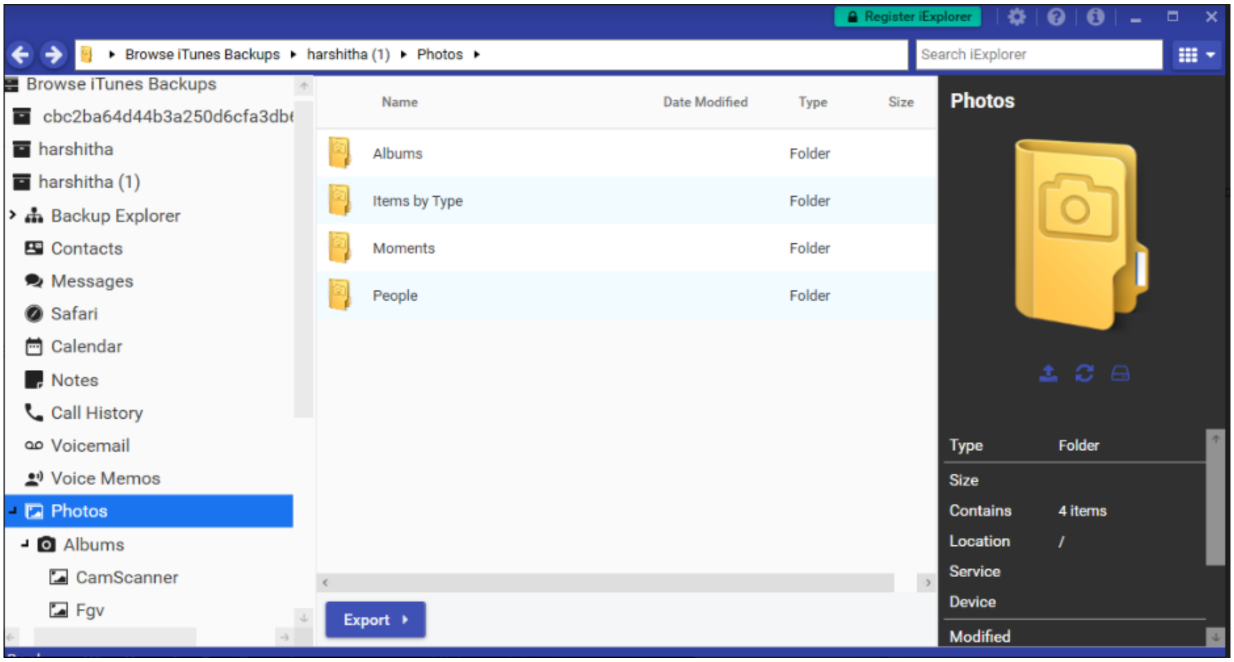
On My iPhone	
Notes	10
Cocubes	2
Freshersworld	1
Naukri	2
All On My iPhone	15
Gmail	
Notes	8

Rahul wifi
2/29/2016 2:56 PM
http://bit.ly/Minions__love_every
2/26/2016 2:41 AM
DE3034BE-27BC-448B-8F5E-E2
2/25/2016 3:01 PM
Plot no 25 26
2/17/2016 10:25 AM
mime-attachment
10/10/2015 9:13 AM
rvarun33.rv@gmail.com
10/1/2015 8:06 AM
pg18
9/29/2015 11:56 AM
pg16
9/29/2015 11:56 AM
pg12
9/29/2015 11:55 AM
testpaln.rar
9/22/2015 2:14 PM

Rahul wifi
2 years ago 2/29/2016 2:56 PM

Rahul wifi
8a4df893

Figure 29: Analyzing notes in iExplorer of iPhone 6plus



Name	Date Modified	Type	Size
Albums		Folder	
Items by Type		Folder	
Moments		Folder	
People		Folder	

Type	Folder
Size	
Contains	4 items
Location	/
Service	
Device	
Modified	

Figure 30: Analyzing photos in iExplorer of iPhone 6plus

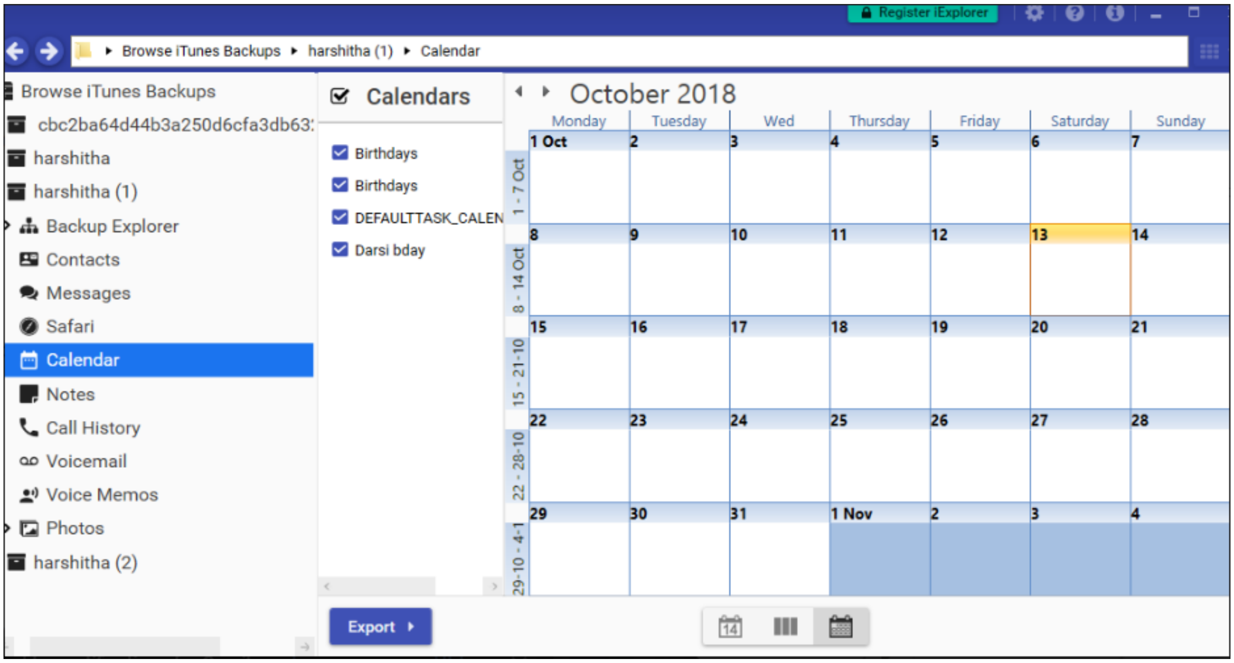
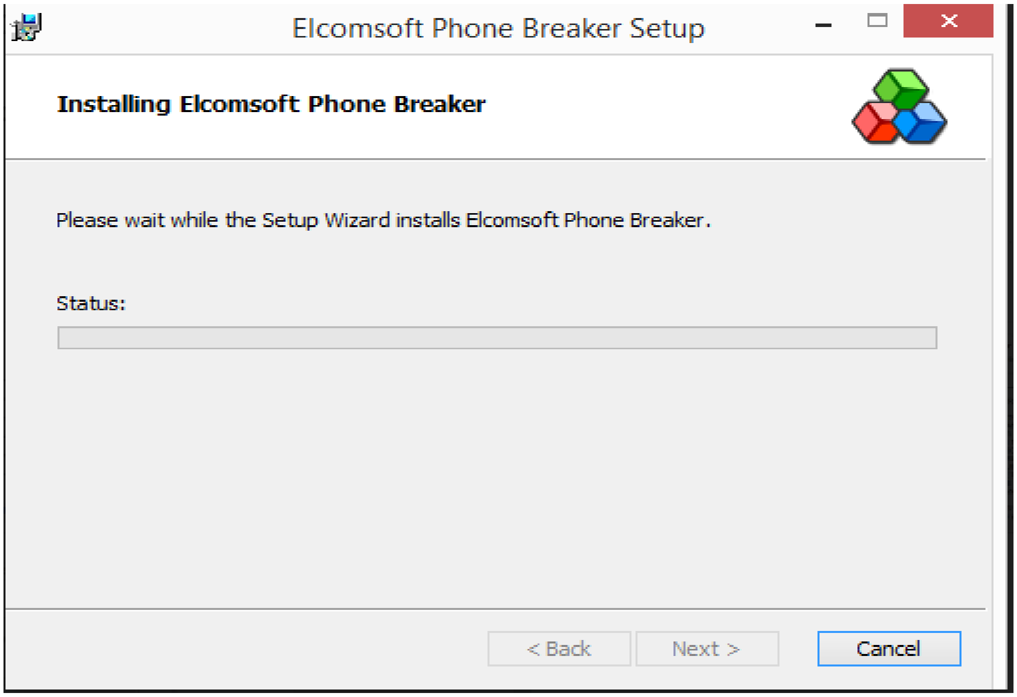


Figure 31: Analyzing calendar in iExplorer of iPhone 6plus

Elcomsoft phone breaker.



Installing Elcomsoft Phone Breaker

Please wait while the Setup Wizard installs Elcomsoft Phone Breaker.

Status:

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.

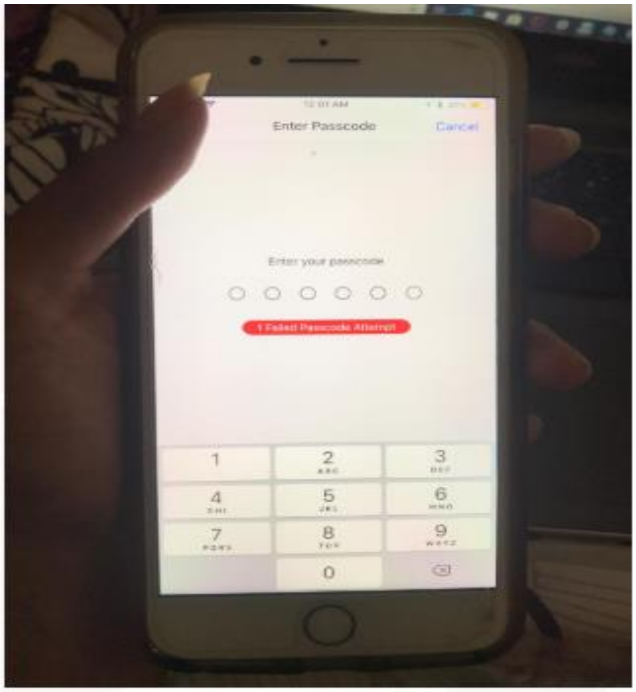
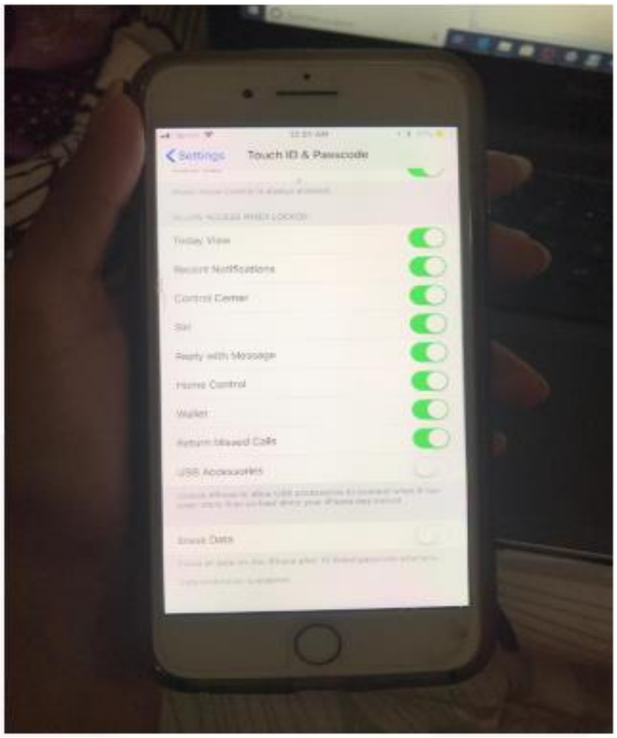


Figure 33: Failed passcode attempts count

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.



