

3-2019

Comparison of Forensic Analysis Results Obtained by Various Types of Acquisitions

Sandeep Chinthapatla
schinthapatla@stcloudstate.edu

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

Recommended Citation

Chinthapatla, Sandeep, "Comparison of Forensic Analysis Results Obtained by Various Types of Acquisitions" (2019). *Culminating Projects in Information Assurance*. 78.
https://repository.stcloudstate.edu/msia_etds/78

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 rswexelbaum@stcloudstate.edu.

Comparison of Forensic Analysis Results Obtained by Various Types of Acquisitions

by

Sandeep Chinthapatla

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

October, 2019

Starred Paper Committee:
Mark Schmidt, Chairperson
Lynn Collen
Sneh Kalia

Abstract

Smartphones have become an essential commodity for people all around the world. Literally, almost every person in the world is migrating towards smartphones. It has become a trend because it has almost the same computing power as a computer and the major advantage is that it is portable. All the tasks a computer can do can be done by a smartphone and that is what people like about it.

The most popular smartphone in the world is the “Apple iPhone”. Because of its features and specifications many people in the world use it for various purposes. The iPhone is used by various groups of individuals such as students, faculty, business man, factory workers etc. Because of its large group of users, there might be chances that it can be used for false purposes too. So, there has been a rise in the new scope of the subject known as “iPhone forensics”. This involves analysis of the user’s data from backup such as retrieving messages, photos, keystrokes, notes, browser’s cache, etc.

There have been several methods which used for retrieving the user’s data. All these applications were developed by several organizations worldwide. They can be either free versions which are open source or available to buy.

This paper briefly discusses all the aspects starting from what an iPhone is to how forensics can be done on an iPhone. It mainly deals with the methods of how data is retrieved using different forensic tools and how the retrieved data is analyzed. After performing various analysis, we see that the logical acquisition is much better than other approaches as it yields better results and we see it from our experiments performed.

Table of Contents

	Page
List of Table	5
List of Figures	6
Chapter	
I. Introduction	11
Problem Statement	14
Nature and Significance of the Problem	15
Objective of the Project	15
Study Questions	16
Limitations of the Project	16
Definition of Terms	16
Summary	18
II. Background and Review of Literature	19
Introduction	19
Background Related to the Problem	19
Literature Related to Problem	19
Literature Related to Methodology	28
Summary	39
III. Methodology	41
Introduction	41
Design of the Study	41
Data Collection	41

Chapter	Page
Budget	42
IV. Data Presentation and Analysis	43
Introduction	43
Data Presentation	43
Data Analysis	55
Summary	87
V. Results, Conclusion, and Recommendations	88
Introduction	88
Results	88
Conclusion	89
Future Work	90
References	91

List of Table

Table	Page
1. CF Types and the Corresponding XML Tags of Plist	26

List of Figures

Figure	Page
1. iPhone versions	12
2. iOS security	14
3. Digital forensic process	21
4. iPhone architecture	23
5. HFS plus volume allocation	25
6. Chain of custody	30
7. iExplorer	33
8. Elcomsoft tool	34
9. iFunBox	35
10. iTunes Microsoft store	43
11. iTunes homepage	44
12. iExplorer	44
13. iExplorer setup	45
14. Macroplant security warning	45
15. iExplorer preview	46
16. Elcomsoft phone breaker	46
17. Elcomsoft phone breaker setup	47
18. EPB setup	47
19. EPB preview	48
20. iFunBox	48
21. iFunBox setup	49

Figure	Page
22. iFunBox setup	49
23. iFunBox agreement	50
24. iFunBox setup progress	50
25. iFunBox preview	51
26. FTK imager download page	51
27. FTK form	52
28. FTK download link	52
29. FTK exe file	53
30. FTK installation wizard	53
31. FTK imager preview	54
32. Backup folder preview	54
33. In depth backup folder preview	55
34. Backup folder file interests	55
35. Backup folder	56
36. Backup folder files of interest	56
37. XML view of Manifest.plist file	57
38. XML view key info	57
39. Manifest.plist file list view	58
40. Manifest.plist file list view key info	59
41. List view key info	59
42. Application list	60
43. Deleted application list	61

Figure	Page
44. Status.plist view	61
45. Snapshot folder	62
46. Insight of snapshot folder	62
47. Snaps view	63
48. iPhone explorer view	64
49. iPhone explorer messages view	65
50. iPhone explorer call history view	65
51. iPhone explorer photos view	66
52. iPhone explorer contacts view	66
53. iPhone explorer history view	67
54. iPhone explorer notes view	67
55. iPhone explorer applications view	68
56. Elcomsoft phone breaker preview	68
57. Elcomsoft phone breaker tools	69
58. Elcomsoft phone breaker passwords	69
59. Elcomsoft phone breaker password recovery wizard	70
60. iFunbox preview	71
61. iFunbox photos	71
62. iFunbox applications view	72
63. iFunbox toolbox	73
64. iFunbox toolbox view	73
65. iFunbox toolbox insight view	74

Figure	Page
66. Elcomsoft iOS forensic toolkit preview	74
67. iOS version	75
68. iPhone connected to laptop	75
69. iPhone DFU mode	76
70. Kit preview	77
71. Partition selection	77
72. Image completion	77
73. FTK imager preview	78
74. Evidence type selection	78
75. Image files	79
76. Hex viewer	79
77. Hex code inspection	80
78. iOS version inspection	81
79. Pangu website	81
80. Electralyzed jailbreak wizard	82
81. Jailbreak wizard	82
82. Jailbreak options	83
83. Jailbreak description	83
84. Installation compatibility	84
85. Installation step for pangu	84
86. Installation popup	85
87. Profile view	85

Figure	Page
88. Launchpad view	86
89. App view	86

Chapter I: Introduction

iPhone is a line of smartphones released in the year 2007 which are designed and marketed by Apple Inc. They run on Apple iOS mobile operating system (Wikipedia, n.d.). It is a revolutionary product which revolutionized the way people look at a smartphone. It created a huge impact on the people of the 21st century.

The main reason for the popularity of iPhone is the wide range of applications it provides, and the support provided by Apple Inc. A smartphone can generally be compared to a small computer and iPhone is no less than that. Due to a wide range of applications, there will be storage of data in different types. And this storage is volatile, and it is changed constantly unless the device is turned off (Engman, 2013).

As devices become more popular people become more interested in how and what data is stored on the smartphones. This resulted in advancement in the field of Forensics for mobile devices and primarily iPhone forensics. But as new models are released every year several new problems arise as the software's which were used on previous devices may not function properly on the newer versions of operating systems and devices.

Every year a new iPhone is released in the market with a new operating system. This is a major concern as both hardware and software are changed organizations need to come up with new tools. This makes it difficult as they need to invest a lot of time and effort in developing new tools which support the new enhanced operating system.



Figure 1. iPhone versions (“The Mercury news,” n.d.).

iPhone file system. “A file system handles the persistent storage of data files, apps, and the files associated with the operating system itself. Therefore, the file system is one of the fundamental resources used by all processes” (Apple, n.d.).

HFS file system. In early 90’s Apple introduced a new type of file system called the hierarchical file system (HFS). It was designed to be a new dynamic file system and is formatted with a 512-byte block scheme. This file system has two types of blocks known as logical blocks and allocation blocks. The logical blocks are numbered from the first block to the last block available on the volume and it will remain static. Allocated blocks can be tied together as groups to be utilized more efficiently (Proffit, 2012).

APFS file system. This file system was introduced by Apple in the year of 2017. It was designed for flash-based devices. It was mainly introduced because of its higher read/write

speeds which are comparable in number with the solid-state drives. It also has the efficient way of storing data which makes the data utilization more efficient (Tech republic, n.d.).

SQLite Database. This is the most popular database used for modern mobile devices to store data. This is completely relational and contained in a small C programming library. It has been also implemented by Apple development community and all the native applications such as Messages, music, calendar etc are stored in this database structure and organized efficiently (Proffit, 2012).

iOS security. Apple's main motive is to provide security as its core element. They went out to create the best mobile platform and completely redesigned the security architecture. They went on to incorporate complex methodologies so that they can keep the user data secure and in an encrypted fashion (Apple business). The several ways they categorized the security approach is as follows:

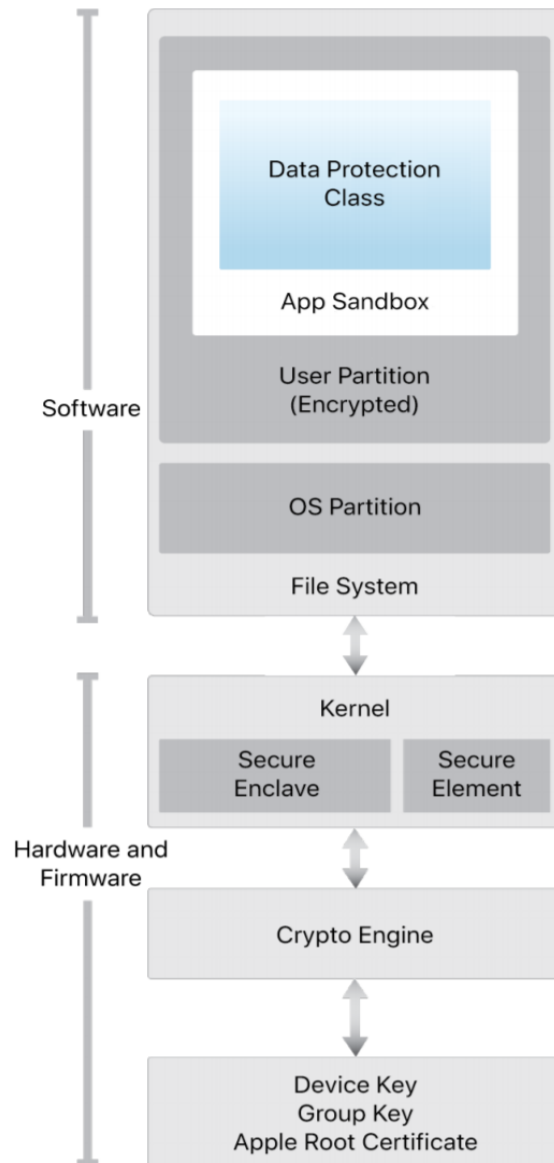


Figure 2. iOS security (Apple business).

Problem Statement

The main problem is as new iPhone's come into the market new hardware and software changes take place which results in developing new forensic tools for newer devices. Apart from this, the other aspect in consideration is the security. Apple is making devices more secure day

by day so that third party software or tools cannot penetrate deep into the system. This approach came into place because of the malicious applications that are becoming viral in the market.

So, we come with several approaches which we would discuss in the paper are as follows:

1. How do we perform a forensic analysis on an iPhone?
2. Which tools to use to perform the forensic analysis?
3. What is the information that we need to examine?
4. How many various methods can be applied to perform the analysis?
5. How many types of approaches yield the same result?
6. How effective will the approaches be?

Nature and Significance of the Problem

The techniques and procedures that are followed by forensic investigators to solve the iPhone cases are no longer possible because of the major changes in software and security methods provided.

As per the statistics from Wikipedia, the recent Q1 sales of 2018 is 77.3 million. The average sales as per my estimation for each quarter is almost 25million (Wikipedia). By this we can clearly understand how many devices Apple produces and how many are sold. As the user base is so large the chances of committing crimes through these devices is also high.

From the above figure, we see a major rise in the usage of smartphones. The transformation of how people used basic phones in daily life has taken a major leap towards using smartphones.

Objective of the Project

The main objective of the study is to find out how forensic investigators are facing troubles while trying to use different methods for performing forensic analysis on iPhone. In this

approach, I would also be considering the different methods of backup and tools used to retrieve the key information from an iPhone and compare the results from each approach.

Study Questions

The study questions may constitute like: what are the difficulties caused by the forensic investigators while using tools to retrieve information? Would the backup be sufficient to retrieve information? Would the deleted files be recoverable by the different methods? Would the results match when different approaches are used?

Limitations of the Project

The main limitation of this project is would the tools and methods that we use for retrieval of data would be successful or not. This concern is mainly because of the security provided on iPhones. To be precise it is something dealing with the data which is stored in an encrypted way.

Definition of Terms

Smartphone: “A smartphone is a handheld personal computer with a mobile operating system and an integrated mobile broadband cellular network connection for voice, SMS, and Internet data communication”. “Today, smartphones largely fulfill their users' needs for a telephone, digital camera and video camera, GPS navigation, a media player, clock, news, calculator, web browser, handheld video game player, flashlight, compass, an address book, note-taking, digital messaging, an event calendar, etc.” (Wikipedia, n.d.).

iPhone: “iPhone is a line of smartphones designed and marketed by Apple Inc. They run Apple's iOS mobile operating system. The first-generation iPhone was released on June 29, 2007, and there have been multiple new hardware iterations with new iOS releases since”. “The original iPhone was described as "revolutionary" and a "game-changer" for the mobile phone

industry. Newer iterations have also garnered praise, and the iPhone's success has been credited with helping to make Apple one of the world's most valuable publicly traded companies”

(Wikipedia, n.d.).

iOS: iOS was formerly known as iPhone OS is an operating system provided by Apple exclusively for its devices. It has been unveiled during the launch of the first-generation iPhone and has been releasing with upgrades every year since then. The current version of iOS is iOS 11

(Wikipedia, n.d.).