< Settings Touch ID & Passcode

ALLOW ACCESS WHEN LOCKED:

Today View ●

Recent Notifications ●

Control Center ●

Siri ●

Reply with Message ●

Home Control ●

Wallet ●

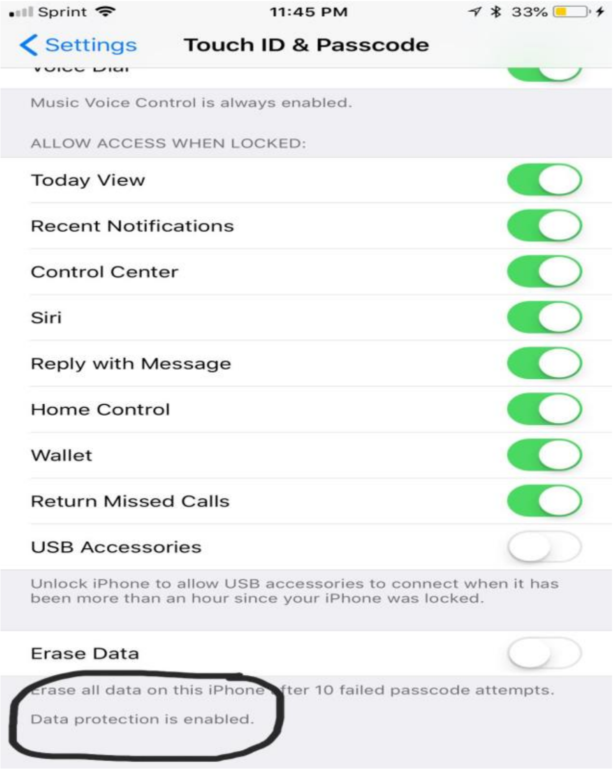
Return Missed Calls ●

USB Accessories ○

Erase Data ○

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.



Sprint 11:45 PM 33%

< Settings Touch ID & Passcode

Voice Dial ☑

Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

Today View ☑

Recent Notifications ☑

Control Center ☑

Siri ☑

Reply with Message ☑

Home Control ☑

Wallet ☑

Return Missed Calls ☑

USB Accessories □

Unlock iPhone to allow USB accessories to connect when it has been more than an hour since your iPhone was locked.

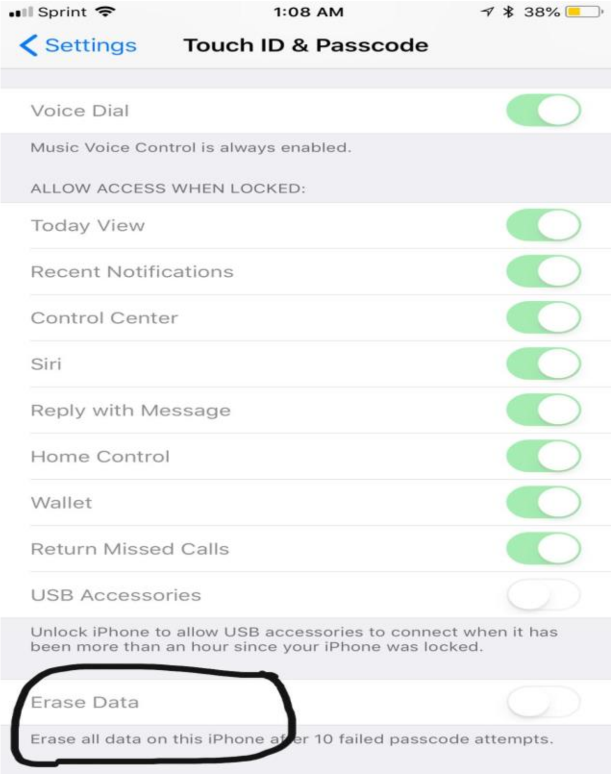
Erase Data □

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

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.



Voice Dial

Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

Today View

Recent Notifications

Control Center

Siri

Reply with Message

Home Control

Wallet

Return Missed Calls

USB Accessories

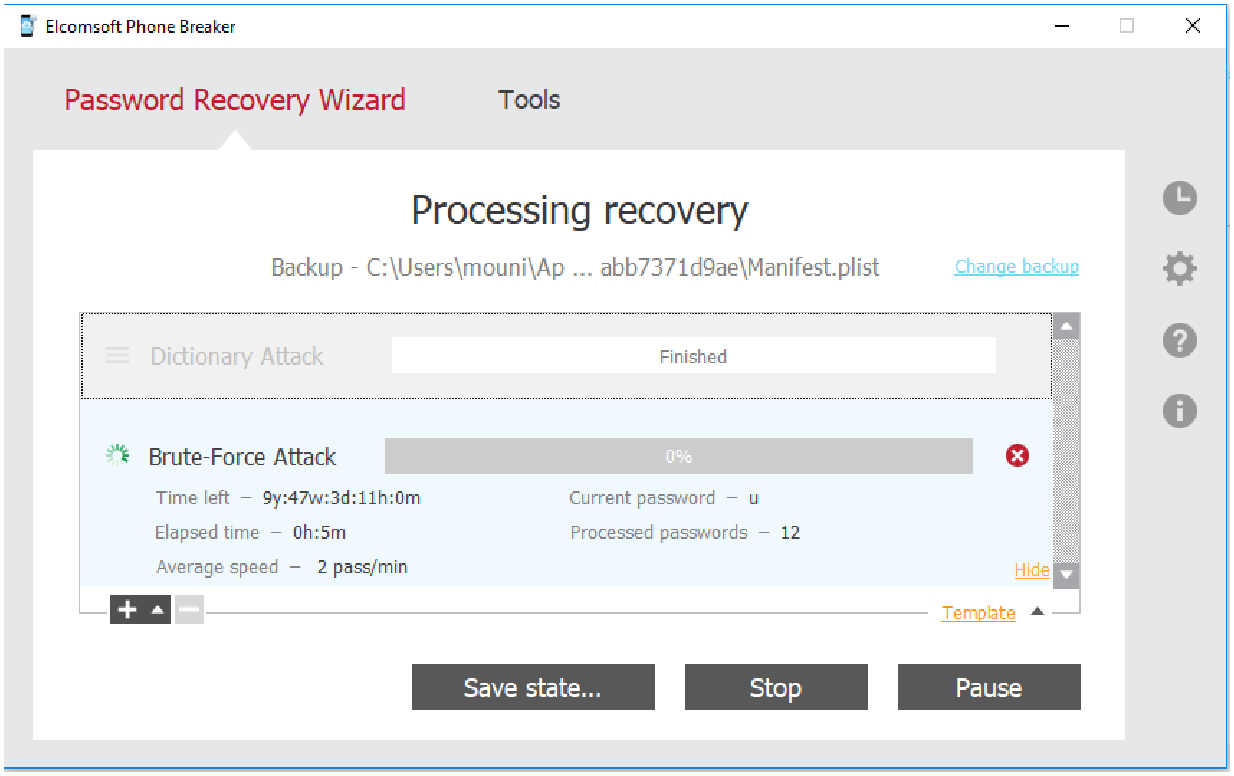
Unlock iPhone to allow USB accessories to connect when it has been more than an hour since your iPhone was locked.

Erase Data

Erase all data on this iPhone after 10 failed passcode attempts.

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.



Processing recovery

Backup - C:\Users\mouni\Ap ... abb7371d9ae\Manifest.plist

Dictionary Attack — Finished

Brute-Force Attack — 0%

Time left – 9y:47w:3d:11h:0m

Current password – u

Elapsed time – 0h:5m

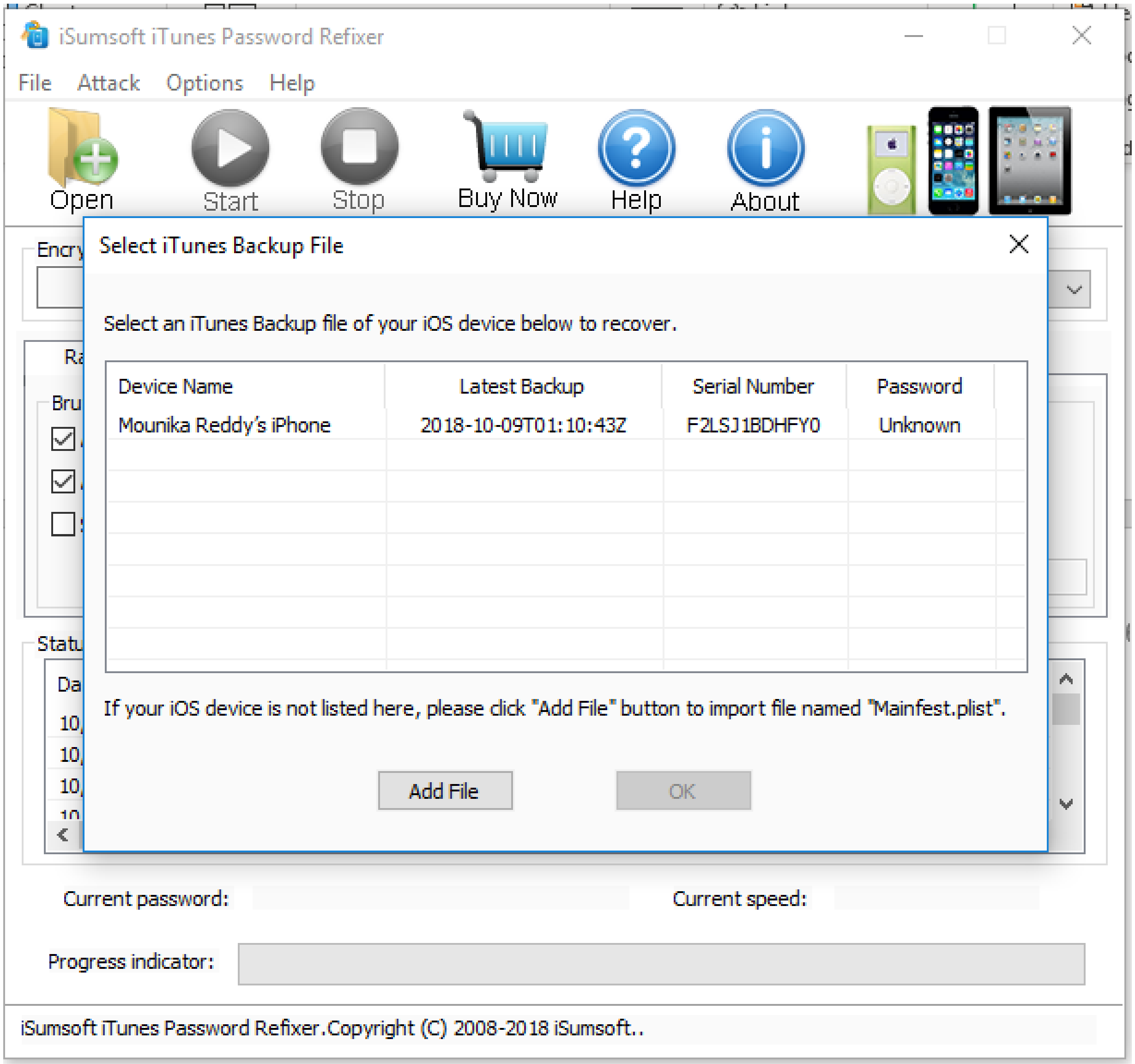
Processed passwords – 12

Average speed – 2 pass/min

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.



Select iTunes Backup File

Select an iTunes Backup file of your iOS device below to recover.

Device Name	Latest Backup	Serial Number	Password
Mounika Reddy's iPhone	2018-10-09T01:10:43Z	F2LSJ1BDHFY0	Unknown

If your iOS device is not listed here, please click "Add File" button to import file named "Mainfest.plist".

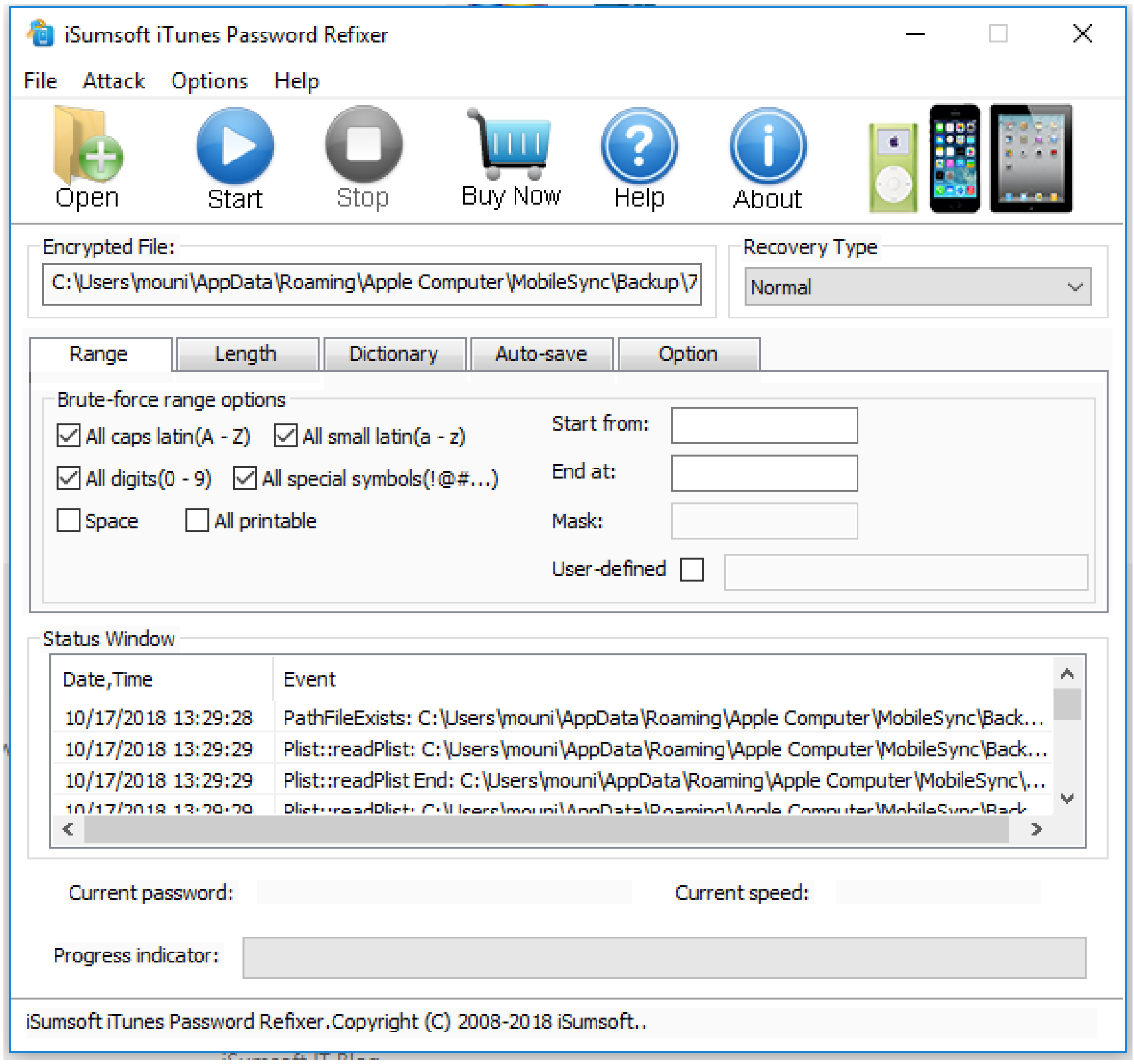
Current password:

Current speed:

Progress indicator:

iSumsoft iTunes Password Refixer.Copyright (C) 2008-2018 iSumsoft..

Figure 38: iSumsoft iTunes password refixer



Encrypted File: C:\Users\mouni\AppData\Roaming\Apple Computer\MobileSync\Backup\7

Recovery Type: Normal

Brute-force range options

☑ All caps latin(A - Z) ☑ All small latin(a - z)

☑ All digits(0 - 9) ☑ All special symbols(!@#...)

☐ Space ☐ All printable

Start from:

End at:

Mask:

User-defined ☐

Status Window

```
Date,Time              Event
10/17/2018 13:29:28    PathFileExists: C:\Users\mouni\AppData\Roaming\Apple Computer\MobileSync\Back...
10/17/2018 13:29:29    Plist::readPlist: C:\Users\mouni\AppData\Roaming\Apple Computer\MobileSync\Back...
10/17/2018 13:29:29    Plist::readPlist End: C:\Users\mouni\AppData\Roaming\Apple Computer\MobileSync\...
10/17/2018 13:29:29    Plist::readPlist: C:\Users\mouni\AppData\Roaming\Apple Computer\MobileSync\Back
```

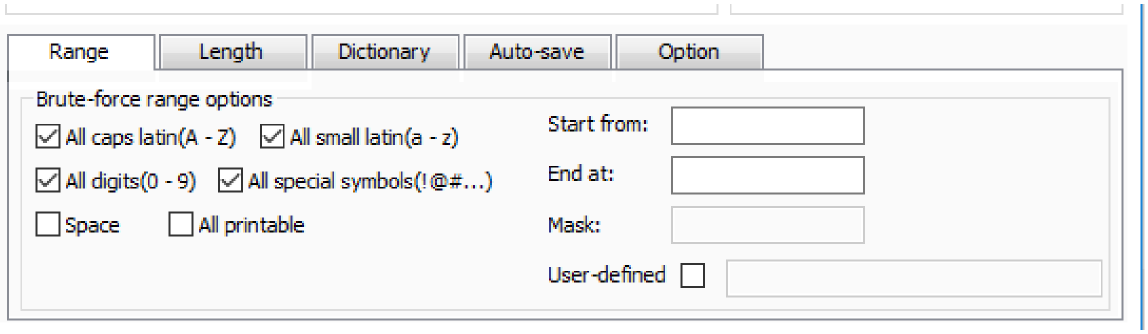
Current password:

Current speed:

Progress indicator:

iSumsoft iTunes Password Refixer.Copyright (C) 2008-2018 iSumsoft..

Figure 39: Initializing iSumsoft iTunes password refixer



Brute-force range options

☑ All caps latin(A - Z) ☑ All small latin(a - z)

☑ All digits(0 - 9) ☑ All special symbols(!@#...)

☐ Space ☐ All printable

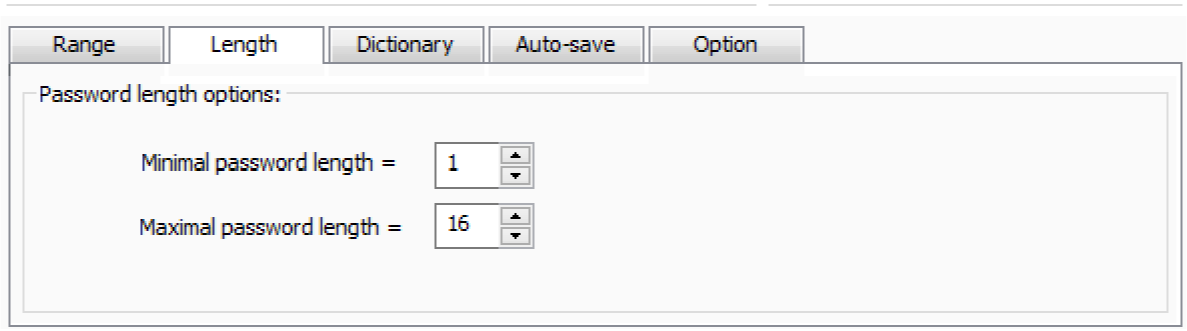
Start from:

End at:

Mask:

User-defined ☐

Figure 40: Setting the range

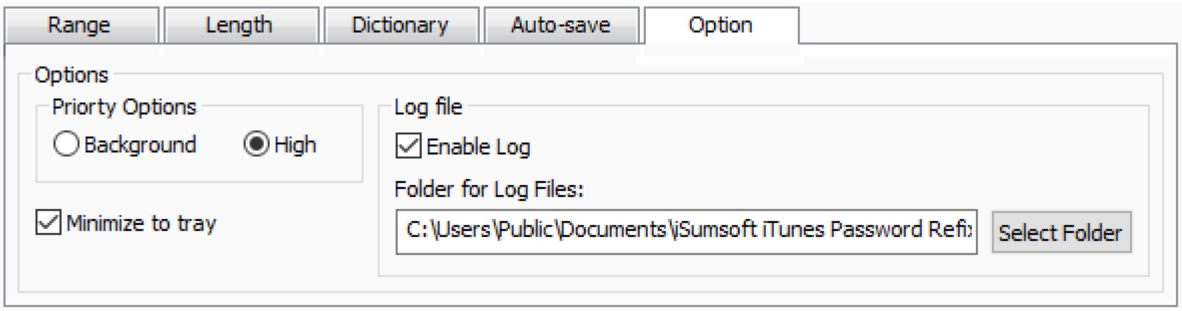


Password length options:

Minimal password length = 1

Maximal password length = 16

Figure 41: Setting the length



Options

Priorty Options

○ Background ● High

☑ Minimize to tray

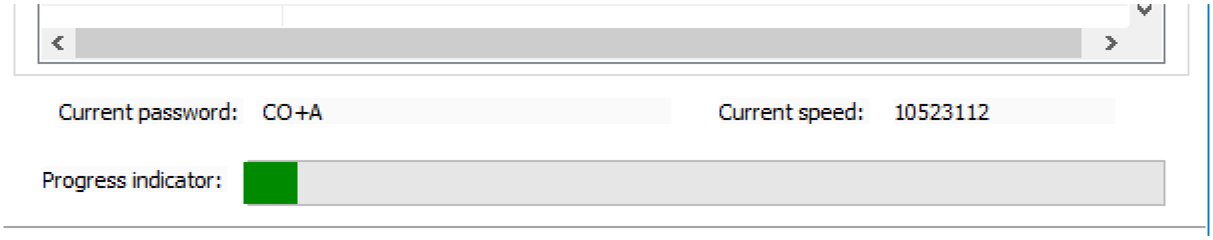
Log file

☑ Enable Log

Folder for Log Files:

C:\Users\Public\Documents\iSumsoft iTunes Password Refi:

Figure 42: Setting the logfile location



Current password: CO+A

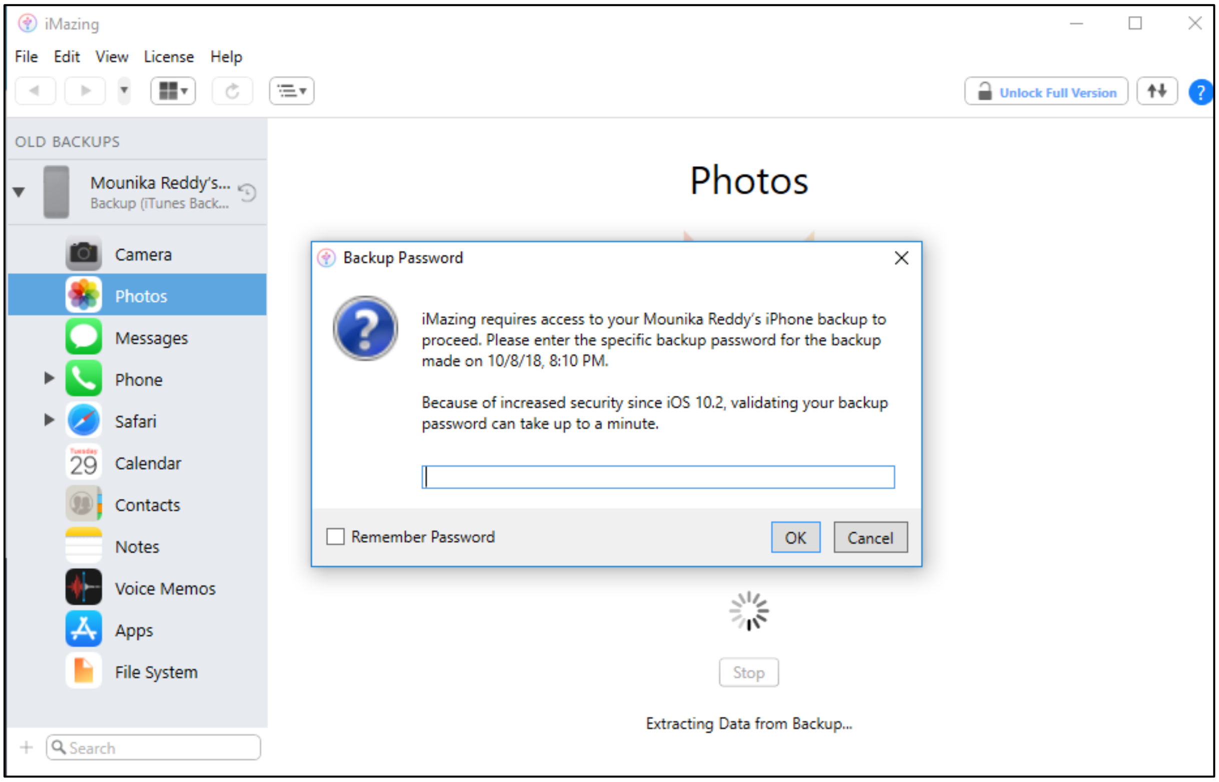
Current speed: 10523112

Progress indicator:

Figure 43: Processing the refixer

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.