All the versions of iPhone can be given as follows:

1. iPhone OS 1
2. iPhone OS 2
3. iPhone OS 3
4. iOS 4
5. iOS 5
6. iOS 6
7. iOS 7
8. iOS 8
9. iOS 9
10. iOS 10
11. iOS 11 (till date)

Digital forensics. Digital forensics can also be termed as “digital forensic science”. It can be defined as the branch of forensic science which deals with recovery and investigation of material devices which are in often relation to computer crime. The term Digital forensics was

first used as a synonym for computer forensics but later as new devices with digital storage came into existence it expanded to these devices too (Digital forensics, n.d.).

Summary

In this chapter, we have learned what a smartphone is and how the market for smartphones is rapidly rising. We also discussed what are the main problems faced by forensic experts and security provided by Apple for these devices. A brief description of the definition of terms was also discussed along with a brief intro to study questions such as how iPhone forensics can be done and how efficient they would be in the retrieval of data.

Chapter II: Background and Review of Literature

Introduction

Firstly, there were days as whenever a digital crime occurs people always used to look at an angle that it was committed using a computer. But now the days have changed almost all the devices with digital storage can be used to commit crimes. This has become a major turnover and the main challenges were regarding the retrieval of data and tools used.

The main key aspect that we need to look forward is how we can retrieve data from an iPhone. The challenges that might occur during this process would be the format of how the data is stored in an iPhone in an encrypted way. Will the tools and methods be efficient enough to retrieve the data and produce the same output?

Background Related to the Problem

The main problem faced today by the forensic investigators is how to retrieve the data from the iPhone. There are several methods available in the market, but they need to analyze which method would be best suitable. But before we use these methods the underlying problem is with the security and the encrypted storage of data in an iPhone.

They need to bypass this measure so that they could analyze the data present on the iPhone and perform forensic analysis to retrieve the data. This is one of the main problems to keep in mind when performing a forensic analysis.

Literature Related to Problem

Forensics. Forensics can be defined as “relating to or dealing with the application of scientific knowledge to legal problems especially in regard to criminal evidence” (Merriam Webster, n.d.).

To be precise we can define forensics as gathering all the useful information which could be presented as evidence in the court for solving a case. This information would be collected by various methods and strategies and may be done in all fields.

Digital forensics. Digital forensics can be defined as “The science of identifying, preserving, recovering, analyzing and presenting facts about digital evidence found on computers or digital storage media devices” (Interworks, 2016).

Digital forensics cannot be just limited to the court of law. There may be chances that a company or a firm may be handling some sort of internal affair like violation of certain terms and may not fall under the crime category. So, by this, we understand how it is used to find evidence and use it to present it either in front of the court or solve matters within the organization (Interworks, 2016).

Digital forensic process. The process of digital forensics can be simply given as a five-step process as follows:

1. **Identify:** In this step, we need to identify where the data is stored. This is a key step as this identification would lead to the progress in the investigation.
2. **Preserve:** The next step will be integrity. Because, without integrity, a piece of evidence loses its value or “admissibility” in the court of law. That’s why it’s so important to ensure that the artifacts are unaltered and preserved in their original state.
3. **Recover:** This will be the next step in the process. As the name suggests it deals with recovering the files which are deleted from the main storage. By this, we could extract several key information which might be helpful in presenting as evidence in the court.

4. Analyze: This step deals with analyzing all the information which we recovered from the storage. The analyzation is done in various methods regarding on how we want the information to be retrieved.
5. Present: This is the final step of the process. Here we present all the findings and document in a proper way so that we have a clear idea of what we have done in the previous steps to perform forensic analysis and also to present in the court as evidence in a proper format (Interworks, 2016).

The process can be explained in the below Figure as follows:

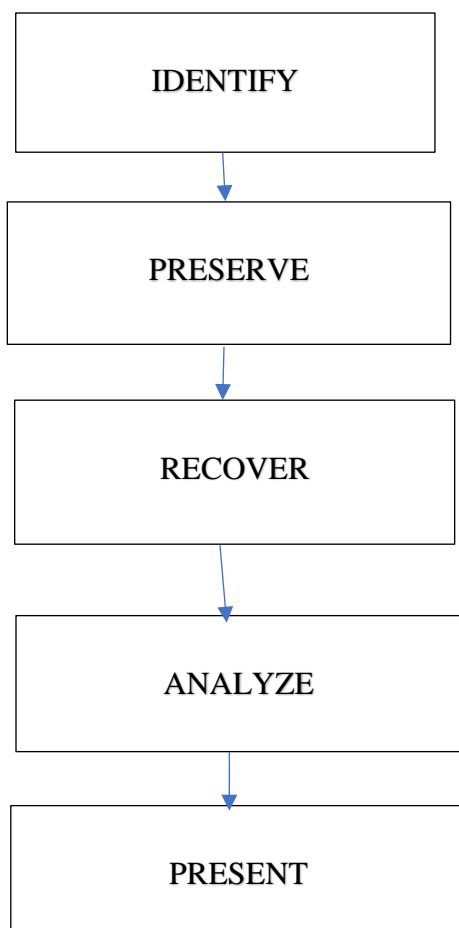


Figure 3. Digital forensic process.

Security. The system security is defined so that both the hardware and software are secure across all components of every iOS device. This makes the forensic analysis more difficult as the device is secured in all ways. The way Apple categorizes the security approach is as follows:

1. System security
2. Encryption
3. Data protection
4. App security
5. Network security
6. Internet services
7. Apple pay
8. Device
9. Privacy controls

Security enhancements over the years. Earlier during the initial stages of smartphones, there was not much concern about security. But as years passed by digital attacks started to tremendously increase. This made Apple Inc. make devices more secure. Over the years the iPhone has taken many transformations both physically and in the aspect of security.

UID and GID were introduced so that they can identify the device and the model. Apart from that passcode was introduced which secured the device. Later Touch Id was introduced which took users finger print and authenticated users with identified finger prints. During the launch of iPhone X in the year of 2017 Apple Inc. introduced FaceId. This feature stores the user's face as a pattern and recognizes and unlocks the phone if the user puts themselves in front of the front camera.

The architecture of iOS devices. The iPhone architecture is a sophisticated architecture. It is mainly designed in regard to the general architecture so that whatever operation is done by the user the system responds accordingly and gives the desired output.

The input is given by the user through the hardware and this request goes through the firmware then the processor and a signal are produced. This signal in turn produces a system call and gives the output back into the hardware so that the user gets the desired output.

iPhone Architecture



Figure 4. iPhone architecture (Mallepally).

iPhone RAM. The RAM that is present in an iPhone is very different from what other smartphones use. The type RAM what an iPhone uses is the Flash RAM. The speed of the device is an increase because of using this RAM as it is fast and performs tasks efficiently (Mallepally).

The file system of iOS devices.

iOS storage with HFS + File system. Until 2017 the file system that was used by Apple for its devices was the HFS file system. This was developed by Apple and can be expanded as “Hierarchical file system” which is a dynamic file system. It is formatted with 512 bytes block

scheme to meet new several objectives by Apple. As discussed earlier it has two types of blocks known as Logical and allocation blocks.

“The structures of file system include a volume header, startup file, allocation file, attributes files, extents overflow file and a catalog file” (Proffit, 2012).

HFS + Volume header. In this the sectors 0 and 1 of, the volume is boot blocks. This stores a wide variety of data such as the size of allocation blocks, a timestamp regarding when the volume was created or location of other volumes.

HFS + Allocation value. The main function is to track which allocation blocks are used by the system or are free. It specifies the free block by storing it as data in bitmap specifying it with “clear bit”.

HFS + Extents overflow file. “The extent overflow file tracks all allocation blocks that belong to a file. The information recorded lists all extents used by a file and its’ allocated blocks in the proper order. This information is stored in a balanced tree format” (Proffit, 2012).

HFS + Catalog file. It describes the folder and file hierarchy of a volume which contains metadata about all the files and folders and their respective timestamps. It uses a balanced tree log structure which contains nodes which denote the reference to the files and folders.

Partitions. The iOS device will have two partitions. One is the firmware partition which gets updated only when there is a new firmware update and does not contain much of the data which is useful for forensic analysis. The second partition is the primary focus which contains the user data. This is the main partition that forensic analysis should be done so that they could retrieve all the useful and key data which can be provided as evidence in the court of law.

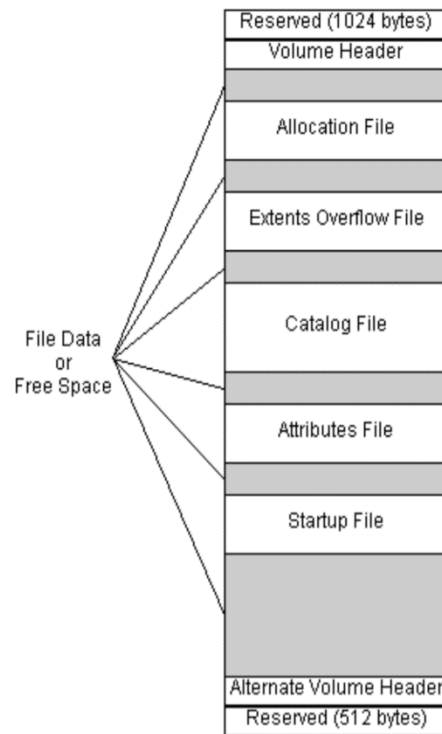


Figure 5. HFS plus volume allocation (Mallepally).

Plists. Plists can be elaborated as “Property lists”. The main functionality of Plists is to organize data into named values and lists of values using several Core Foundation types such as CFString, CFNumber, CFBoolean, CFDate, CFData, CFArray, and CFDictionary. It gives us the means to produce data which is meaningfully structured, storable, transportable and accessible but keeping the data efficient as possible (Apple library, n.d.).

The plists programming interface allows us to convert the hierarchical structured types into two divisions mainly the XML format and a binary format. The representation can be given as follows:

Core foundation types with XML equivalents:

Table 1

CF Types and the Corresponding XML Tags of Plist (Apple library, n.d.)

CF type	XML tag
CFString	<string>
CFNumber	<real> or <integer>
CFDate	<date>
CFBoolean	<true/> or <false/>
CFData	<data>
CFArray	<array>
CFDictionary	<dict>

Failure of data transfer. The main problem that exists will be the failure of data transfer. This may be caused by the encryption of data. This is a new process by which Apple is trying to keep the data secure so that third party applications cannot be accessed by illegal software's and tools.

Encryption. In cryptography, the word encryption can be defined as the process of encoding a message in a way that only authorized users can see the content and unauthorized users cannot see or access the content. This is done in a process such that the plain text is encrypted using an algorithm and the authorized user decrypts it is using a key (Wikipedia, n.d.).

Hardware encryption. Apple has been very keen on the aspect of security right from almost the beginning. From its model of iPhone 3GS it has equipped the device with a dedicated AES coprocessor. This processor stores two keys called the UID and GID. UID is a key which

represents unique key per device. GID is a key which represents unique key per model (Handling iOS encryption in a forensic investigation, 2011).

Software encryption. The files and folders in the device are always encrypted with a unique key. This unique key is generated by the UID, GID and the public key of the application or process. This is stored in a “keybag”. By this, we clearly understand how difficult is to decrypt the files and folders on a system.

Firmware. A firmware is a file which is required for the the efficient functioning of the operating system. With every new Operating System, there would be changes and upgrades to the firmware too. This is also the main problem when performing forensic analysis on iOS devices.

Legal issues.

The Fourth Amendment of the U.S constitution: Generally, officers need to have a warrant in order to search and seize the materials. But as there was a vast change in the smartphone market making laws became much difficult. Now as per the law the officers can perform a search a phone without a warrant and if the search exploits any personal information or privacy of the individual then the court must exclude any evidence obtained as a result of a tainted search (Morrissey, 2011).

This generally happens because it is not easy to change the laws and update them. What technology is in boom today will not have a guarantee that it would still be in a boom in the coming years. Because of this, we can't rapidly make changes to the constitution and bylaws as per our wish.

Literature Related to Methodology

Chain of custody. “Chain of custody (CoC), in legal contexts, refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence” (Wikipedia, n.d.).

“When evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to prevent tampering or contamination. The idea behind recording the chain of custody is to establish that the alleged evidence is in fact related to the alleged crime, rather than having, for example, been “planted” fraudulently to make someone appear guilty.” It is both a chronological and logical process.

Property Record Number: _____

Anywhere Police Department
EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
 Submitting Officer: (Name/ID#) _____
 Victim: _____
 Suspect: _____
 Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Technical Working Group on Biological Evidence Preservation. *The Biological Evidence Preservation Handbook: Best Practices for Evidence Handlers*. U.S. Department of Commerce, National Institute of Standards and Technology. 2013.

EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM (Continued)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Final Disposal Authority
<p>Authorization for Disposal</p> <p>Item(s) #: _____ on this document pertaining to (suspect): _____ is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)</p> <p><input type="checkbox"/> Return to Owner <input type="checkbox"/> Auction/Destroy/Divert</p> <p>Name & ID# of Authorizing Officer: _____ Signature: _____ Date: _____</p>
<p style="text-align: center;">Witness to Destruction of Evidence</p> <p>Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ ID#: _____ in my presence on (date) _____</p> <p>Name & ID# of Witness to destruction: _____ Signature: _____ Date: _____</p>
<p style="text-align: center;">Release to Lawful Owner</p> <p>Item(s) #: _____ on this document was/were released by Evidence Custodian _____ ID#: _____ to _____</p> <p>Name _____ Address: _____ City: _____ State: _____ Zip Code: _____</p> <p>Telephone Number: (____) _____</p> <p>Under penalty of law, I certify that I am the lawful owner of the above item(s).</p> <p>Signature: _____ Date: _____</p> <p>Copy of Government-issued photo identification is attached. <input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.</p>

Figure 6. Chain of custody (National Institute of Standards and Technology, n.d.).

Acquisition. Acquisition can be defined as a way in which we take control over an entity.

In our case, it is the device which we use to perform forensic analysis that is the “iPhone”.

According to my research, there are mainly four ways for acquiring forensic data from an iOS device. They are:

1. Acquisition via iTunes backup
2. Acquisition via logical methods
3. Acquisition via physical methods
4. Acquisition via jail breaking

We will discuss these four steps briefly as follows:

Acquisition via iTunes backup. As the name suggests in this method the acquisition is done via iTunes backup. The backup is generally retrieved from the workstation which is a Windows or a Mac OS to which the iPhone is usually connected. The iTunes usually does an automated backup in a directory on the system whenever the device is connected. It happens whenever there is a software update, or a sync process is performed.

In a Windows operating system the backup is usually stored in this directory:

`%systempartition%\Users\%username%\AppData\Roaming\Apple Computer\MobileSync\Backup\`

Similarly, in a Mac OS, the backup is usually stored in this directory:

`Users/%username%/Library/Application Support/MobileSync/Backup`

In this directory, we find several interesting files which can be used for forensic investigation. The root of the backup folder mainly contains several key files as status, info and manifest plist files. From this the status.plist file provides data about the latest backup. The info.plist file contains the data which confirms that the backup file matches the device. In this

file, the IMEI number and the phone number can be found. The backup files what we get would be in binary format, so we need to convert it into the human readable format. (Proffit, 2012)

Tools for this approach. For this approach we use iTunes which is provided by Apple Inc. We need to find the path where the backup is stored and can use any third-party application which supports reading of hex data.

Problems with this approach. As discussed in earlier sections as Apple has tightened its security there will be chances that the backup would be encrypted. In this case, we need to investigate a different scenario where we need to purchase additional tools for breaking the passcodes. These tools would enable us to crack the password against the manifest.plist file. One tool which is available on the market is the Elcomsoft phone breaker which will be discussed in later sections.

Acquisition via logical methods. This is one of the most widely used and popular approaches. “Using this approach, the allocated and active files on the iOS device are recovered and analyzed using a synchronization method which is built into the operating system.” All the information regarding the call logs, contacts, photos, etc. can be gathered. This information is what a forensic investigator mainly needs to perform forensic analysis.

Tools for this approach.

iPhone Explorer. iPhone explorer also known as iExplorer is an application developed by Macroplant. As the method suggests we look for logical data on the device. All the files what the forensic investigator needs such as SMS, call log, contacts, messages, etc. are available through this software. The other advantage of using this tool is that we can also restore the information if the device is reset also.

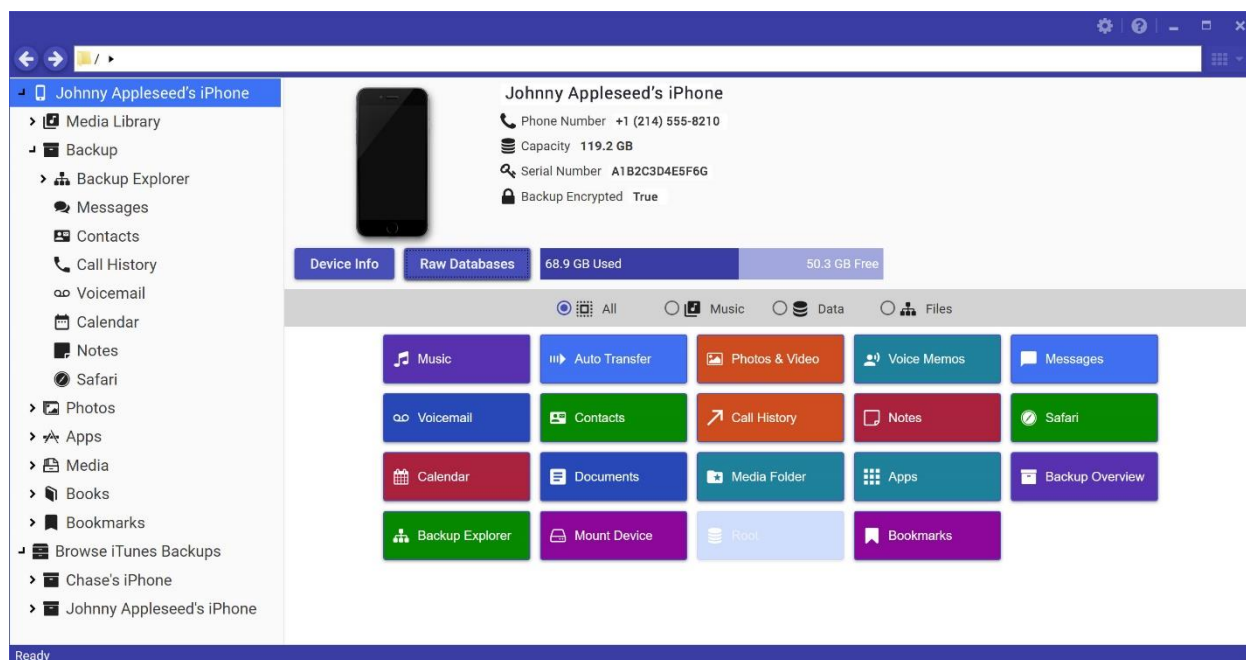


Figure 7. iExplorer (Macroplant, n.d.).

Elcomsoft phone breaker. This tool is developed by Elcomsoft proactive software. It is also one of the methods of logical acquisition of data. It's the main purpose is to decode or break the passcode on iPhone and also break into encrypted backups. By breaking into encrypted backups, we overcome the problem with iTunes backup. This is a major relief as we can obtain and analyze all the information from the backup.

This software also gives a major advantage of breaking the keychain and also accessing iCloud without login and password. We can also decrypt the keys from the users Apple account and use it for access (Elcomsoft, n.d.).

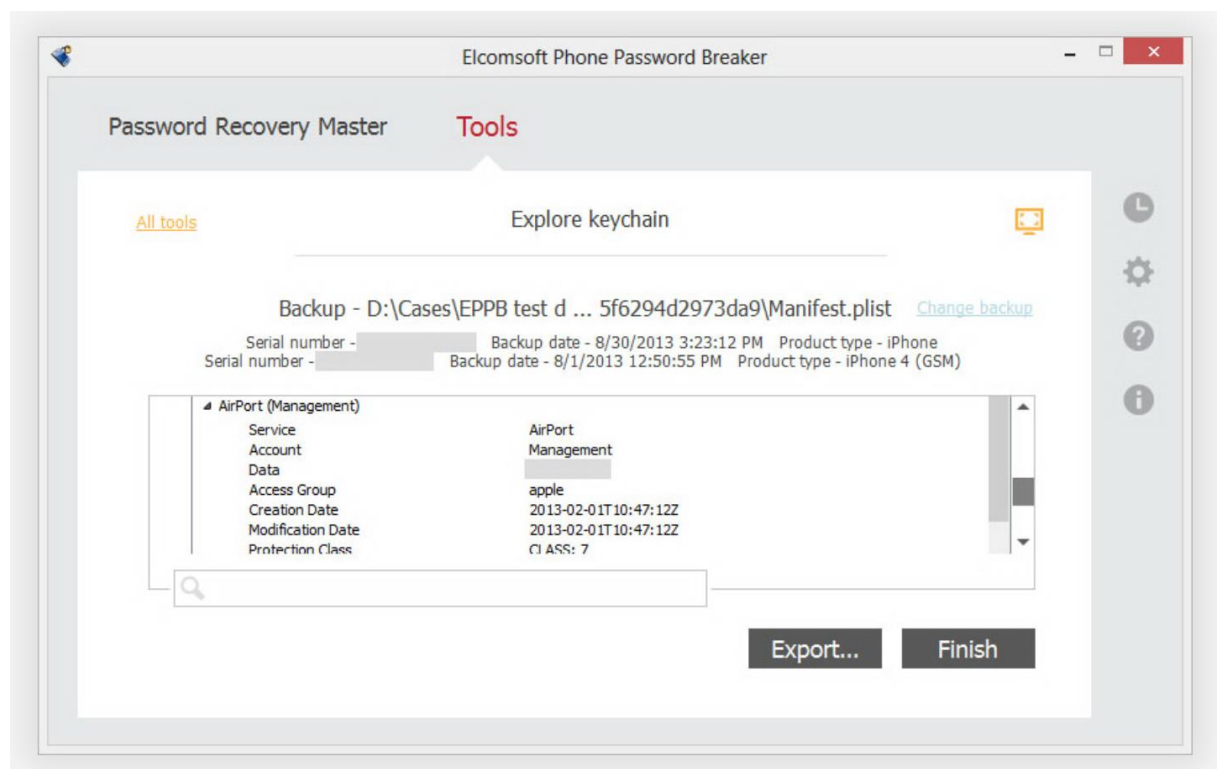


Figure 8. Elcomsoft tool (Elcomsoft, n.d.).

iFunbox. iFunbox is a file and management tool for all iOS devices. It provides a file manager view so that we can easily see what files are present in which folder. It provides a root file system for jailbreak iOS devices by which we can access the data faster and search it. It is a free software and is widely used in the market as a file manager app for iOS devices as the devices don't have one (iFunbox, n.d.).

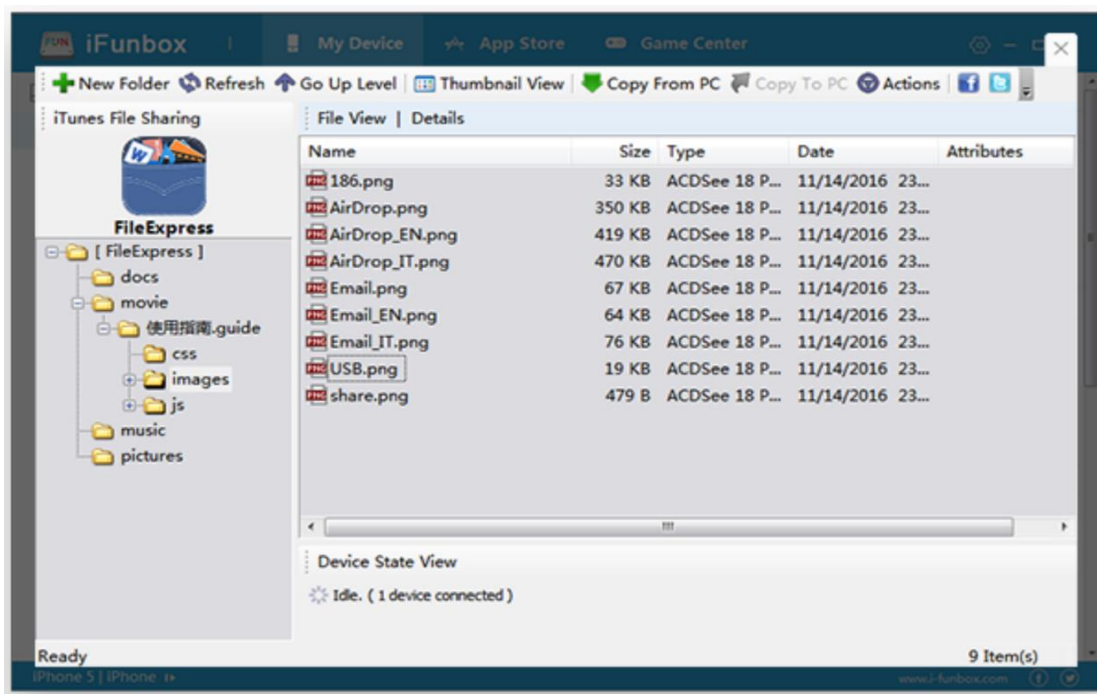


Figure 9. iFunBox (iFunBox, n.d.).

Acquisition via physical methods. A forensic investigator usually likes to get a bit by bit copy of the original data. To get this there are several tools available in the market to perform forensic analysis on laptops, computers and other devices. But as the smartphone market rose tremendously an investigator has the challenge regarding the removal of storage media on iPhone as it is embedded.

One of the first original methods was developed by Zdziarski but as the tool was so perfect and out of the box that Law Enforcement took over it. Apart from this, there are other ways to get the image by using the tools which are discussed as follows:

1. **Elcomsoft iOS forensic toolkit.** This is a tool kit provided by Elcomsoft by which we can perform the physical acquisition of an iPhone. It has various options that we can use to perform operations based on our need. It is not an open-source tool and requires us to pay a certain amount to use.

Acquisition via jail breaking. Jail breaking can be defined as a technique in which we remove the software restrictions imposed by Apple. It permits the root access by which we can install third party applications. It is like the way in which we perform Android rooting in which we can install several custom applications. The status of jail breaking is still in confusion in several countries. Firstly, Apple was not clear and restricted the process but later on, as years passed by it said that it is fine to jailbreak a device. The main problem with jailbreak now is that as newer software versions are released the security is tightened by Apple. This major change has made developers restrict towards not releasing newer patches for the Operating System (Wikipedia, n.d.).