Backup Password

iMazing requires access to your Mounika Reddy's iPhone backup to proceed. Please enter the specific backup password for the backup made on 10/8/18, 8:10 PM.

Because of increased security since iOS 10.2, validating your backup password can take up to a minute.

☐ Remember Password

Extracting Data from Backup...

Figure 44: Extracting backup data using iMazing

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.

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.

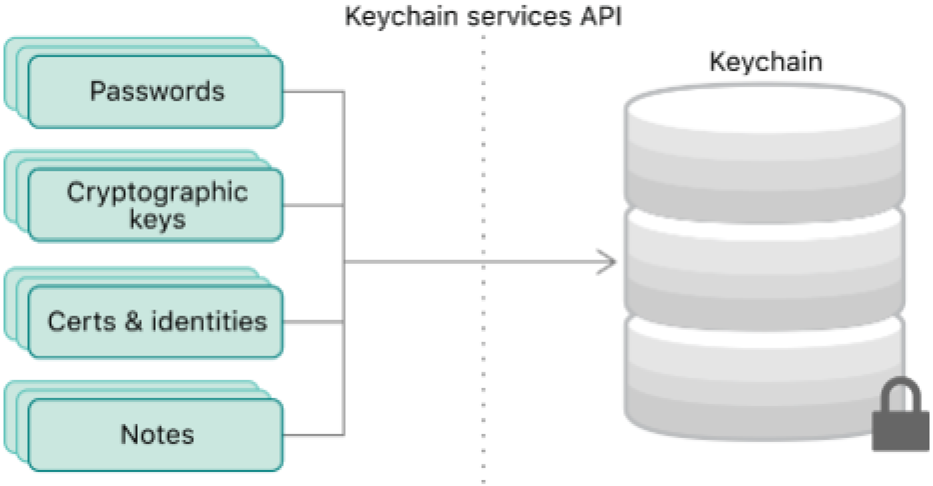


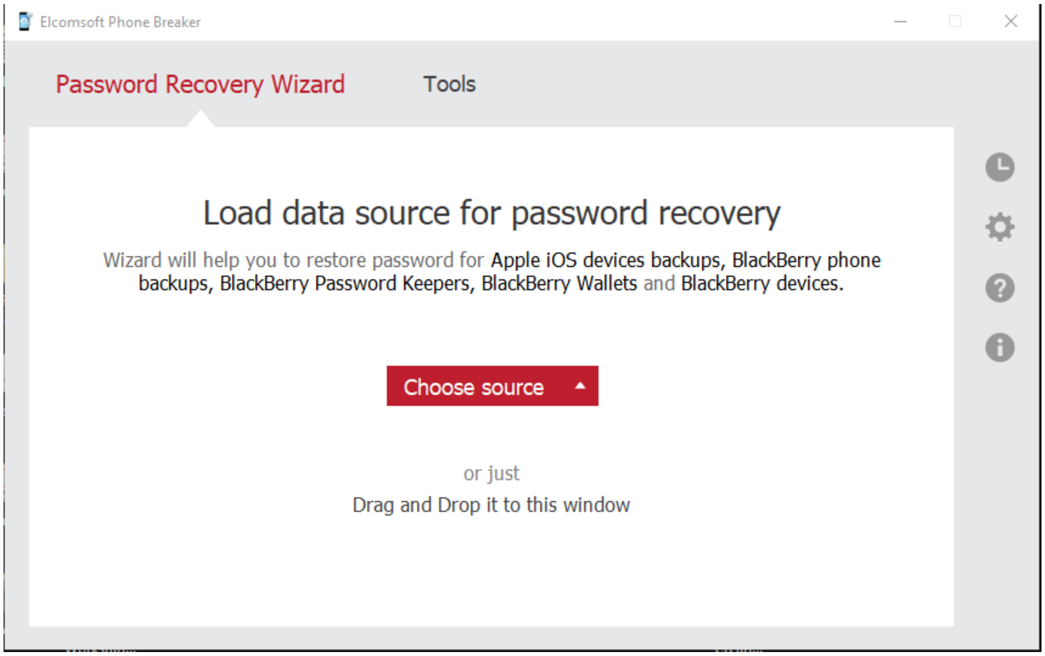
Figure 45: Securing the user’s secrets in a keychain (Apple, Inc, n.d.)

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.

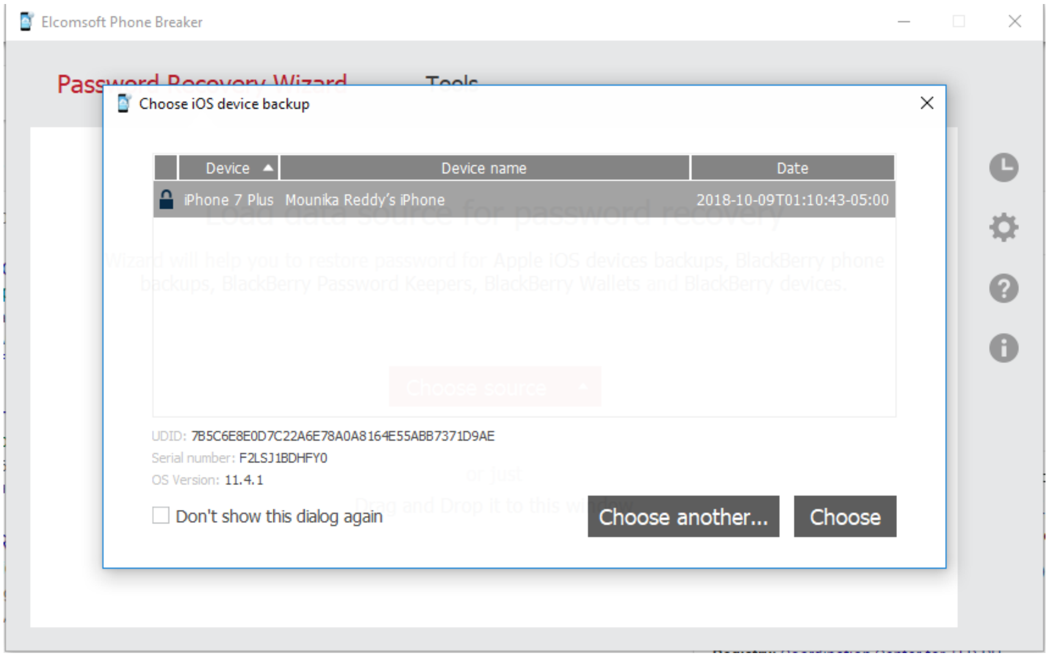


Load data source for password recovery

Wizard will help you to restore password for Apple iOS devices backups, BlackBerry phone backups, BlackBerry Password Keepers, BlackBerry Wallets and BlackBerry devices.

or just
Drag and Drop it to this window

Figure 46: Loading data for password recovery(a)

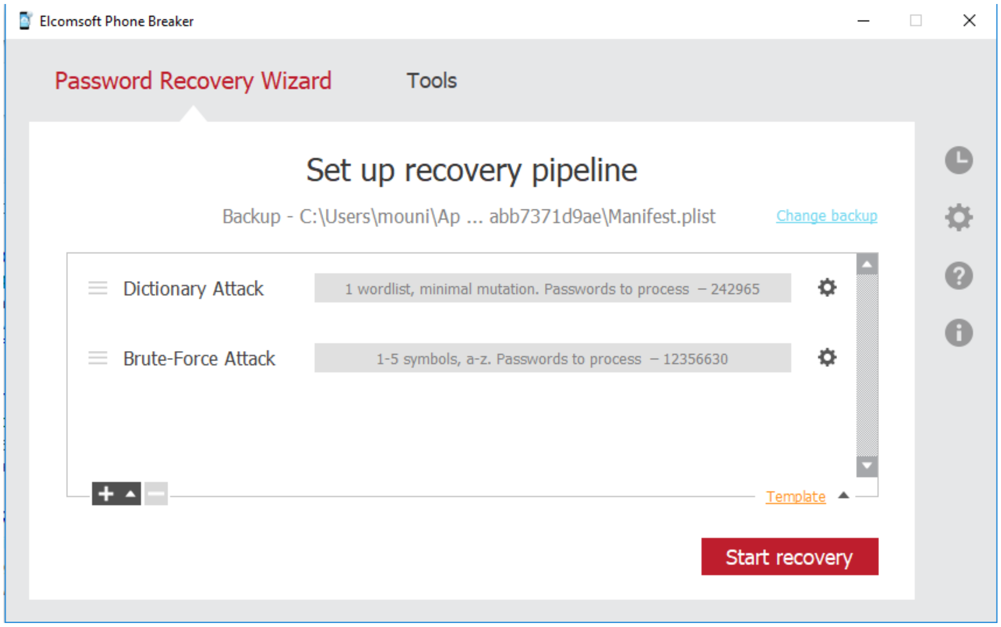


	Device	Device name	Date
🔒	iPhone 7 Plus	Mounika Reddy's iPhone	2018-10-09T01:10:43-05:00

UDID: 7B5C6E8E0D7C22A6E78A0A8164E55ABB7371D9AE
Serial number: F2LSJ1BDHFY0
OS Version: 11.4.1

□ Don't show this dialog again

Figure 47: Loading data for password recovery(b)



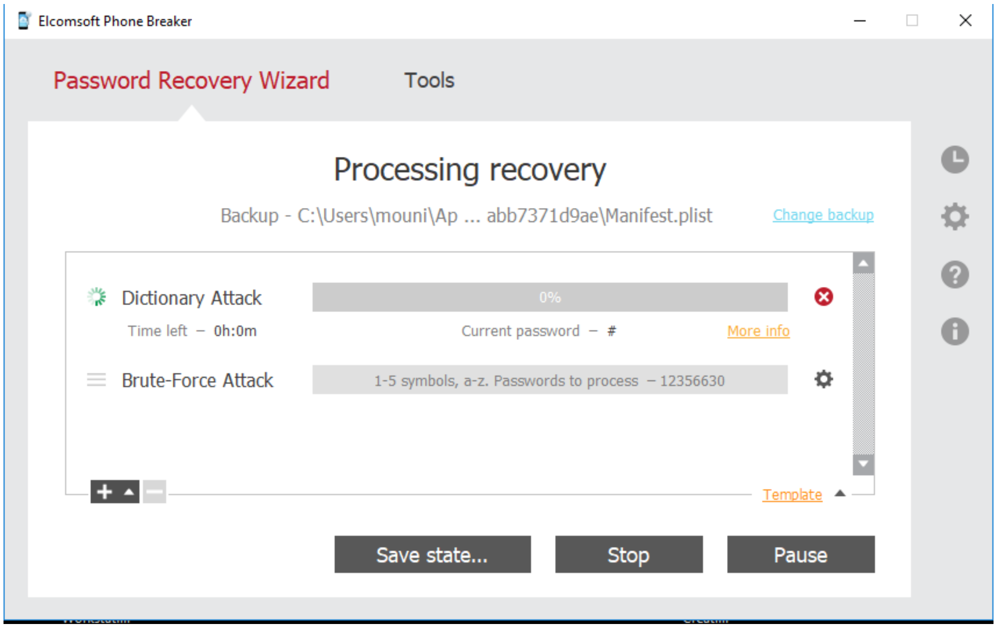
Set up recovery pipeline

Backup - C:\Users\mouni\Ap ... abb7371d9ae\Manifest.plist

Dictionary Attack — 1 wordlist, minimal mutation. Passwords to process – 242965

Brute-Force Attack — 1-5 symbols, a-z. Passwords to process – 12356630

Figure 48: Attacks for password recovery



Processing recovery

Backup - C:\Users\mouni\Ap ... abb7371d9ae\Manifest.plist

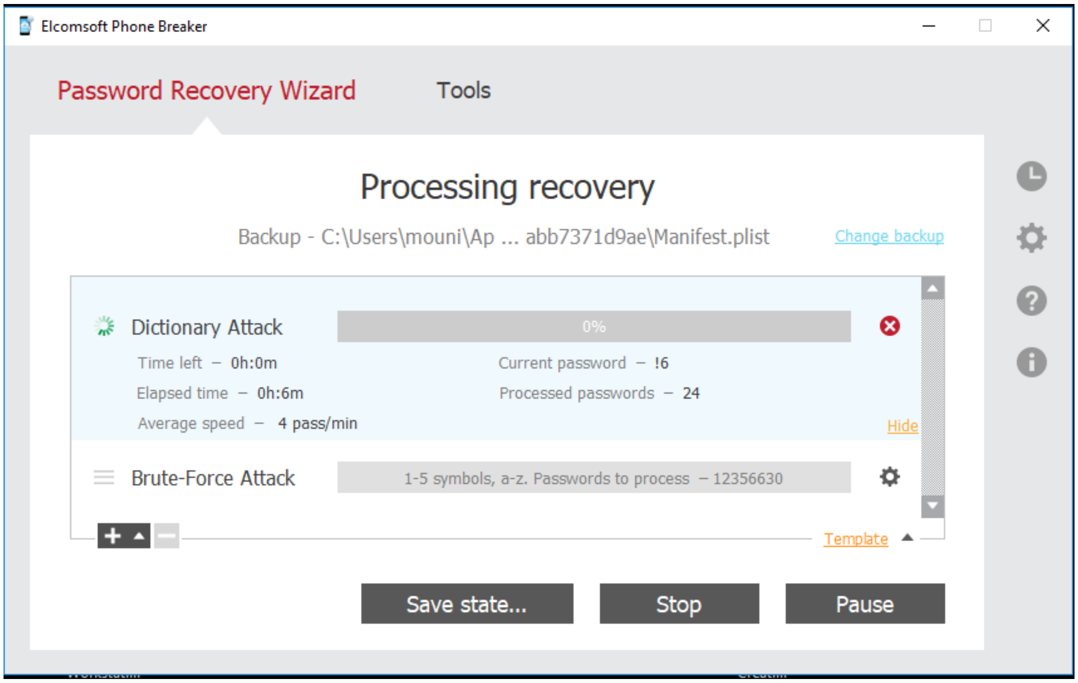
Dictionary Attack — 0%

Time left – 0h:0m

Current password – #

Brute-Force Attack — 1-5 symbols, a-z. Passwords to process – 12356630

Figure 49: Processing dictionary attack(a)



Processing recovery

Backup - C:\Users\mouni\Ap ... abb7371d9ae\Manifest.plist

Dictionary Attack 0%

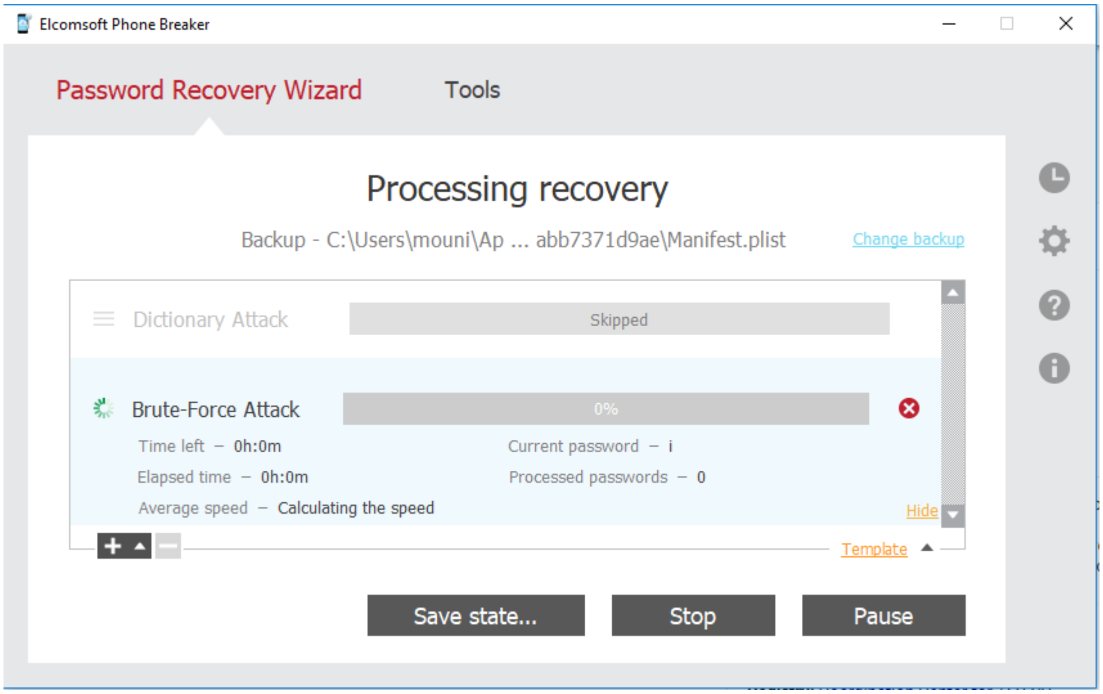
Time left – 0h:0m Current password – !6

Elapsed time – 0h:6m Processed passwords – 24

Average speed – 4 pass/min

Brute-Force Attack 1-5 symbols, a-z. Passwords to process – 12356630

Figure 50: Processing dictionary attack(b)



Processing recovery

Backup - C:\Users\mouni\Ap ... abb7371d9ae\Manifest.plist

Dictionary Attack Skipped

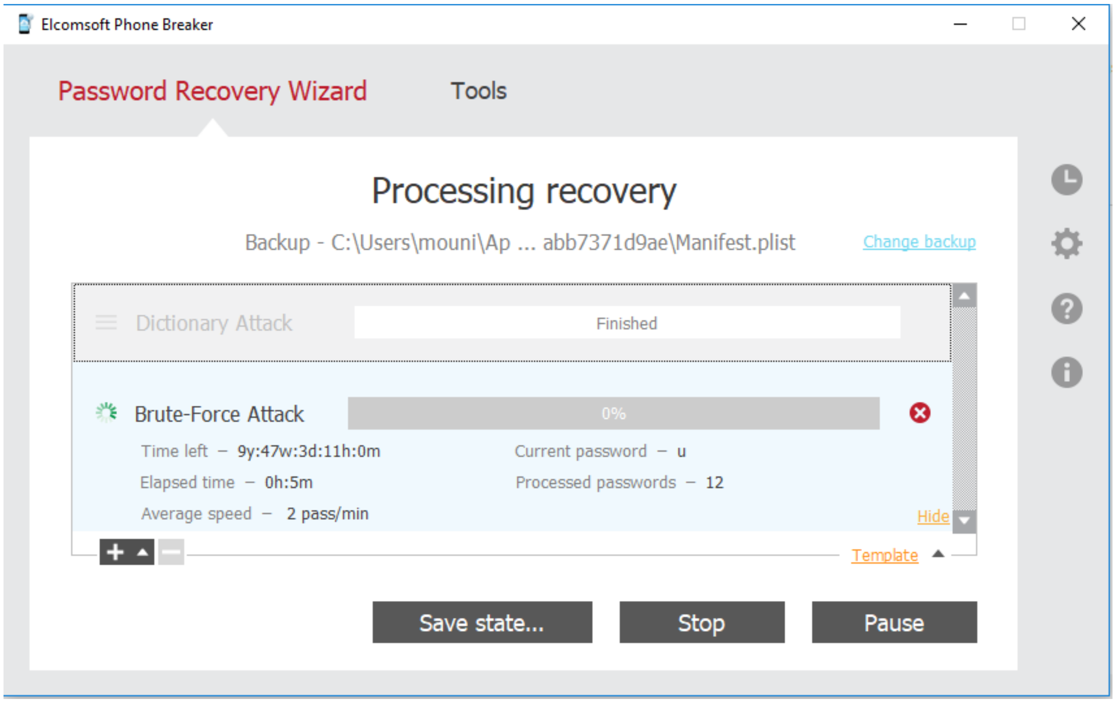
Brute-Force Attack 0%

Time left – 0h:0m Current password – i

Elapsed time – 0h:0m Processed passwords – 0

Average speed – Calculating the speed

Figure 51: Processing brute force attack



Processing recovery

Backup - C:\Users\mouni\Ap ... abb7371d9ae\Manifest.plist Change backup

Dictionary Attack Finished

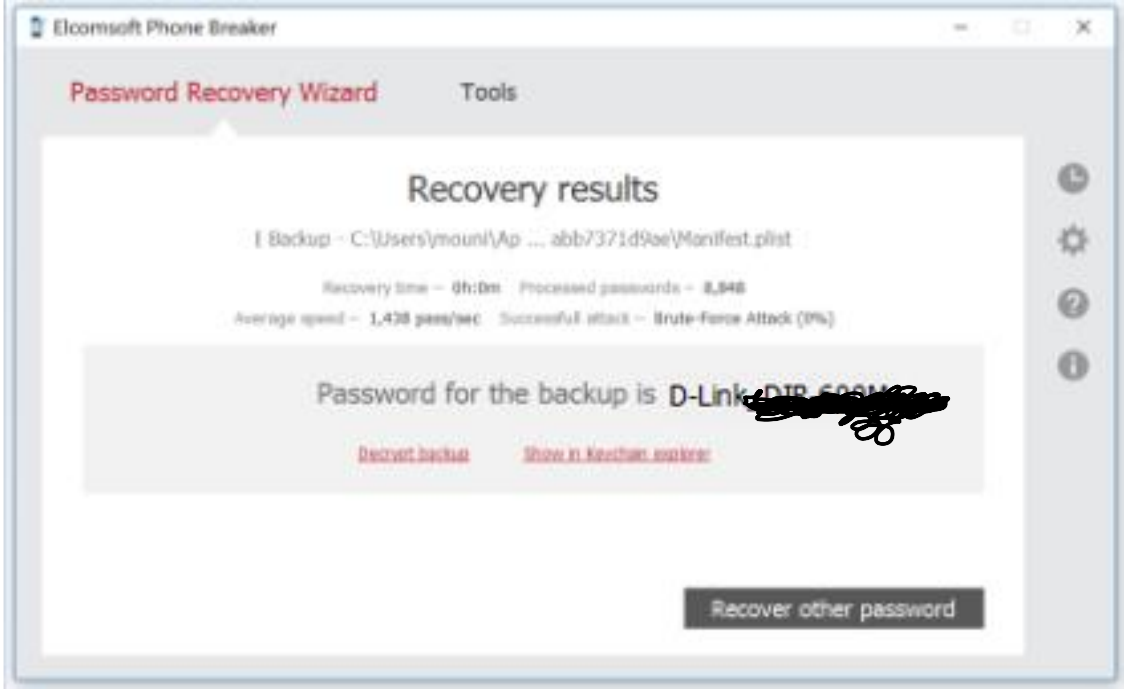
Brute-Force Attack 0%

Time left – 9y:47w:3d:11h:0m
Elapsed time – 0h:5m
Average speed – 2 pass/min
Current password – u
Processed passwords – 12

Hide

Template

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



Recovery results

[Backup - C:\Users\mouni\Ap ... abb7371d9ae\Manifest.plist

Recovery time – 0h:0m Processed passwords – 8,848
Average speed – 1,438 pass/sec Successful attack – Brute-Force Attack (0%)

Password for the backup is D-Link[redacted]

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.