The most popular tools for jailbreak are redSn0w, envasion, and pwnage and Pangu. This process usually involves putting the device in DFU mode (Device Firmware Update) and making sure to install the custom firmware file on the iOS device. By this there were several advantages to the users such as their phones would get unlocked and can be used by any carrier and also, they could install custom apps and many more.

In this method, the workstation is placed in the same wireless network as the device. Then we would pass an SSH command so that we get an image of the device. By this image, the forensic analysts could carry out the investigation. For older devices such as iPhone 3GS it would definitely work but move forward as hardware and software encryption came into place, the image we get will be in an encrypted format and we need to perform the phone breaking process. The SSH command what we give to the shell is: (Proffit, 2012)

```
ssh root@172.16.103.106 dd if=/dev/rdisk0 bs=1M | dd of=ios-root.img
```

There are at present four types of jailbreaks (Wikipedia, n.d.). They can be explained briefly as follows:

Untethered jailbreak. In this process, if the device is turned off and, on the kernel, will be patched without the help of a computer. This is hard to do as it involves a lot of reverse engineering process which requires many years of experience.

Tethered jailbreak. In this process whenever the device gets rebooted, we need to have a computer because it does not have a patched kernel. By this, the phone goes into an unstable state. The jailbreak process is again done so that the device functions properly.

Semi-tethered jailbreak. In this process when the device is rebooted the user needs to use the tool to patch the kernel. If we do not do so the device still performs with the original state and not with the patched kernel.

Semi-untethered jail break. This is a new term and this process was introduced recently. In this when the device boots it does not have the patched kernel but can be patched again if an application is installed on the phone.

Analysis tools. The analysis tools are popular forensic tools that can connect to a mounded iOS image and provide the functionality of analysis. There are many analysis tools out in the market. Some of them are open source and popular and some of them are developed by well-known industries. The analysis tool that we would be using for performing the forensic analysis is a very well-known software called FTK imager. Apart from this, we can also use Encase too (Proffit, 2012).

FTK imager. The forensic toolkit was developed by AccessData. FTK Imager is a simple and concise tool which is a standalone part of the Forensic toolkit. As the name suggests FTK imager is used to create an image of the storage device that can be later reconstructed for analysis (Wikipedia, n.d.).

Files of interest. As the name suggests the files of interest are the main things what we need to look for after we have acquired the device physically or have a backup or image of the storage. Any forensic analyst would generally analyze these files as these provide the evidence what they require.

The files of interest are something as follows:

Applications. The files from the applications installed on the device play an important role. As the crime or illegal activity can be done using certain applications. So, the evidence may be found in these applications files.

Photos. Photos also play a key role and act as an evidence because there might be chances that the person who did a crime may take some photos regarding the crime and delete it. While the forensic analysts perform analysis, they can recover these files.

Keystrokes. All the keystrokes will be stored by the device. By this, we can search for evidence from the user's keystrokes and analyze what they have typed for evidence.

Passwords. Passwords can be helpful to forensic analysts in a lot of ways. First of all they can gain access to the accounts associated with the password and then gain access to all other accounts so that they can search for evidences regarding the crime.

Notes. Notes can be also a key evidence as people generally use it to take notes and add some information which they want to view later. For example in my case I write down tasks what I need to do in a project so that I can view them later and I don't forget it. So, there may be chances that the criminals may use it to take notes such as where they are going to keep the files or evidences associated with the crime.

Text messages. Text messages are the main form of communication used by people. It should not be missed during forensic analysis as it might contain several keen information

regarding the crime. There may be chances that a criminal after committing a crime will communicate with other people to tell them that the job is done, or something related in similar. By performing forensic analysis this key information can be used as an evidence in court.

Call history. Call history usually stores all the calls received, calls made, and calls missed by a person. In a forensic perspective there may be chances that a criminal might contact someone after the crime is committed and delete the log. But by performing forensic analysis we can retrieve the data along with the timestamp and use it as an evidence in the court.

Geographic location. Geographic location mainly gives us the information about the locations recently gone or passed through. For example if a person commits a crime in Minneapolis and if the police suspect him and take him into custody and question him about where he was on a date and he says a place consider Chicago. But after forensic analysis it was clear that the person was present at the place of crime that is Minneapolis then he is acquitted with charges. In this way geographic location plays a key role in forensic analysis.

Browser searches. Last but not the least browser searches also play a key role in forensics. Consider a person committing a crime. Let's suppose he has looked up on the Internet about how to commit a crime then based on his browser searches we can clearly convict him with the crime using the browser searches.

Summary

In this chapter, we discussed about literature related to a problem such as how security constraint prevents forensic analysis on iPhone. We also learnt the file storage system of iPhone along with its architecture. Later on we learnt about literature related to methodology in which we discussed about types of acquisitions on iPhone.

We also discussed various methods in which we can perform the forensic analysis and tools that can be used for this process. All the legal issues associated with the forensic analysis has also been discussed.

The main key terms that we need to focus on called the data of interest has also been discussed. Based on this any forensic analyst would look for these terms so that they can collect the evidence and submit it in the court.

Chapter III: Methodology

Introduction

In this chapter, we will be discussing the methodology about how we are performing the forensic analysis on iPhone. Along with this we also discuss the tools and techniques that we are going to use to perform forensics. We also consider the hardware and software requirements of the device that we are going to use to perform forensics and also the machine that we are going to use.

Design of the Study

The approach that we are going to use is a quantitative study. To begin with, we use an iPhone with the iOS operating system. The main aspect of this research is to retrieve lost data from an acquired iPhone using various approaches. To do this step we need to perform forensic analysis and use several tools so that we can retrieve the deleted data. Several tools what we are going to use have been discussed earlier. Once we acquire the phone using various approaches, we then use this tool and do the operations required. Then we format the report as per the need with all the files that we have restored.

Data Collection

This process involves acquiring an iPhone which has all the media such as photos, videos, and all other sorts of files such as messages, call history, browser cookies, etc.

Then we are going to use the forensic tools and acquisitions discussed in the above chapters so that even if these files get deleted, we can retrieve them. The main approach that we will be looking for is comparing the different types of acquisitions with various tools and see if they are able to retrieve the same data or not.

Hardware and Software requirements. To perform forensics there are many tools that we are going to use which have been discussed earlier. Some of the other requirements are as follows:

1. iPhone
2. iOS operating system
3. Tools and FTK imager
4. Laptop to perform forensics
 - (a) RAM- 8GB
 - (b) Windows 10 Operating system
 - (c) HDD- 1TB
 - (d) Processor- i5 5200U @ 3.0 GHz

Budget

For performing forensics, we require an iPhone and various tools. We require them to purchase so that we can effectively perform forensics. The approximate cost that we would be spending is as follows:

1. iPhone: 300\$-400\$ (may use two models)
2. Tools- 100\$-200\$ (All the tools that I am using are free or mostly open-source)

Chapter IV: Data Presentation and Analysis

Introduction

In this chapter, we will discuss how data is collected using various types of acquisitions mentioned in the previous chapter. We would be analyzing all the data obtained using various tools and provide evidence and findings. We would also discuss how we setup the environment for performing this experiment.

Data Presentation

The data collected is all the information we get from various types of acquisitions we perform. It is in various formats such as images, word documents, pdf files etc. Each of these files have a key information regarding the data that is a valuable evidence for performing forensics.

Installation of software's

Installation of iTunes.

1. First, we go to the website <https://www.apple.com/itunes/download/> to download iTunes.
2. Then we choose the type of operating system we wish to download the version for. As I am using Windows 10, I have downloaded the iTunes for Windows.

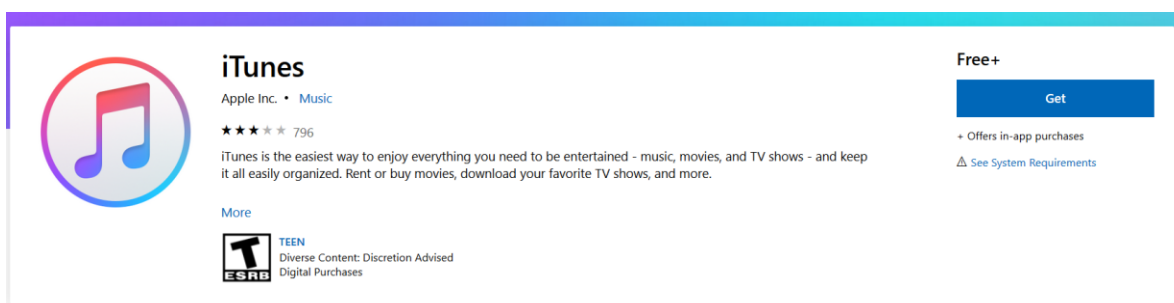


Figure 10. iTunes Microsoft store (iTunes, n.d.).

3. Then after the installation setup, iTunes looks like this,

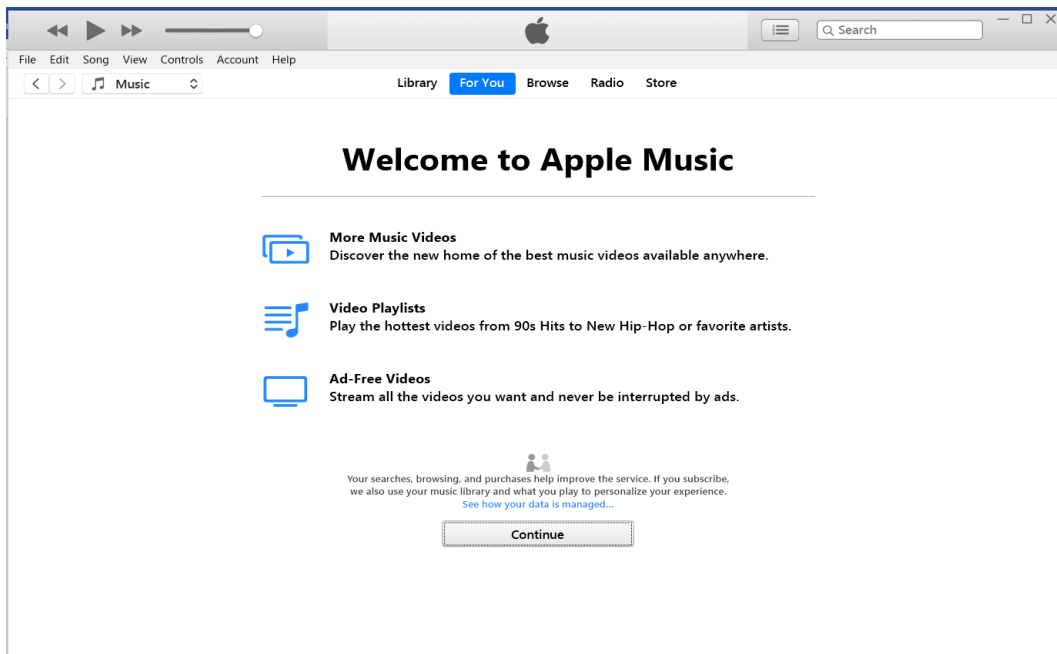


Figure 11. iTunes homepage.

Installation of iPhone Explorer.

1. First we go to <https://macroplant.com/iexplorer> and hit the download button to install the version for Windows.

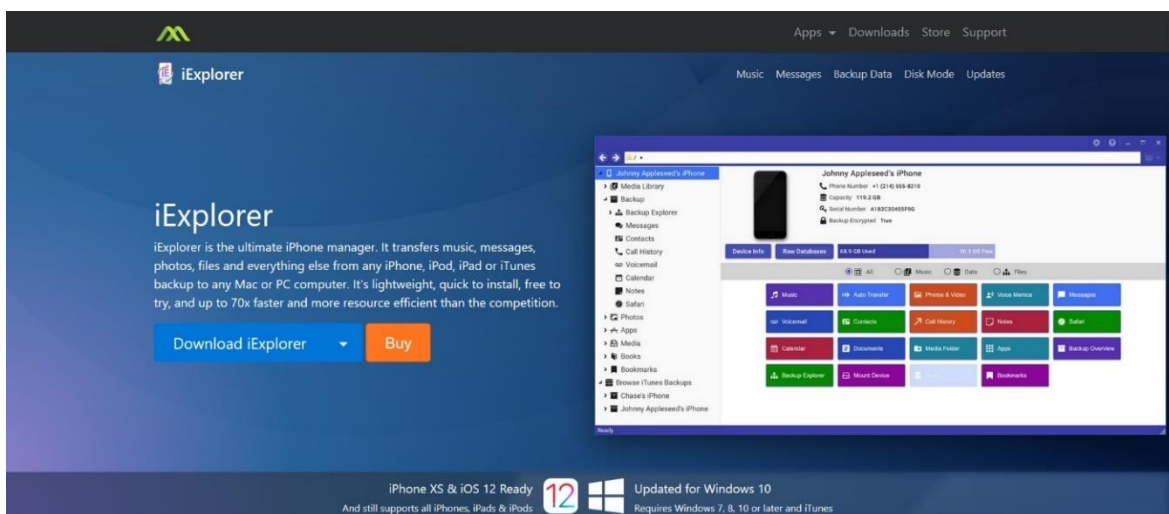


Figure 12. iExplorer (Macroplant website, n.d.).