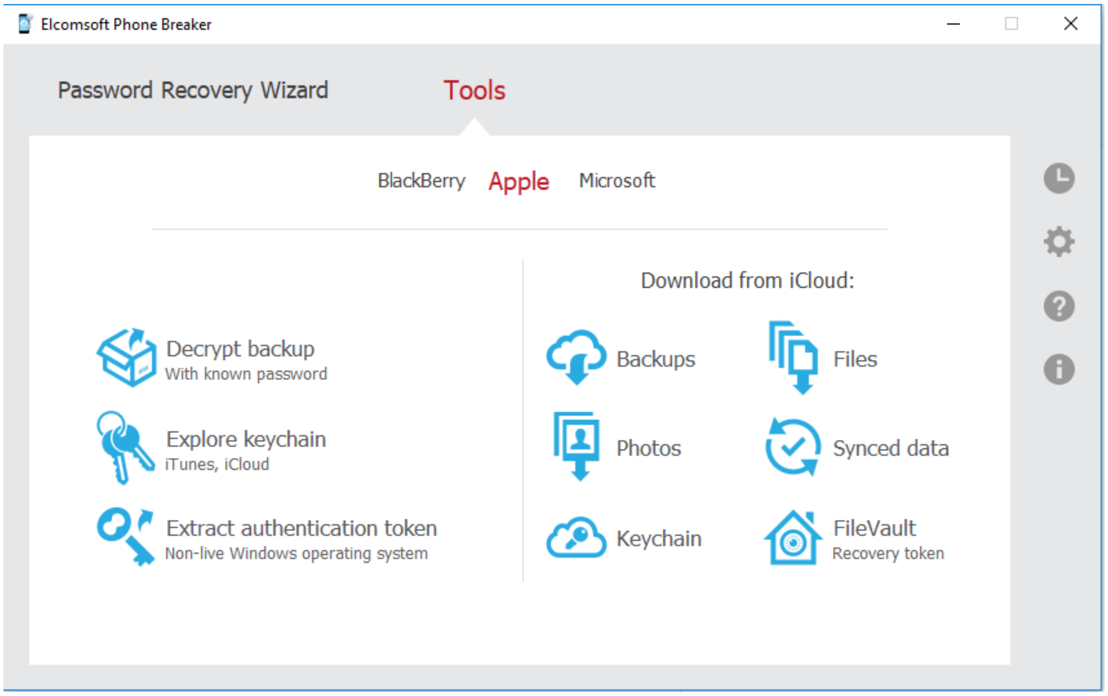
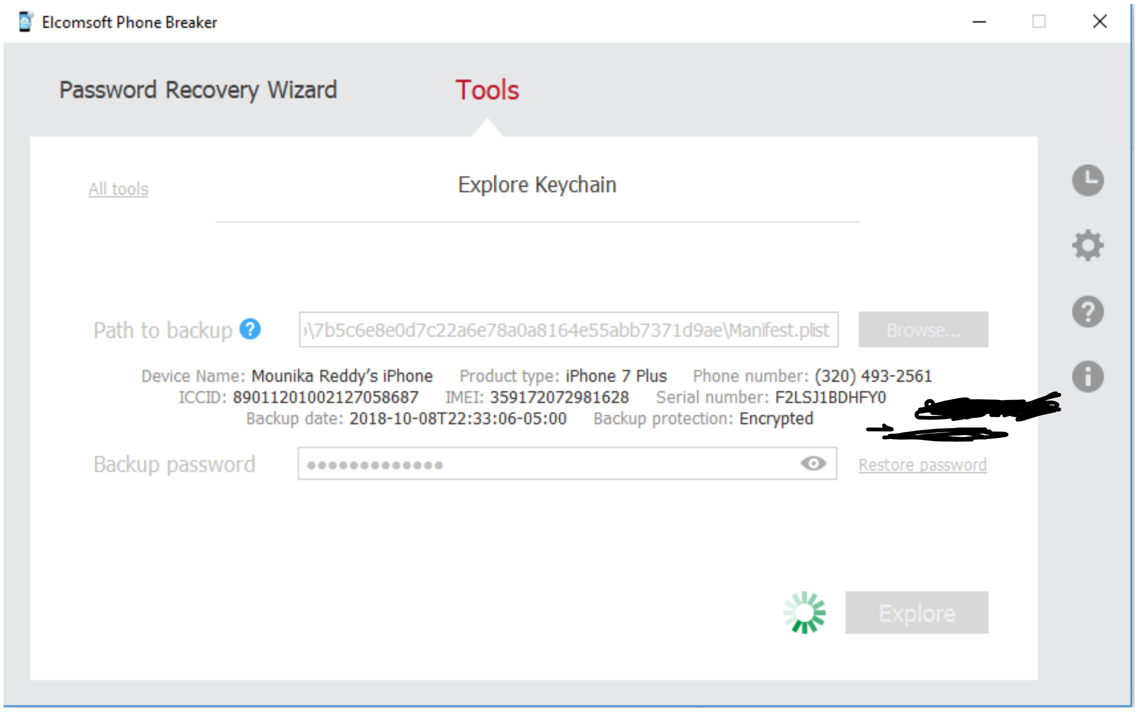


Figure 54: Tools in Elcomsoft phone breaker

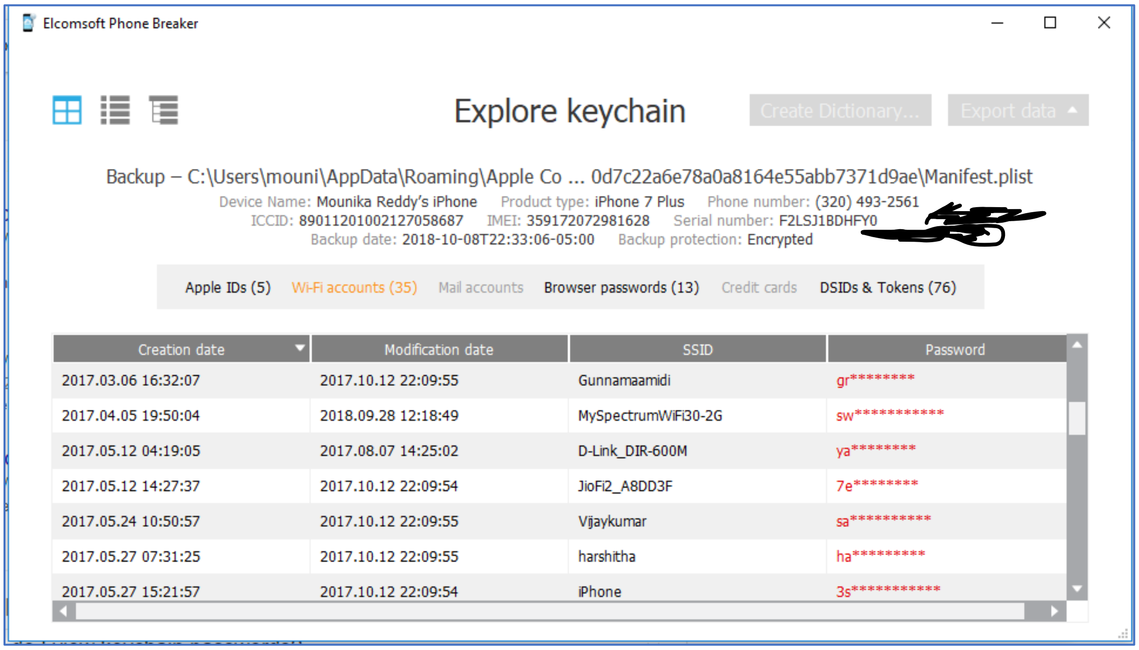


Path to backup: \7b5c6e8e0d7c22a6e78a0a8164e55abb7371d9ae\Manifest.plist

Device Name: Mounika Reddy's iPhone   Product type: iPhone 7 Plus   Phone number: (320) 493-2561
ICCID: 89011201002127058687   IMEI: 359172072981628   Serial number: F2LSJ1BDHFY0 [redacted]
Backup date: 2018-10-08T22:33:06-05:00   Backup protection: Encrypted

Backup password: •••••••••••••

Figure 55: Exploring keychains



Backup – C:\Users\mouni\AppData\Roaming\Apple Co ... 0d7c22a6e78a0a8164e55abb7371d9ae\Manifest.plist

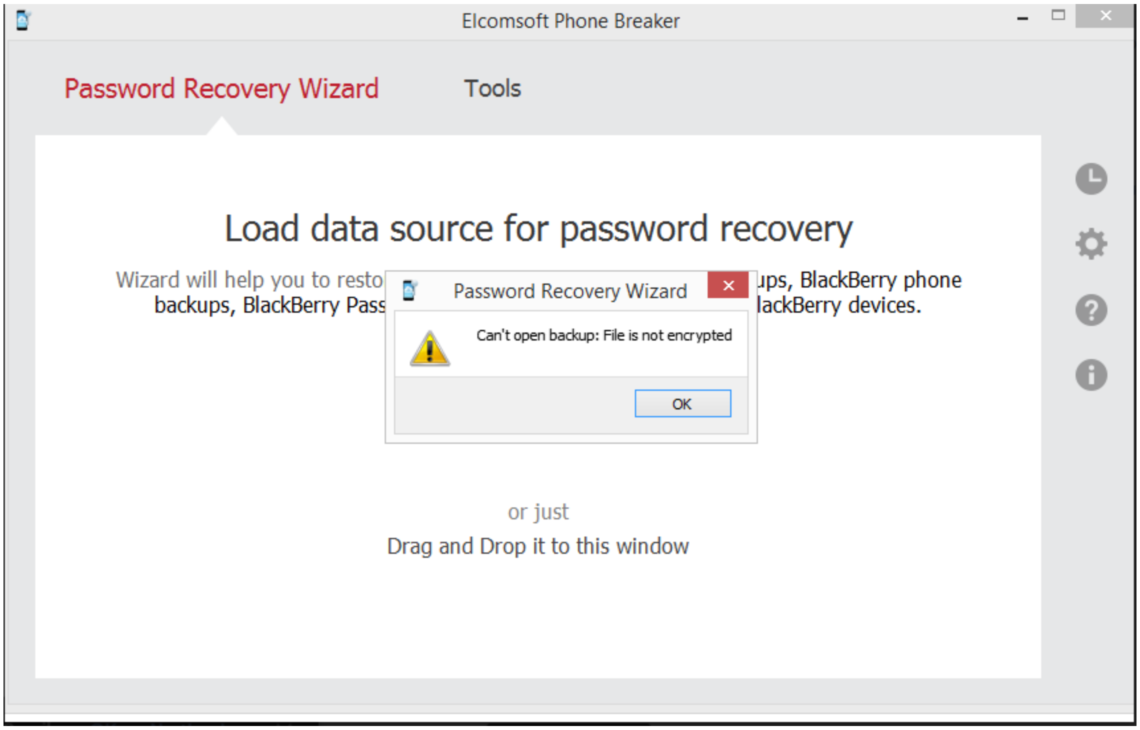
Device Name: Mounika Reddy's iPhone   Product type: iPhone 7 Plus   Phone number: (320) 493-2561
ICCID: 89011201002127058687   IMEI: 359172072981628   Serial number: F2LSJ1BDHFY0 [redacted]
Backup date: 2018-10-08T22:33:06-05:00   Backup protection: Encrypted

Apple IDs (5)   Wi-Fi accounts (35)   Mail accounts   Browser passwords (13)   Credit cards   DSIDs & Tokens (76)

Creation date	Modification date	SSID	Password
2017.03.06 16:32:07	2017.10.12 22:09:55	Gunnamaamidi	gr********
2017.04.05 19:50:04	2018.09.28 12:18:49	MySpectrumWiFi30-2G	sw***********
2017.05.12 04:19:05	2017.08.07 14:25:02	D-Link_DIR-600M	ya********
2017.05.12 14:27:37	2017.10.12 22:09:54	JioFi2_A8DD3F	7e********
2017.05.24 10:50:57	2017.10.12 22:09:55	Vijaykumar	sa**********
2017.05.27 07:31:25	2017.10.12 22:09:55	harshitha	ha*********
2017.05.27 15:21:57	2017.10.12 22:09:54	iPhone	3s***********

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.



Elcomsoft Phone Breaker

Password Recovery Wizard

Tools

Load data source for password recovery

Wizard will help you to resto ups, BlackBerry phone backups, BlackBerry Pass lackBerry devices.

Password Recovery Wizard

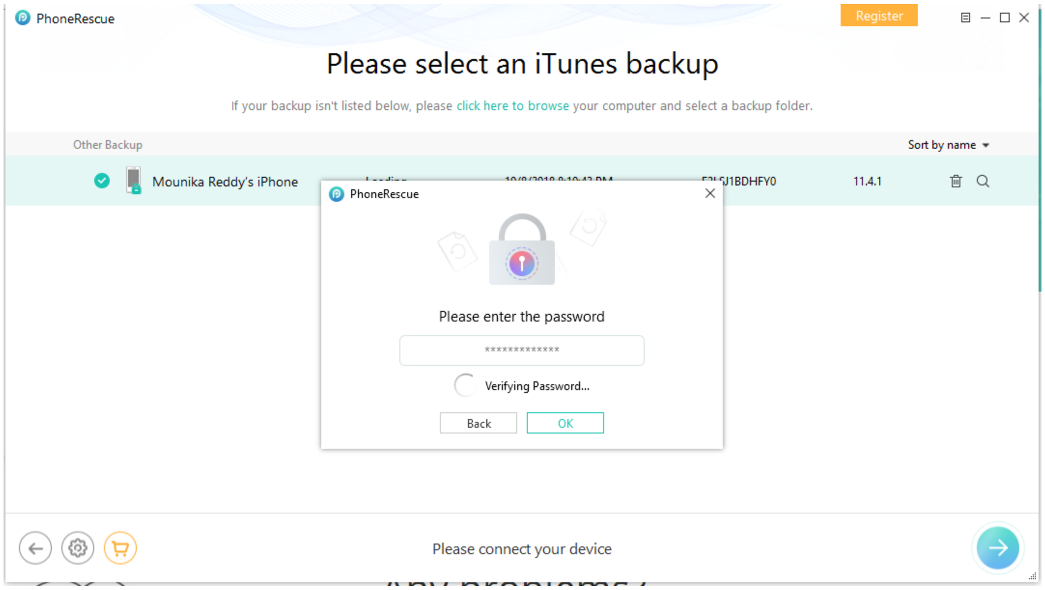
Can't open backup: File is not encrypted

or just

Drag and Drop it to this window

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.