2. Then save the executable file which can be seen in the picture below:

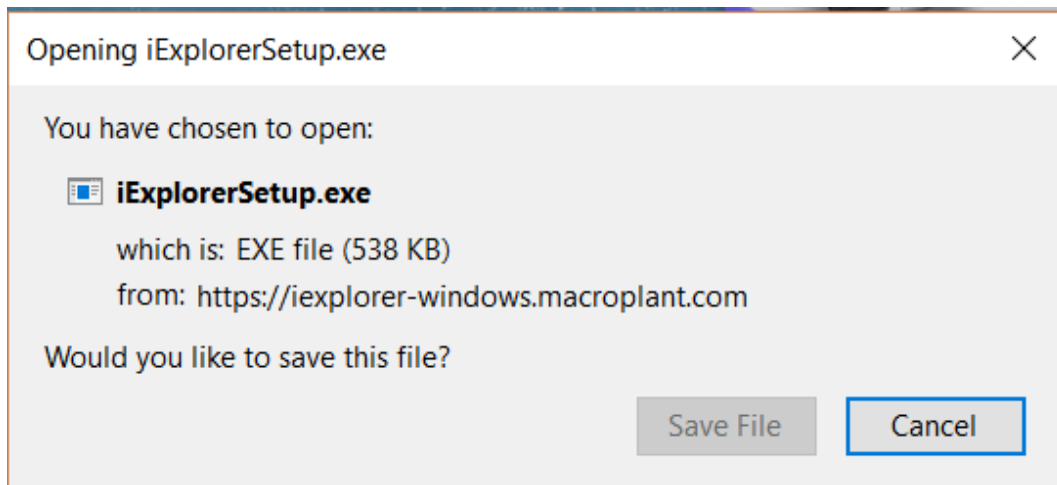


Figure 13. iExplorer setup.

3. Then run the application as Windows always prevents files downloaded from the Internet to run.

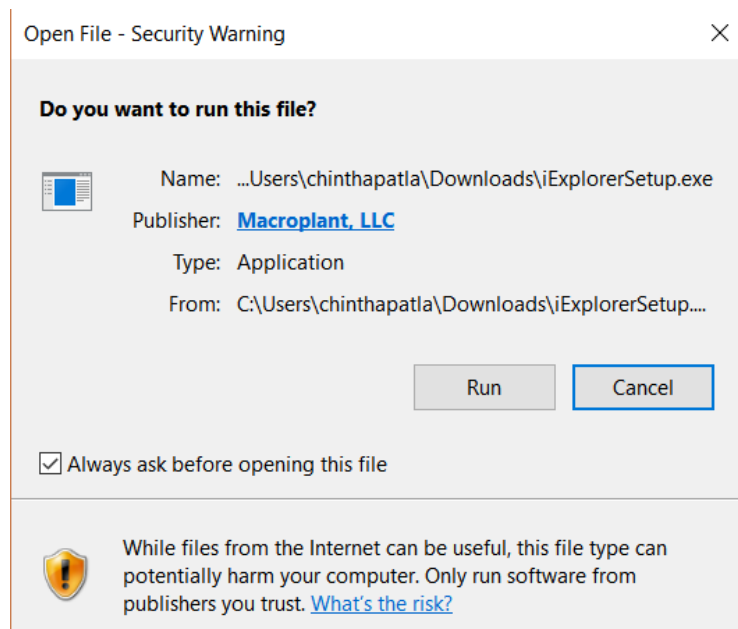


Figure 14. Macroplant security warning.

4. Then after we install the application, we can see the preview as follows:

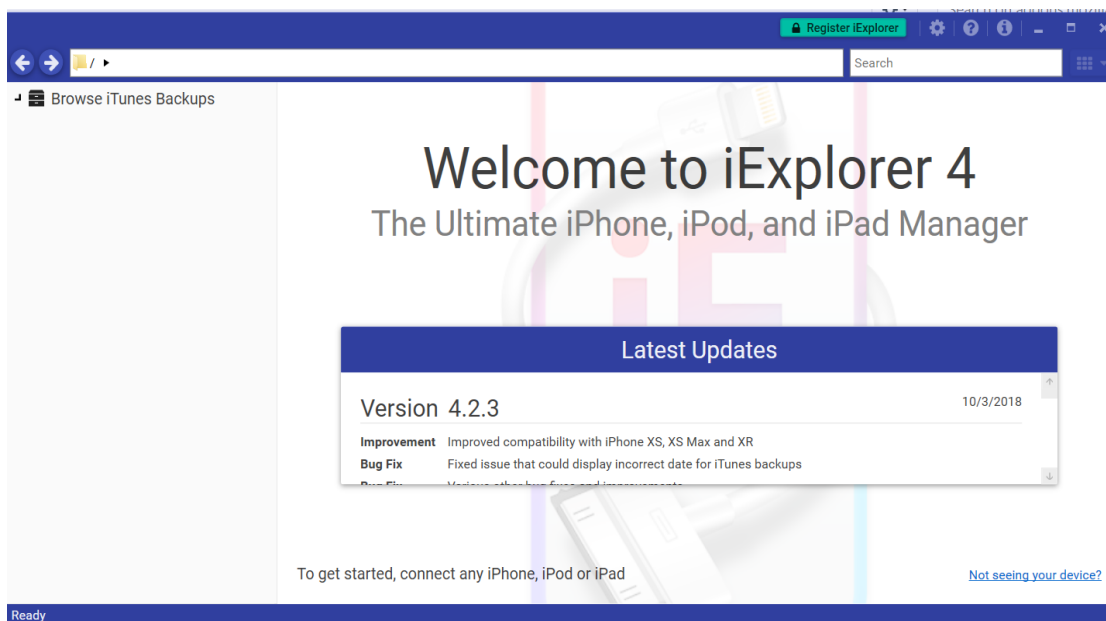


Figure 15. iExplorer preview.

Installation of Elcomsoft phone breaker.

1. First, we go to <https://www.elcomsoft.com/products.html> webpage and click download the version of Elcomsoft phone breaker.

Elcomsoft Phone Breaker



Gain full access to information stored in FileVault 2 containers, iOS, Apple iCloud, Windows Phone and BlackBerry 10 devices! Download device backups from Apple iCloud, Microsoft OneDrive and BlackBerry 10 servers. Use Apple ID and password or extract binary authentication tokens from computers, hard drives and forensic disk images to download iCloud data without a password. Decrypt iOS backups with GPU-accelerated password recovery.

[Learn more](#)

Figure 16. Elcomsoft phone breaker (Elcomsoft Inc, n.d.).

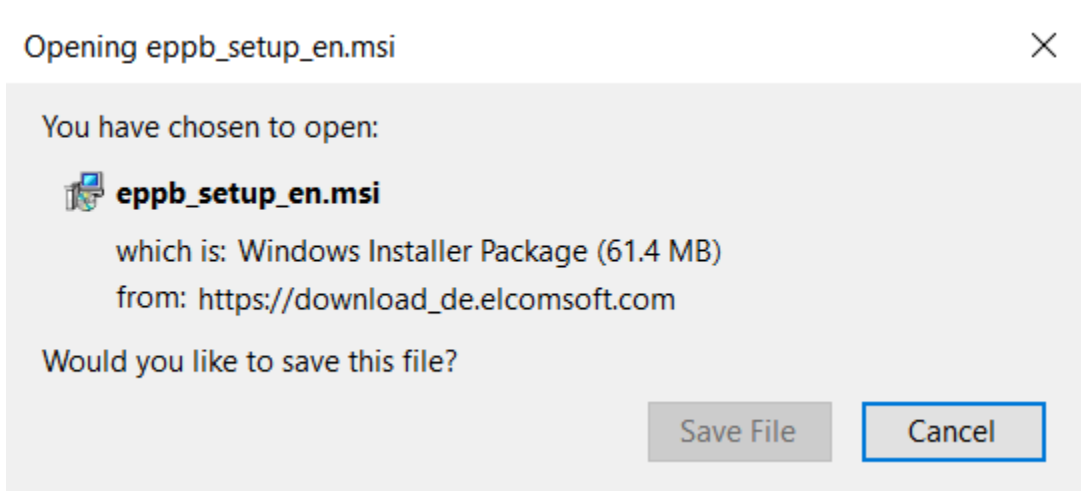


Figure 17. Elcomsoft phone breaker setup.

2. Then we click on the path to specify and enter the trial key provided.

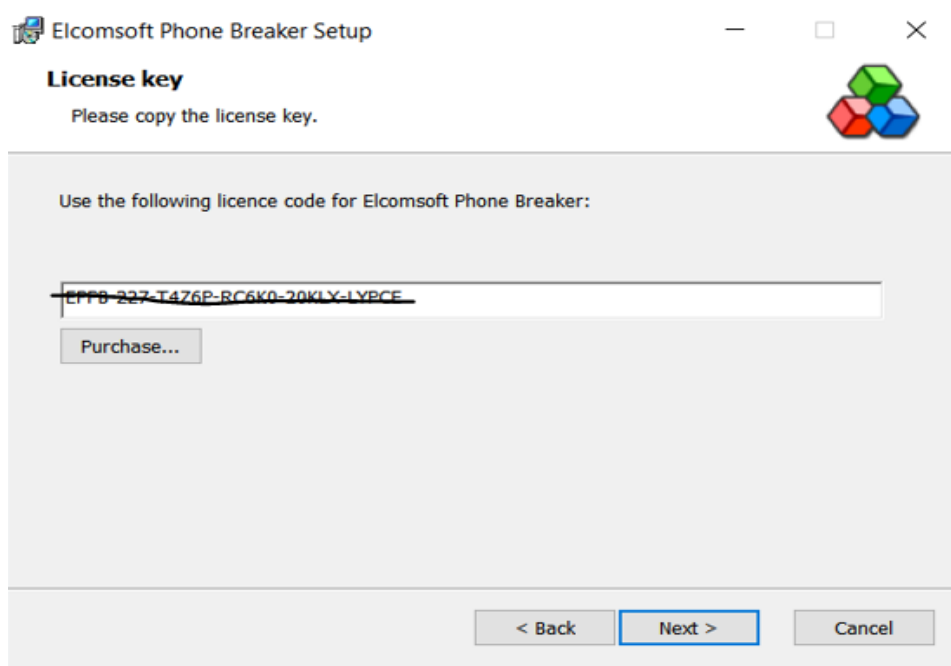


Figure 18. EPB setup.

3. Then after that we can see the preview of the software as follows:

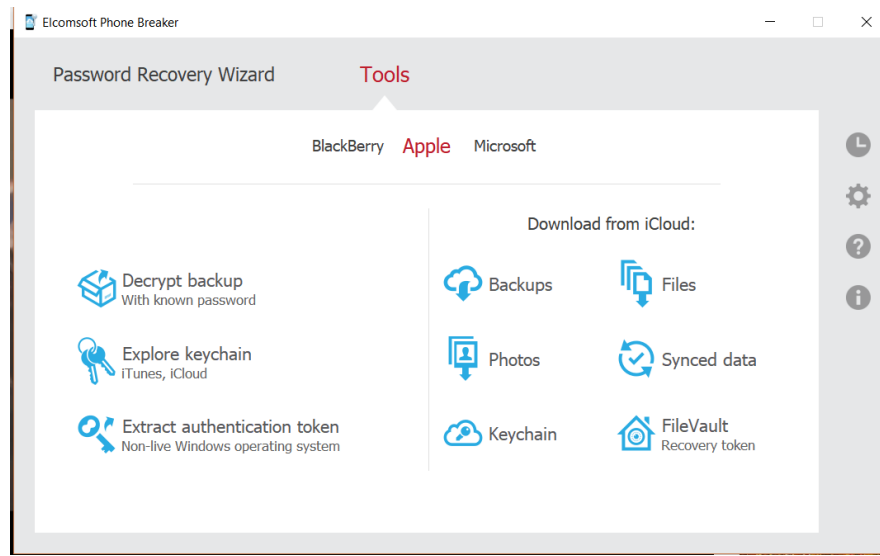


Figure 19. EPB preview.

Installation of iFunbox.

1. First, we go to the http://www.i-funbox.com/en_download.html webpage and click on download.

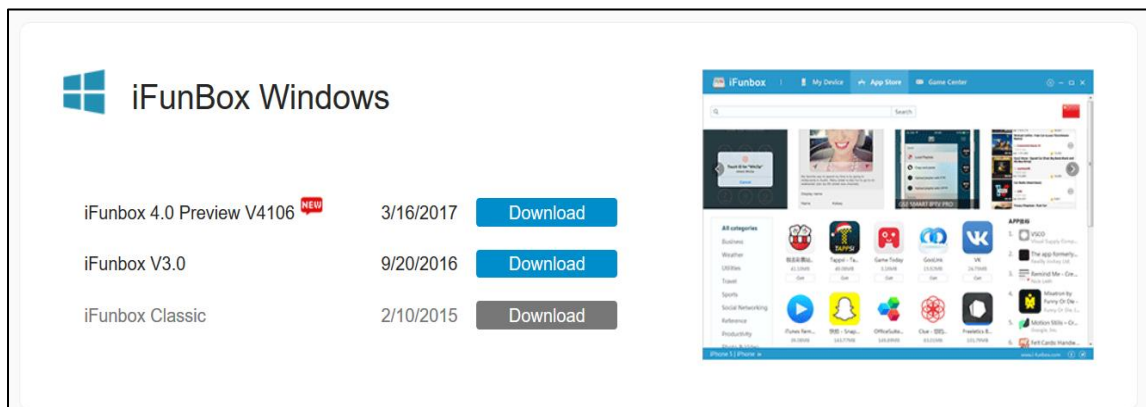


Figure 20. iFunBox (iFunbox, n.d.).