Please select an iTunes backup

If your backup isn't listed below, please click here to browse your computer and select a backup folder.

Please enter the password

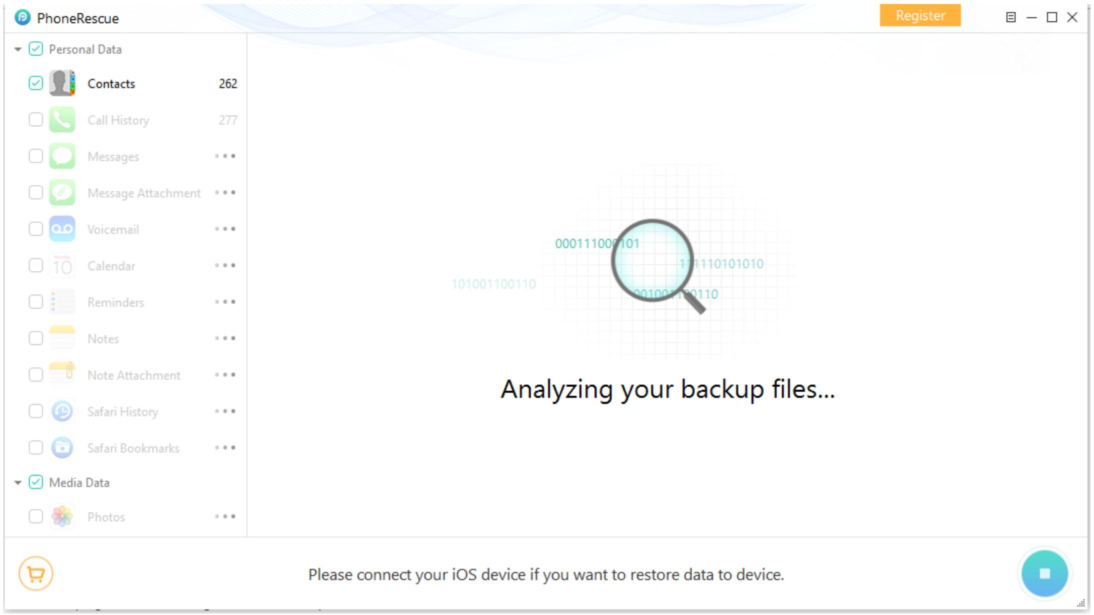
****

Verifying Password...

Please connect your device

Figure 58: Verifying password on PhoneRescue

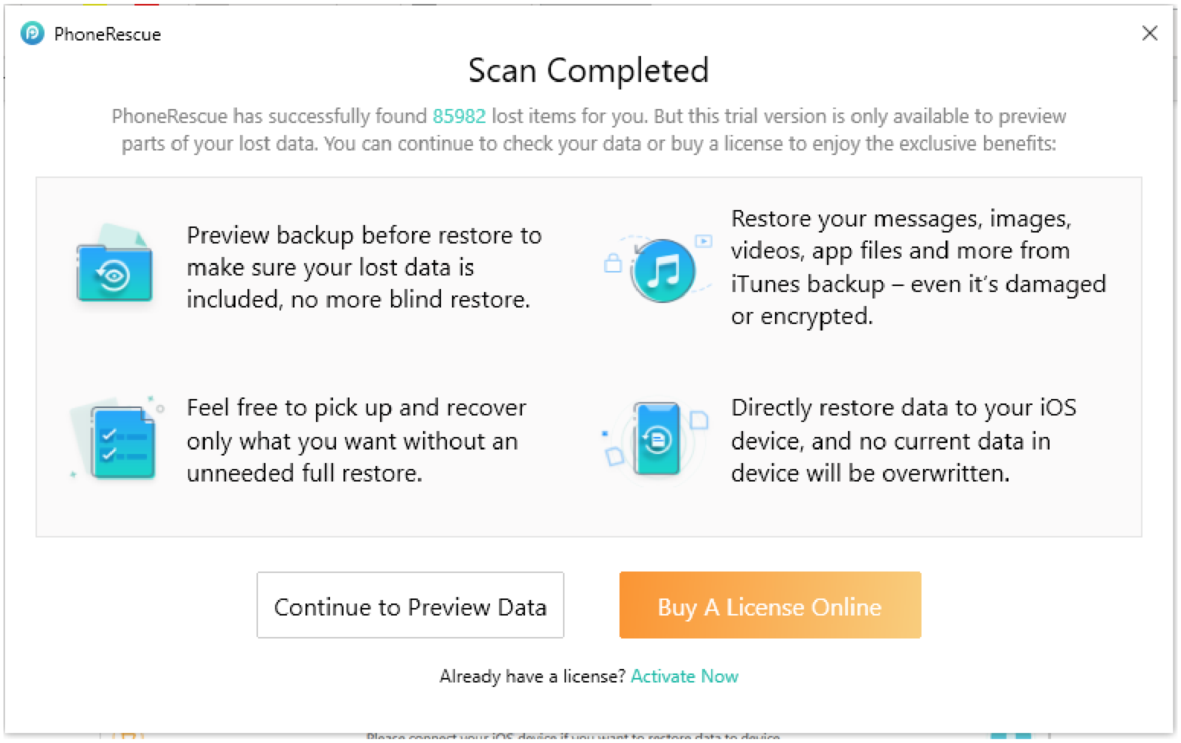
It took 11 hours to acquire all the data after verifying the password. The time depends on the amount of data. In this software, we can choose what data to be acquired. I selected to acquire the entire data hence took me ample amount of time.



Analyzing your backup files...

Please connect your iOS device if you want to restore data to device.

Figure 59: Analyzing files on PhoneRescue



PhoneRescue

Scan Completed

PhoneRescue has successfully found 85982 lost items for you. But this trial version is only available to preview parts of your lost data. You can continue to check your data or buy a license to enjoy the exclusive benefits:

Preview backup before restore to make sure your lost data is included, no more blind restore.

Restore your messages, images, videos, app files and more from iTunes backup – even it's damaged or encrypted.

Feel free to pick up and recover only what you want without an unneeded full restore.

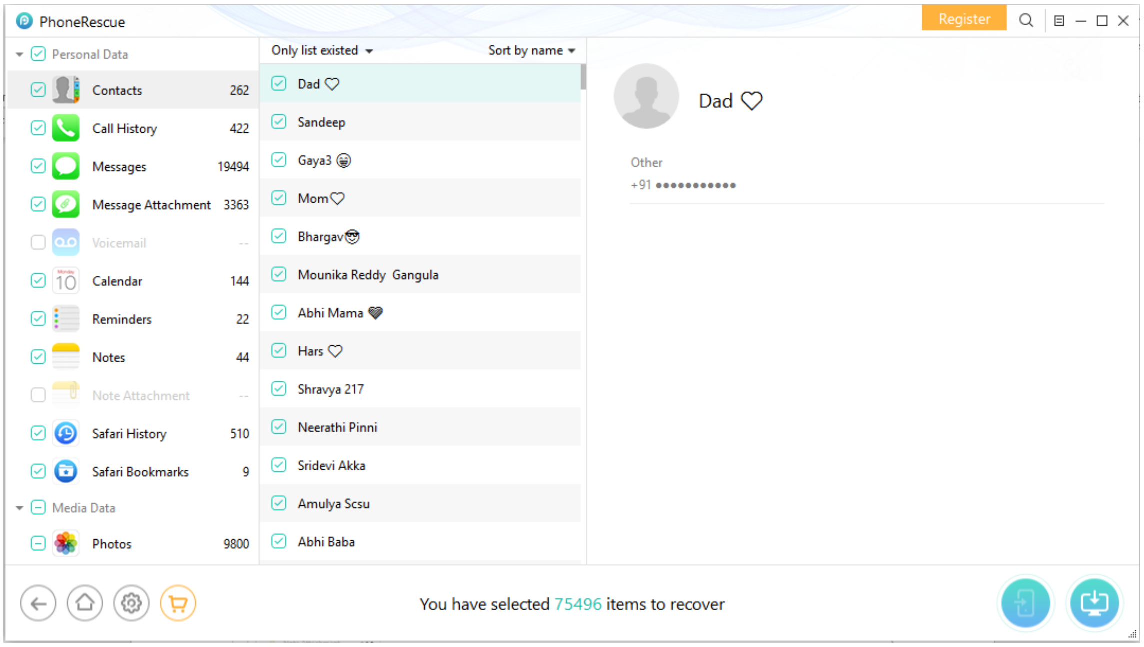
Directly restore data to your iOS device, and no current data in device will be overwritten.

Continue to Preview Data | Buy A License Online

Already have a license? Activate Now

Figure 60: Completion of PhoneRescue scan

I recovered 85982 deleted items from the backup.



PhoneRescue   Register

☑ Personal Data

☑ Contacts	262
☑ Call History	422
☑ Messages	19494
☑ Message Attachment	3363
□ Voicemail	--
☑ Calendar	144
☑ Reminders	22
☑ Notes	44
□ Note Attachment	--
☑ Safari History	510
☑ Safari Bookmarks	9

⊟ Media Data

⊟ Photos	9800

Only list existed ▾   Sort by name ▾

- ☑ Dad ♡
- ☑ Sandeep
- ☑ Gaya3 😁
- ☑ Mom♡
- ☑ Bhargav😎
- ☑ Mounika Reddy Gangula
- ☑ Abhi Mama 🖤
- ☑ Hars ♡
- ☑ Shravya 217
- ☑ Neerathi Pinni
- ☑ Sridevi Akka
- ☑ Amulya Scsu
- ☑ Abhi Baba

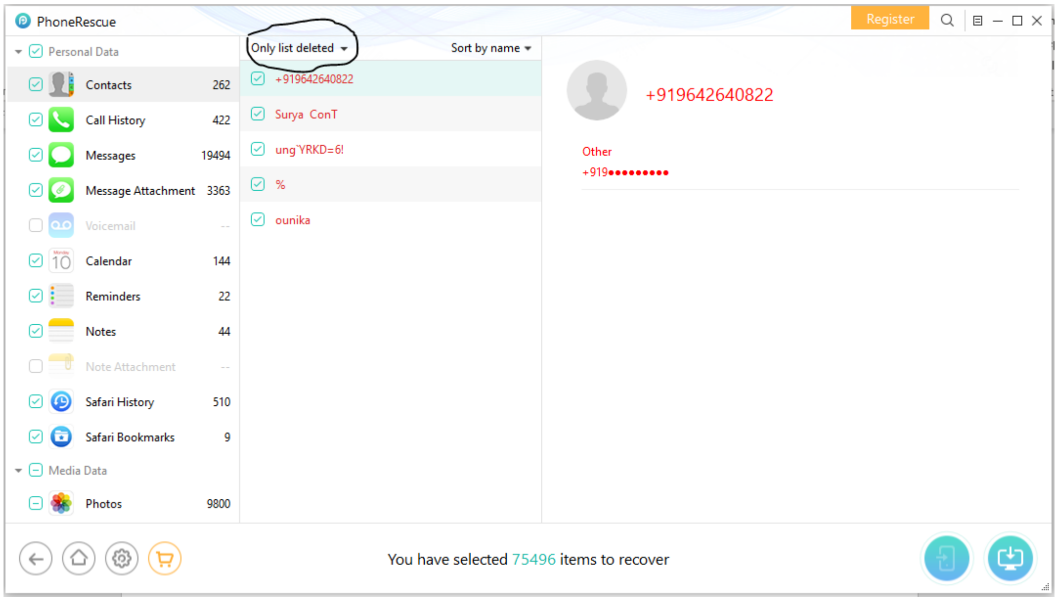
Dad ♡

Other
+91 ●●●●●●●●●●●

You have selected 75496 items to recover

Figure 61: Analyzing recovered data

In the below screenshot you can see the deleted contacts.



☑	Personal Data	
☑	Contacts	262
☑	Call History	422
☑	Messages	19494
☑	Message Attachment	3363
□	Voicemail	--
☑	Calendar	144
☑	Reminders	22
☑	Notes	44
□	Note Attachment	--
☑	Safari History	510
☑	Safari Bookmarks	9
☑	Media Data	
☑	Photos	9800

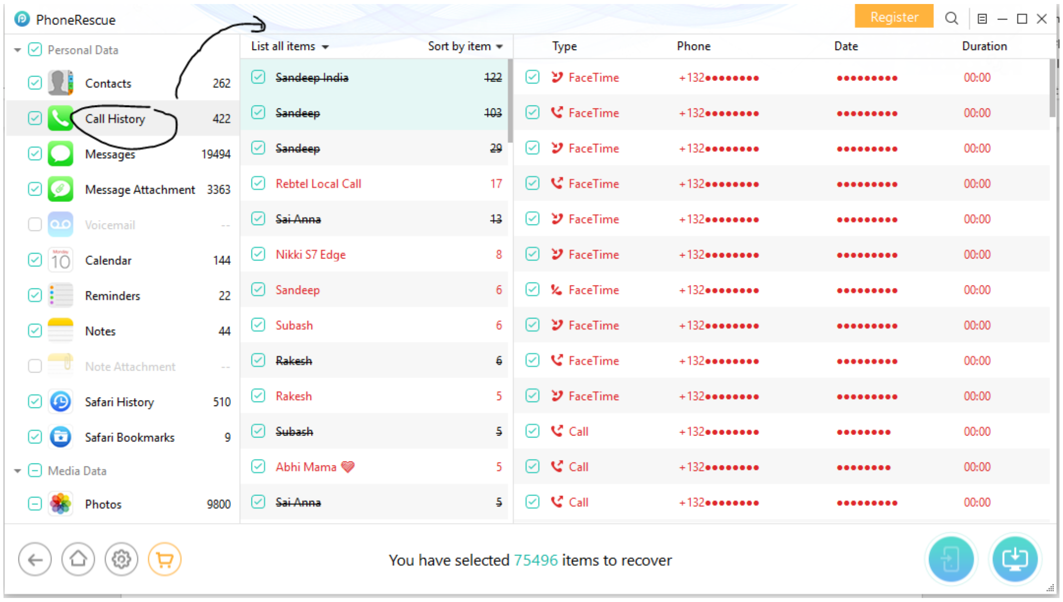
- ☑ +919642640822
- ☑ Surya ConT
- ☑ ung`YRKD=6!
- ☑ %
- ☑ ounika

+919642640822

Other
+919●●●●●●●●●●

You have selected 75496 items to recover

Figure 62: Acquiring deleted contacts



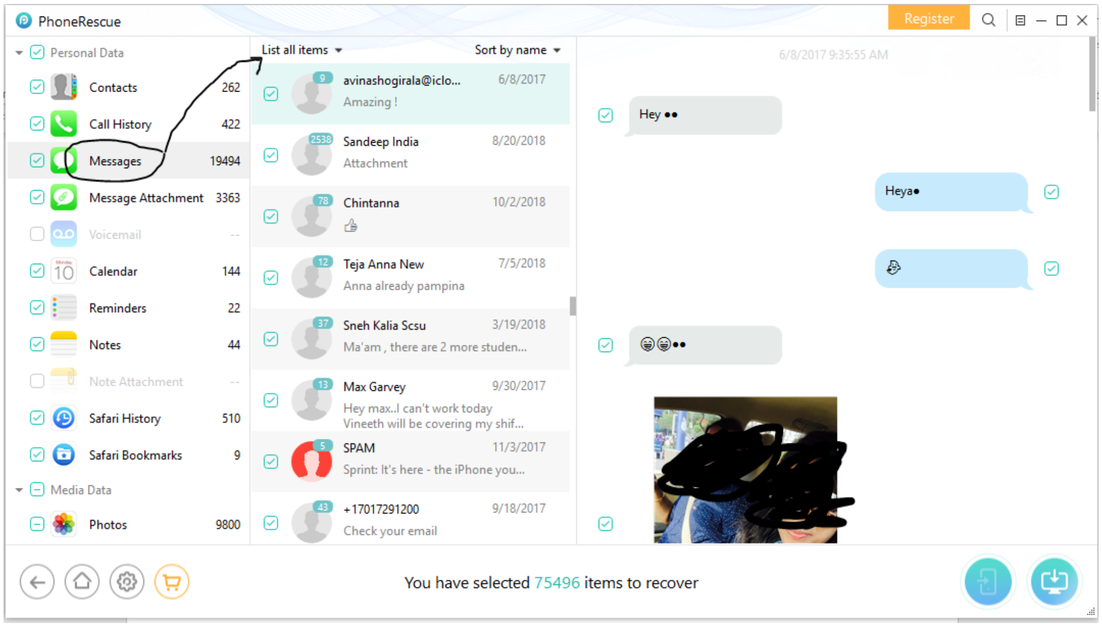
☑	Personal Data	
☑	Contacts	262
☑	Call History	422
☑	Messages	19494
☑	Message Attachment	3363
□	Voicemail	--
☑	Calendar	144
☑	Reminders	22
☑	Notes	44
□	Note Attachment	--
☑	Safari History	510
☑	Safari Bookmarks	9
☑	Media Data	
☑	Photos	9800

☑	~~Sandeep India~~	~~122~~
☑	~~Sandeep~~	~~103~~
☑	~~Sandeep~~	~~29~~
☑	Rebtel Local Call	17
☑	~~Sai Anna~~	~~13~~
☑	Nikki S7 Edge	8
☑	Sandeep	6
☑	Subash	6
☑	~~Rakesh~~	~~6~~
☑	Rakesh	5
☑	~~Subash~~	~~5~~
☑	Abhi Mama ❤	5
☑	~~Sai Anna~~	~~5~~

	Type	Phone	Date	Duration
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	FaceTime	+132●●●●●●●●●	●●●●●●●●●	00:00
☑	Call	+132●●●●●●●●●	●●●●●●●●	00:00
☑	Call	+132●●●●●●●●●	●●●●●●●●	00:00
☑	Call	+132●●●●●●●●●	●●●●●●●●●	00:00

You have selected 75496 items to recover

Figure 63: Acquiring deleted call history



PhoneRescue

Register

Personal Data

Contacts	262
Call History	422
Messages	19494
Message Attachment	3363
Voicemail	--
Calendar	144
Reminders	22
Notes	44
Note Attachment	--
Safari History	510
Safari Bookmarks	9

Media Data

Photos	9800

List all items ▾ Sort by name ▾

9	avinashogirala@iclo...	6/8/2017
	Amazing !	
2538	Sandeep India	8/20/2018
	Attachment	
78	Chintanna	10/2/2018
	👍	
12	Teja Anna New	7/5/2018
	Anna already pampina	
37	Sneh Kalia Scsu	3/19/2018
	Ma'am , there are 2 more studen...	
13	Max Garvey	9/30/2017
	Hey max..I can't work today Vineeth will be covering my shif...	
5	SPAM	11/3/2017
	Sprint: It's here - the iPhone you...	
43	+17017291200	9/18/2017
	Check your email	

6/8/2017 9:35:55 AM

Hey ••

Heya•

👍

😃😃••

[redacted]

You have selected 75496 items to recover

Figure 64: Acquiring deleted messages

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

Afonin, O. (2017, September 7). *New security measures in iOS 11 and their forensic implications.* Retrieved from https://blog.elcomsoft.com: https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/.

Apple, Inc. (n.d.). *iOS security*. Retrieved from https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf.

Apple, Inc. (n.d.). *Keychain Services*. Retrieved from https://developer.apple.com/documentation/security/keychain_services.

Chain of Custody. (n.d.). Retrieved from https://www.google.com/search?client=firefox-b-1-ab&biw=1366&bih=654&tbm=isch&sa=1&ei=3BPIWo28OuqpjwTt4Z_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...1c..64.psy-ab..0.0.0....0.6.

CSI. (n.d.). *Crime Science Investigator*. Retrieved from https://www.crimesceneinvestigatoredu.org/what-is-forensic-science/.

Data Preservation. (n.d.). Retrieved from Center for Computer Forensics: http://www.computer-forensics.net/what-is-data-preservation.html.

Dennon, A. (n.d.). *The digital forensics process.* Pennsylvania Institute of Certified Public Accountants.

EDRM. (n.d.). Retrieved from EDRM: http://www.edrm.net/glossary/chain-of-custody/.

Epifani, M., & Stirparo, P. (2015). *Learning iOS forensics.* Birmingham: PACKT Publishing.

Get iPad/ iPhone out of Recovery Mode. (2012, April 3). Retrieved from https://ipadhelp.com/ipad-help-tips-tricks/get-ipad-iphone-out-of-recovery-mode/.

Hoog, A., & Strzempka, K. (2011). *iPhone and iOS forensics: Investigation, analysis and mobile security for Apple iPhone,iPad and iOS devices.* Elsevier.

Hsamandoudy. (2017, September 27). *How to use iPhone analyzer to acquire backup data*. Retrieved from infosecaddicts: https://infosecaddicts.com/iphone-analyzer-acquiring-backup-data/.

Hsamanoudy. (2017, September 29). *Logical acquisition on an IOS device*. Retrieved from infosecaddicts: https://infosecaddicts.com/logical-acquisition-ios-device/.

iOS architecture. (n.d.). Retrieved from http://www.wiki.org: http://www.wiki.org/iOS-architecture.

iPhone. (n.d.). Retrieved from https://en.wikipedia.org: https://en.wikipedia.org/wiki/IPhone.

iPhone 4S. (n.d.). Retrieved from https://www.google.com/search?q=passcode+in+iPhone+4s&client=firefox-b-1-ab&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiZpqmqvLPaAhUCbKwKHXn-Ck0Q_AUICygC&biw=1366&bih=654#imgrc=pJCLEYci5mhPyM:.

iPhone Backup Extractor. (n.d.). Retrieved from iPhone Backup Extractor: https://www.iphonebackupextractor.com/.

iPhone Explorer. (n.d.). Retrieved from https://macroplant.com: https://macroplant.com/iexplorer.

Keychain Services Programming Guide. (n.d.). Retrieved from Apple Developer: https://developer.apple.com/library/content/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html.

Layered architecture. (n.d.). Retrieved from https://codeingwithios.blogspot.com: https://codeingwithios.blogspot.com/2017/09/ios-layered-architecture.html.

Leong, R. S. (2006). FORZA- digital forensics investigation framework that incorporate legal issues. *The Digital Forensic Research Conference.* Lafayette: Elsevier.

Longenecker, D. (2017, September 19). *Incremental wins: iOS11 stregthens idea of trust.* Retrieved from https://www.securityforrealpeople.com: https://www.securityforrealpeople.com/2017/09/incremental-wins-ios11-strengthens-idea.html.

Lorianne Actus Branches. (n.d.). Retrieved from Lorianne Actus branchees: https://www.lorianne.fr/mode-dfu-iphone-5.html

Mobile Device Forensics. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Mobile_device_forensics.

NIJ. (2016, April 14). *National Institute of Justice* . Retrieved from https://www.nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx.

Passcode on iPhone 7plus. (n.d.). Retrieved from https://www.macrumors.com/how-to/create-a-more-secure-passcode-on-ios-devices/.

Prather, S. (2014). *Minnesota detectives crack the case with digital forensics.* Minnesota: Star Tribune.

Property List Programming Guide. (n.d.). Retrieved from Apple Developer: https://developer.apple.com/library/content/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html.

Recover mode image. (n.d.). Retrieved from Google: https://www.google.com/search?client=firefox-b-1-ab&tbm=isch&q=normal+mode+iphone&chips=

q:normal+mode+iphone,online_chips:recovery+mode&sa=X&ved=0ahUKEwjxw8jev67aAhVWyYMKHeWfCVEQ4lYILigG&biw=1366&bih=654&dpr=1#imgrc=4JZ2gXmhiVNn5M:.

Stephens, B. (n.d.). *Inter works*. Retrieved from https://www.interworks.com/blog/bstephens/2016/02/05/what-digital-forensics.

TBI Infotech. (2015, September 15). Local iOS Data Storage Guidelines for iOS Applications. *Local iOS Data Storage Guidelines for iOS Applications*.

Velu, V. K. (n.d.). *Apple's iOS security model*. Retrieved from https://www.safaribooksonline.com/library/view/mobile-application-penetration/9781785883378/ch02s07.html.

wikipedia. (n.d.). *Acquisition*. Retrieved from Introduction to Digital forensics: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Acquisition.

Wikipedia. (n.d.). *Forensic Science*. Retrieved from https://en.wikipedia.org/wiki/Forensic_science.

Zdziarski, J. (2012, May 12). iOS Forensic Investigative Methods.

Zdziarski, J. (2013, June 12). *Waterboard*. Retrieved from iClarified: (http://www.iclarified.com/31060/jonathan-zdziarski-releases-waterboard-an-open-source-forensic-acquisition-tool-for-ios-devices.