2. Then click on save file.

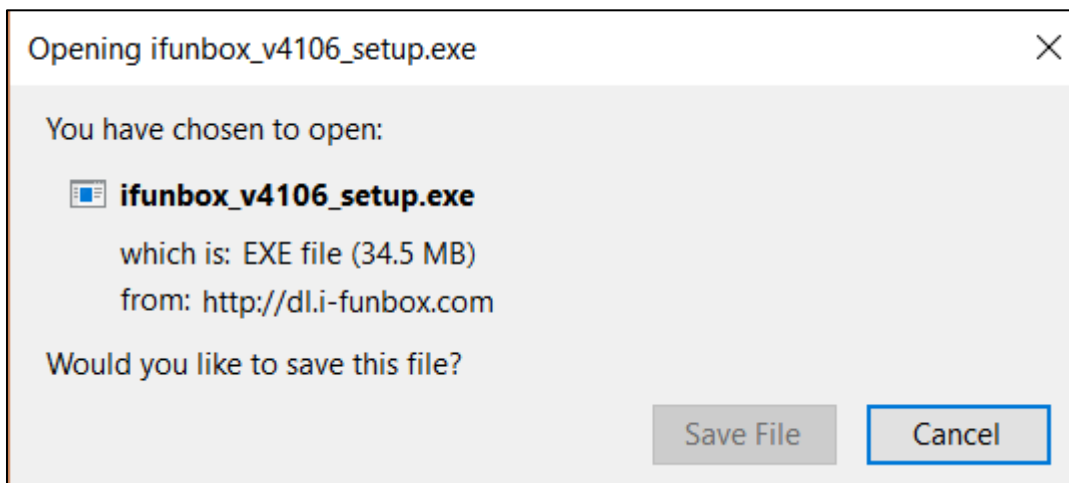


Figure 21. iFunBox setup.

3. Then run the setup file as follows:

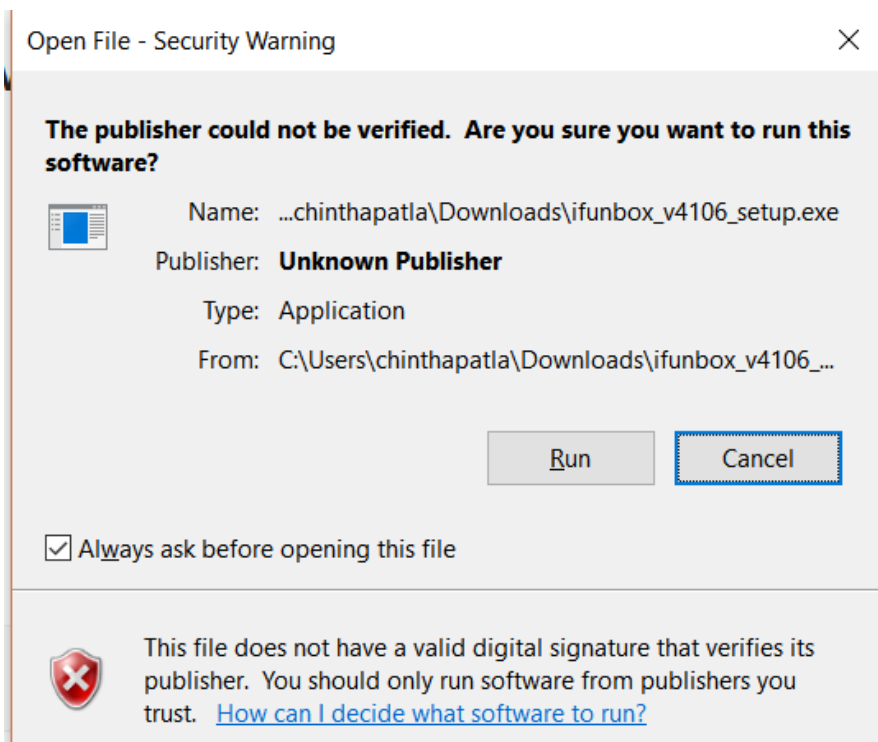


Figure 22. iFunBox setup.

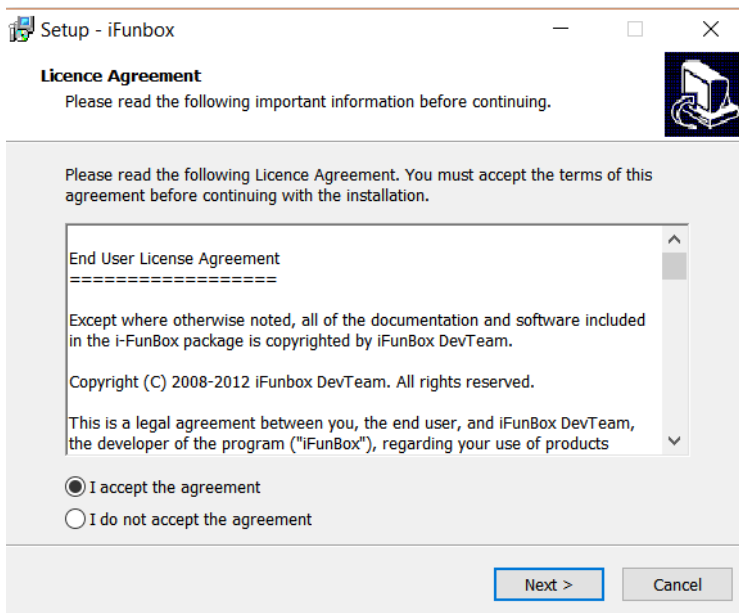


Figure 23. iFunBox agreement.

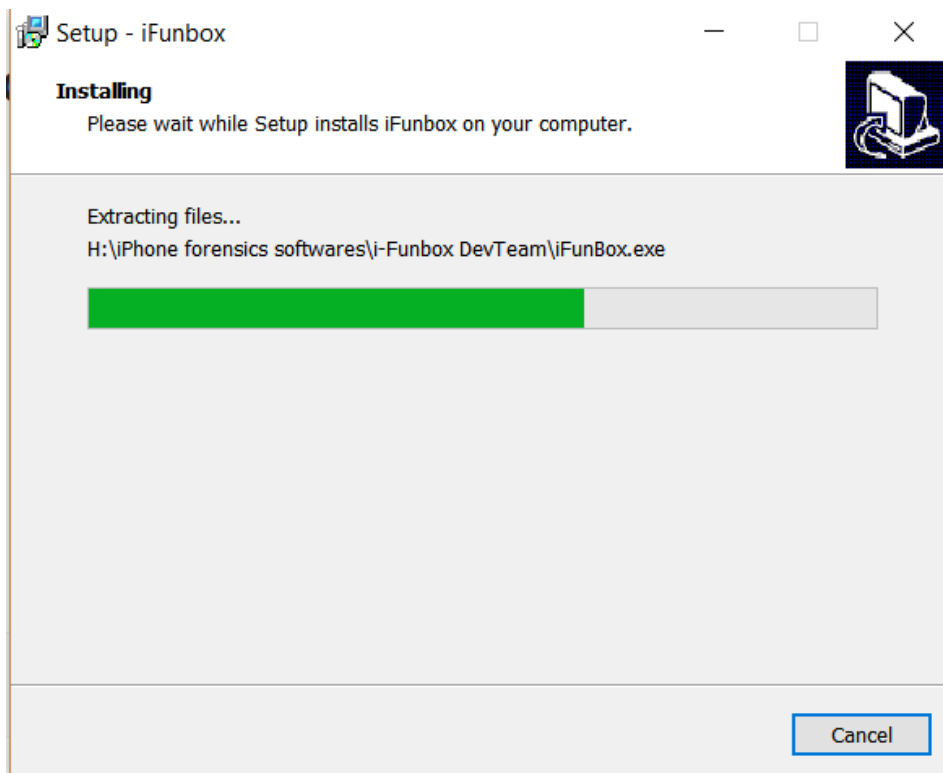


Figure 24. iFunBox setup progress.

4. We can see the preview as follows:

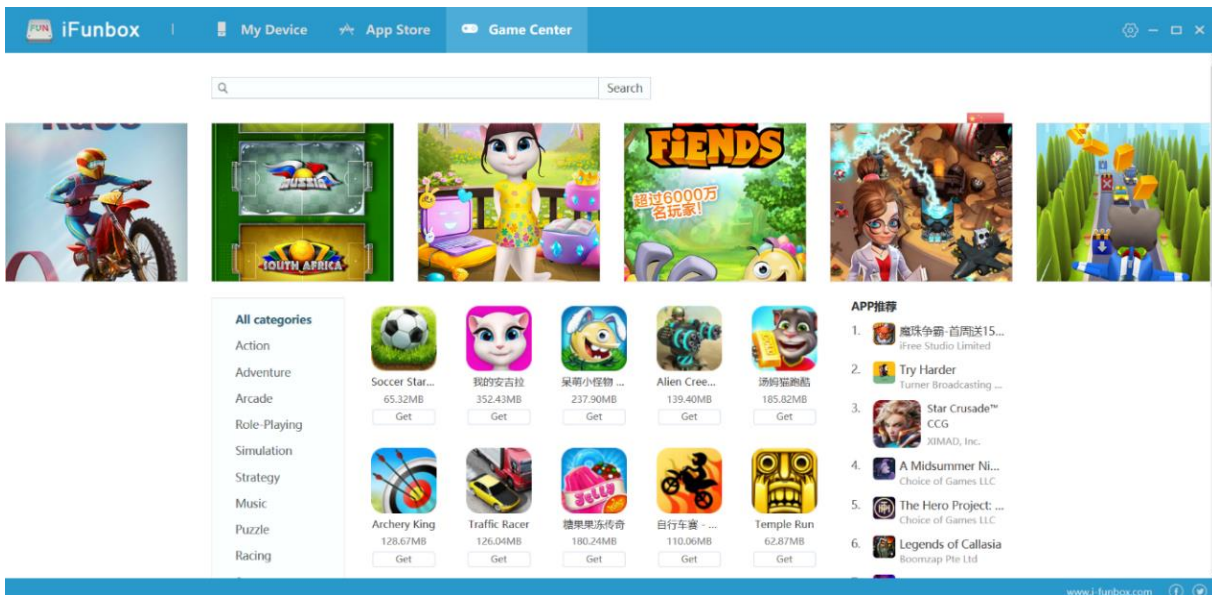


Figure 25. iFunBox preview.

Installation of FTK imager.

1. Go to <https://accessdata.com/product-download> and download FTK imager.

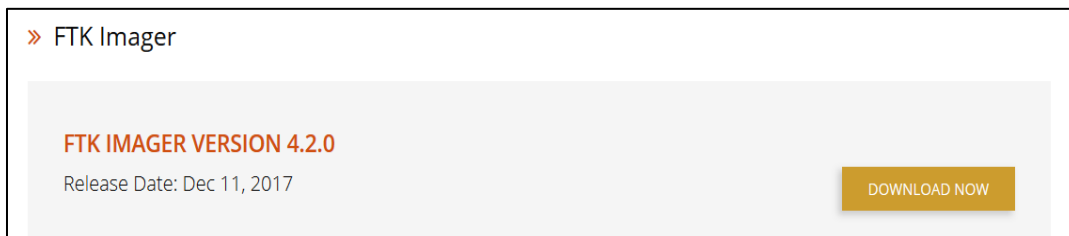


Figure 26. FTK imager download page (FTK imager, n.d.).

2. Then we need to fill in the following form to receive the download link:

To receive the download link, complete the information below

* First Name

* Last Name

* Email

Phone

* Country

* Organization

* Job Title

* Organization Type

Email Opt In
 Yes*

*By selecting 'Yes' you are opting in to marketing communications and consent to receive communications regarding products, services and offerings from AccessData. You may update your [email preferences](#) at any time. Please see our [Privacy Policy](#) for more details.

Figure 27. FTK form.

3. Then we get a confirmation email for download as follows:

[Facebook](#)[Twitter](#)[LinkedIn](#)[Google+](#)[YouTube](#)

Thank you for **downloading FTK® Imager 4.2.0**. If you have any questions or are interested in getting the full version of **FTK**, please email us at sales@accessdata.com.

[Download FTK Imager 4.2.0](#)

For instructions on how to use, view the [eForensics Magazine "FTK Imager Step by Step"](#) issue for step by step instructions or the [FTK User Guide](#).

After you create an image of the data with FTK Imager, you can then use AccessData® Forensic Toolkit® (FTK®) to perform a thorough forensic examination and create a report of your findings. For information about **FTK**, which is recognized around the world as the standard in computer forensic software, visit the [FTK web page](#).

588 West 400 South Suite 350 Lindon, UT 84042 Phone: 801.377.5410
[Contact Us](#)

[unsubscribe from this list](#) | [update subscription preferences](#)

Figure 28. FTK download link.

4. Then we open the installed .exe file after we download and go through the installation process as follows:

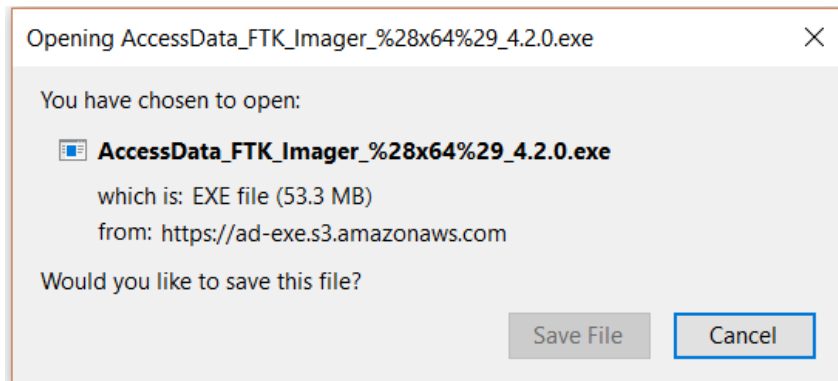


Figure 29. FTK exe file.

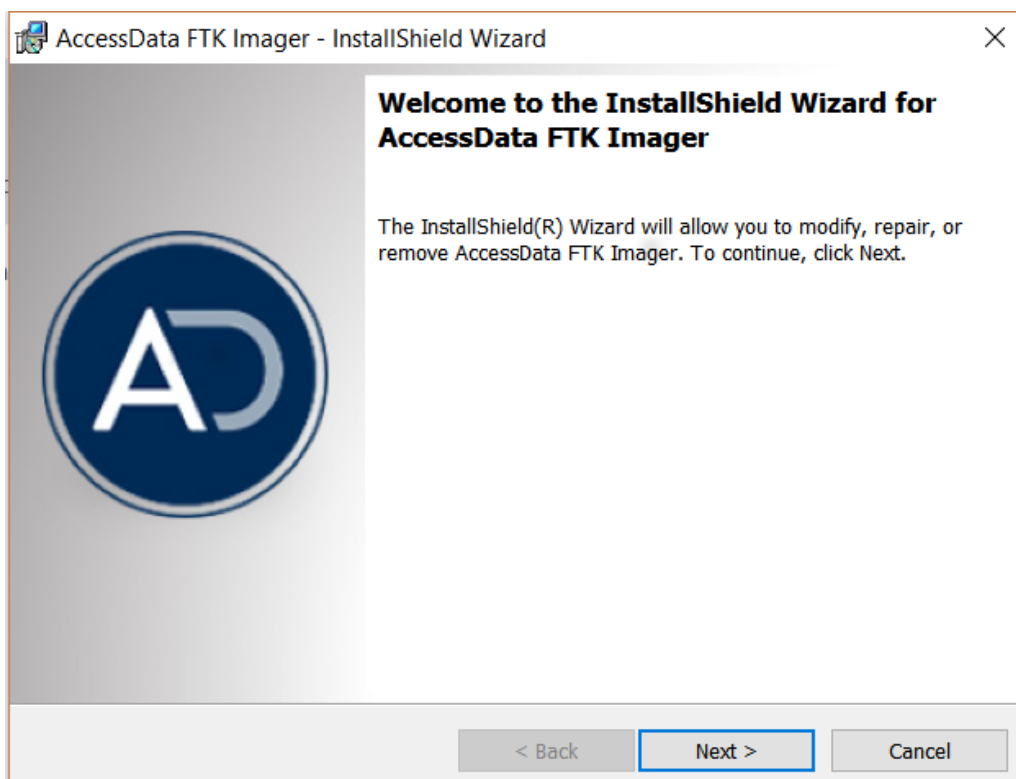


Figure 30. FTK installation wizard.

5. After the installation this is the preview of FTK imager:

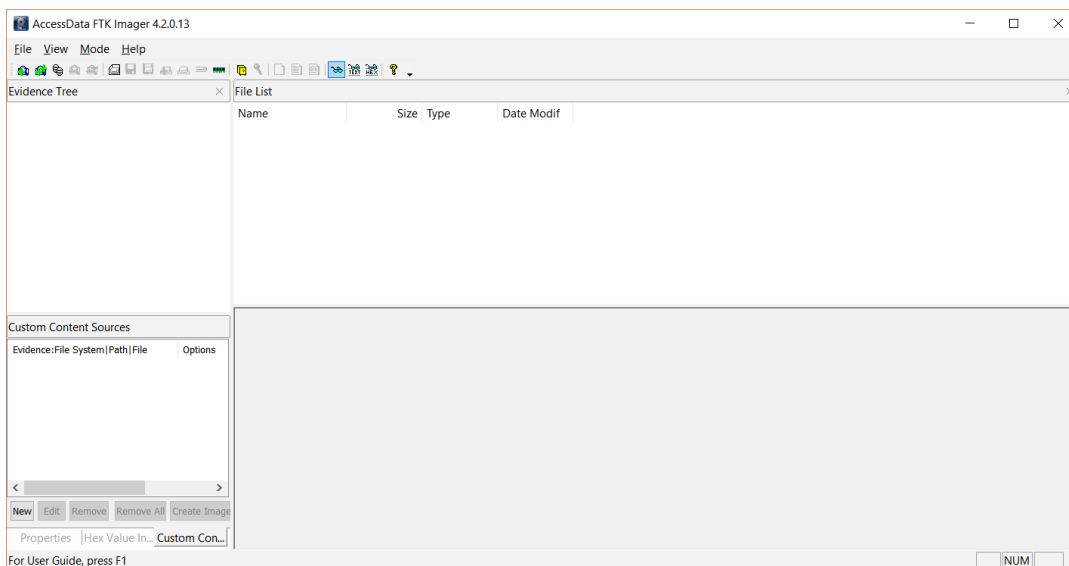


Figure 31. FTK imager preview.

Sources of interest. We have files and folders which are of main interest. For our case we need to take a close look into the folder which contains the iTunes backup. If we take a close look into the folder and perform forensics, we find various evidence files and we can see the screenshots of the folder as follows:

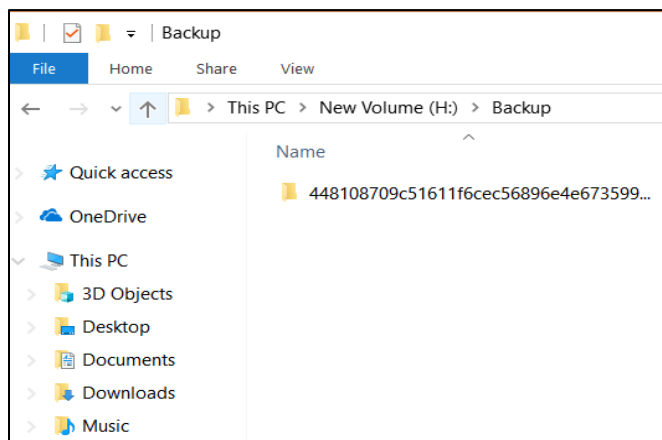


Figure 32. Backup folder preview.

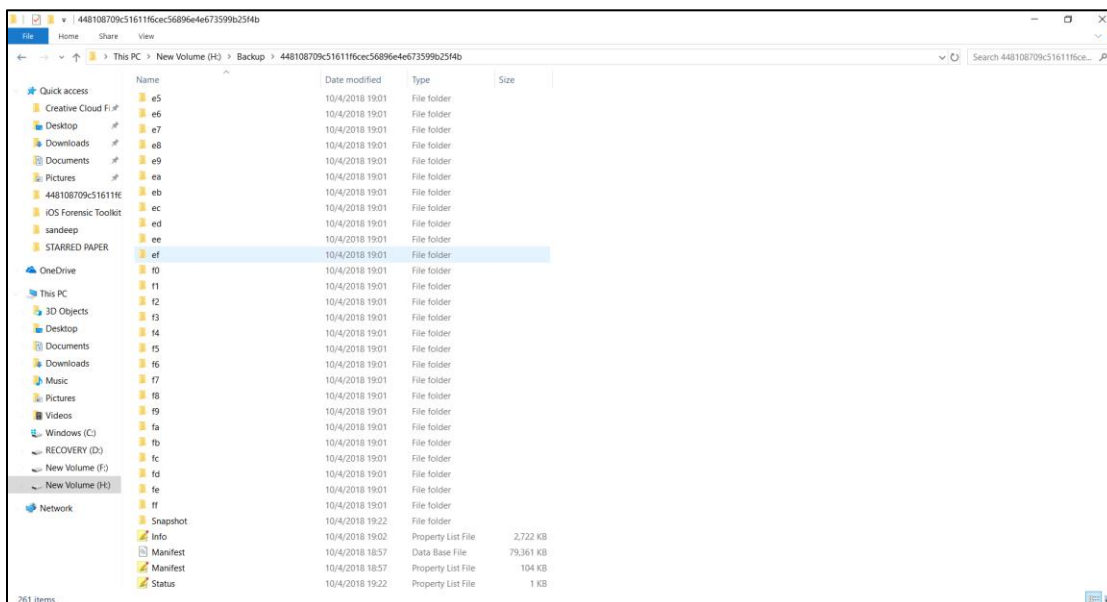


Figure 33. In depth backup folder preview.

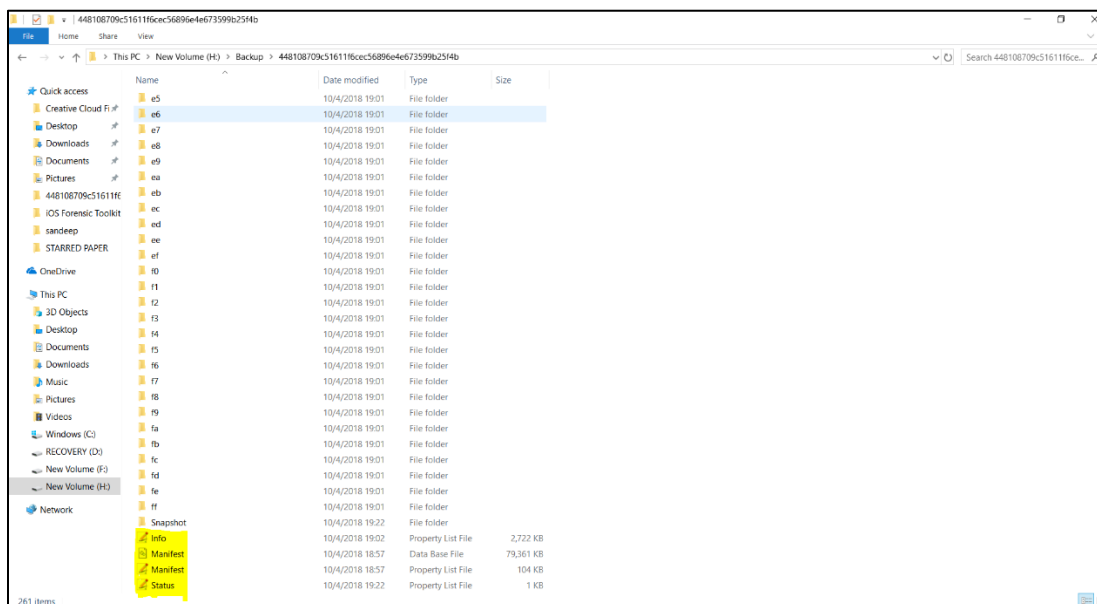


Figure 34. Backup folder file interests

Data Analysis

In this section we analyze all the evidence data which we have collected using various types of acquisitions using all the tools shown in the above section.

Acquisition via iTunes backup. In this procedure we acquire all the evidence information from iTunes backup. The main path where we find the iTunes backup is at the location C:\Users\User\AppData\Roaming\Apple Computer\MobileSync

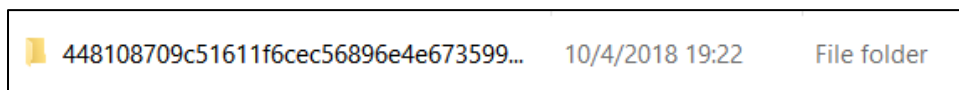


Figure 35. Backup folder.

After we open this folder, we find various files and folders which have all the backup information stored based on the time stamps. The main files of interest are the manifest.plist file which has all the primary information regarding the make and model of the iPhone. We can see the file as follows:





	Info	10/4/2018 19:02	Property List File	2,722 KB
	Manifest	10/4/2018 18:57	Data Base File	79,361 KB
	Manifest	10/4/2018 18:57	Property List File	104 KB
	Status	10/4/2018 19:22	Property List File	1 KB

Figure 36. Backup folder files of interest.

Our next step is to analyze the **Manifest.plist** file. We do it by using a text editor called plist editor pro. When we open the file, we see its content as follows:

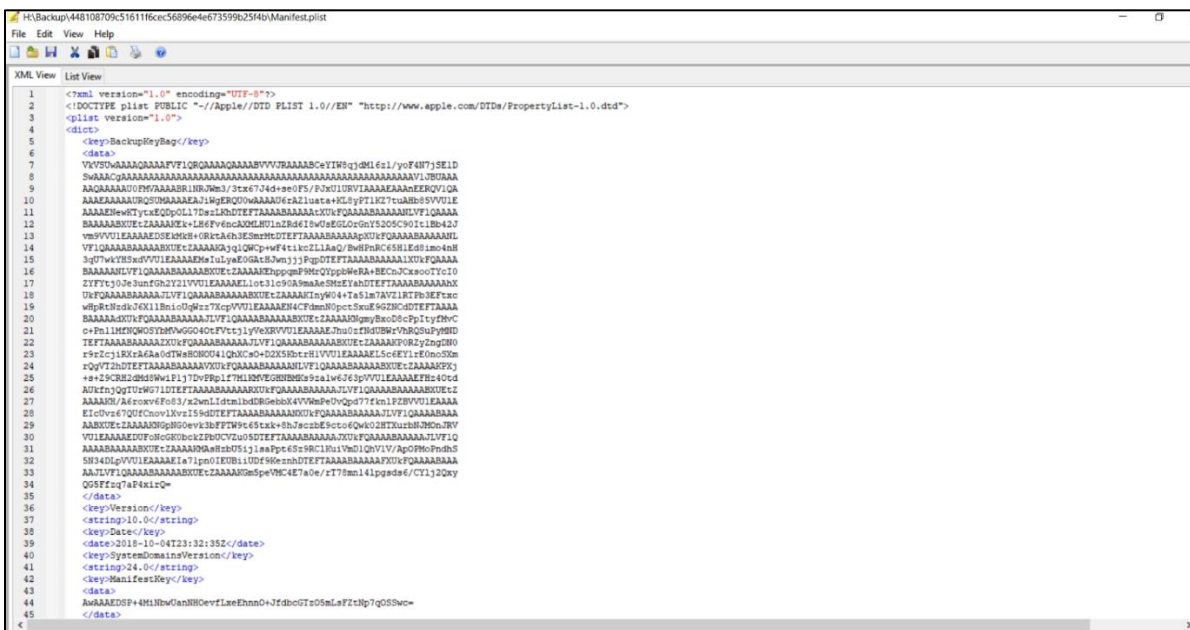


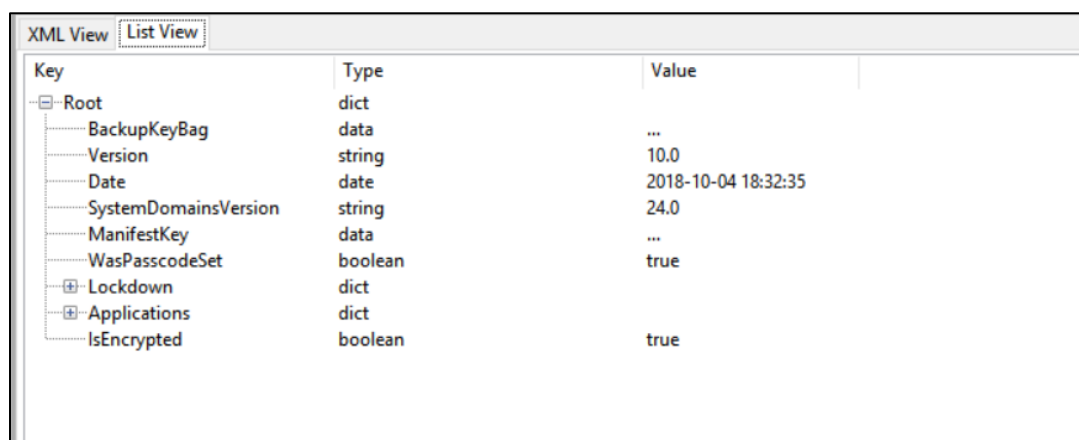
Figure 37. XML view of Manifest.plist file.

If we look closely, we find various directories where all the key information is being stored. We can look at it as follows:



Figure 38. XML view key info.

Now in the plist editor program lets change the mode to list view to get a detailed view of the software version we are using. This step lets the forensic investigator to make things easy as they get to know the iOS version at their first instinct and later can understand various key information whether the backup is encrypted or not and also regarding the date when the device was last backed up. We can see the screenshot of the list view as follows:



Key	Type	Value
-Root	dict	
BackupKeyBag	data	...
Version	string	10.0
Date	date	2018-10-04 18:32:35
SystemDomainsVersion	string	24.0
ManifestKey	data	...
WasPasscodeSet	boolean	true
Lockdown	dict	
Applications	dict	
IsEncrypted	boolean	true

Figure 39. Manifest.plist file list view.

We can see from the above screenshot that the passcode was set to true meaning that the device has a passcode. We can also see that isEncrypted is also true stating that the backup is encrypted.

If we expand the Lockdown section, we get to find more evidence regarding the device as where the contacts are stored, the build version of the iPhone, the product version and also the Unique device Id and the serial number. We can see all those details in the screenshot below:

Lockdown	dict	
com.apple.MobileDeviceCr	dict	
com.apple.TerminalFlashr	dict	
com.apple.mobile.data_syn	dict	
Contacts	dict	
AccountNames	array	iCloud
Sources	array	iCloud
Calendars	dict	
Bookmarks	dict	
Notes	dict	
AccountNames	array	
Sources	array	
com.apple.Accessibility	dict	
ProductVersion	string	12.1
ProductType	string	iPhone9,2
BuildVersion	string	16B5059d
com.apple.mobile.iTunes.a	dict	
com.apple.mobile.wireless_	dict	
UniqueDeviceID	string	448108709c51611f6cec568!
SerialNumber	string	F2LSKALGHFY1
DeviceName	string	iPhone

Figure 40. Manifest.plist file list view key info.

If we take a look at the **info.plist** file we get to find a whole lot of evidence to perform forensics. We get to know the applications installed and deleted on the phone, the GUID, ICCID, MEID, IMEI and even the phone number that was used on the phone.

Key	Type	Value
Root	dict	
Applications	dict	
Build Version	string	16B5059d
Device Name	string	iPhone
Display Name	string	iPhone
GUID	string	A6C1F170126EE007F1199F!
ICCID	string	89011201000537605956
IMEI	string	359174073794380
Installed Applications	array	
Last Backup Date	date	2018-10-04 19:02:42
MEID	string	35917407379438
Phone Number	string	XXXXXXXXXX 5878
Product Name	string	iPhone 7 Plus
Product Type	string	iPhone9,2
Product Version	string	12.1
Serial Number	string	F2LSKALGHFY1
Target Identifier	string	448108709c51611f6cec568!
Target Type	string	Device
Unique Identifier	string	448108709C51611F6CEC56
iBooks Data 2	data	...
iTunes Files	dict	
iTunes Settings	dict	
iTunes Version	string	12.9.0.167

Figure 41. List view key info.

If we dive deep into the installed applications, we can see all the applications that were installed on the phone. Based on those we can try to pull out data. For example, if there is an application such as Uber, we can get to know all the trips the person had with his account by contacting Uber. We can see all the installed applications as follows:

Installed Applications	array	
	string	com.sololearn
	string	com.google.Gmail
	string	com.google.photos
	string	com.ubercab.UberEats
	string	com.samsclub.sng
	string	com.ubercab.UberClient
	string	com.bitstrips.imoji
	string	com.6wunderkinder.wund
	string	com.Saavn.Saavn
	string	de.2kit.cast-browser-roku
	string	com.experian.experianapp
	string	com.tencent.ig
	string	com.amazon.Amazon
	string	com.okta.mobile
	string	com.facebook.Messenger
	string	com.jetsonbike.Jetson
	string	com.discoverfinancial.mo
	string	com.glassdoor.glassdoor
	string	com.apple.supportapp
	string	com.amazon.aiv.AIVApp
	string	com.linkedin.Linkedin
	string	com.apple.mobilegarageb
	string	com.facebook.Facebook
	string	com.zomato.zomato
	string	com.tinyspeck.chatlyio
	string	com.dzo.haumanchalisaa
	string	com.google.ios.youtube
	string	com.usaa.UsaaMobile
	string	com.adrise.tubitv
	string	com.xoom.app

Figure 42. Application list.

Now we explore furthermore we can find all the deleted applications too. This could also help us in playing a key evidence item because we can further investigate if the person has committed crime using any of those applications and deleted it later. In our case we can see the screenshot of the deleted applications as follows:

The screenshot shows the 'DeletedApplications' key in the iTunes Settings plist file. The key is of type 'array' and contains a list of application identifiers. Two identifiers are highlighted in yellow: 'com.xiaomi.miwifi' and 'com.bestbuy.buyphone'.

DeletedApplications	Type	Value
	array	
	string	com.apple.iMovie
	string	com.apple.Keynote
	string	com.cardify.tinder
	string	com.united.UnitedCustomr
	string	com.bsb.hike
	string	com.xiaomi.miwifi
	string	com.abercrombie.hollister
	string	com.teamviewer.rc
	string	com.d2l.brightspace.pulse
	string	com.fodmld.OfficialF1
	string	com.bluebook.theblueboc
	string	com.clearchannel.iheartra
	string	com.hungama.myplay
	string	olacabs.OlaCabs
	string	com.bestbuy.buyphone
	string	com.mcdonalds.mcdonal
	string	bundl.swiggy
	string	com.aircanada.csp.aciclier
	string	com.zomato.zomato

Figure 43. Deleted application list.

Now let's take a look at **status.plist** file. As the name suggests it has all the status of the backup state and also whether the backup is done completely or not. We can see the preview of it as follows:

The screenshot shows the 'status.plist' file in a key-value view. The root key is of type 'dict' and contains several keys related to the backup state.

Key	Type	Value
Root	dict	
IsFullBackup	boolean	true
Version	string	3.3
UUID	string	201FFBEB-8DAB-40FB-881
Date	date	2018-10-04 19:22:03
BackupState	string	new
SnapshotState	string	uploading

Figure 44. Status.plist view.

Apart from all these files there is a folder called **Snapshot** which contains sub folders and files. The snapshot folder stores all the information for each point of time such as when the Wi-

Fi is turned off on the device it saves a snap and when it is turned on again it saves another snap.

By this we have all the snaps what the user has done at each instinct of time. We can see the preview as follows:

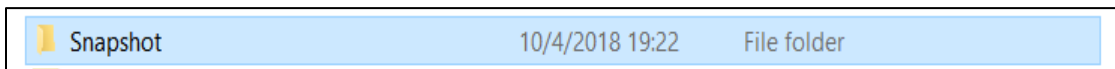


Figure 45. Snapshot folder.

After we open the folder, we can see the sub-folder as follows:

00	10/4/2018 19:34	File folder
0a	10/4/2018 19:34	File folder
0b	10/4/2018 19:34	File folder
0c	10/4/2018 19:34	File folder
0d	10/4/2018 19:34	File folder
0e	10/4/2018 19:34	File folder
0f	10/4/2018 19:34	File folder
01	10/4/2018 19:34	File folder
1a	10/4/2018 19:34	File folder
1b	10/4/2018 19:34	File folder
1c	10/4/2018 19:34	File folder
1d	10/4/2018 19:34	File folder
1e	10/4/2018 19:34	File folder
1f	10/4/2018 19:34	File folder
02	10/4/2018 19:34	File folder
2a	10/4/2018 19:33	File folder
2b	10/4/2018 19:34	File folder
2c	10/4/2018 19:33	File folder
2d	10/4/2018 19:33	File folder
2e	10/4/2018 19:34	File folder
2f	10/4/2018 19:33	File folder
03	10/4/2018 19:34	File folder
3a	10/4/2018 19:34	File folder
3b	10/4/2018 19:34	File folder
3c	10/4/2018 19:34	File folder
3d	10/4/2018 19:33	File folder
3e	10/4/2018 19:34	File folder
3f	10/4/2018 19:34	File folder
04	10/4/2018 19:33	File folder
4a	10/4/2018 19:34	File folder

Figure 46. Insight of snapshot folder.

For example, if we open a sub-folder, we can see the snaps as follows which contains all the information of snaps:

2a2b79c43da3865c5ed20b796af818702a...	10/4/2018 19:23	File	75 KB
2a4bc4f72d2426f98562e37cff76f6b26afff	10/4/2018 19:32	File	1,142 KB
2a4e67cdd6dd8a432af5023eaa00f0afb3...	10/4/2018 19:24	File	88 KB
2a4e563ae26da6c10fa1ed95574382677b...	10/4/2018 19:23	File	24 KB
2a5d5394c6f4807b96ef85b029df6959c04...	10/4/2018 19:29	File	1,082 KB
2a06a10188e81e3fe04dbbb496f80c27de...	10/4/2018 19:25	File	1 KB
2a6a314572d46473aabbcb896fc7bff44ad...	10/4/2018 19:23	File	61 KB
2a6acd6f05173225b7d54a7875080a9006...	10/4/2018 19:24	File	86 KB
2a6b3a06877a4321aec3310ce3c6bc4cb5...	10/4/2018 19:25	File	1 KB
2a6b69d157dce5c099030a5704c491d284...	10/4/2018 19:23	File	57 KB
2a6c753a8ab12a1d53f702269ccbd1e704...	10/4/2018 19:23	File	67 KB
2a7b3ba78311c4752eb70a9ca9b2ae689...	10/4/2018 19:22	File	88 KB
2a8f0c55f71e60f8d1c420f2a4aa89ad431...	10/4/2018 19:22	File	6 KB
2a8f290a7c46f66c2356ec773ce4ab06c9d...	10/4/2018 19:23	File	60 KB
2a9e80d11f980e5c6771e2b0bbcb3fec30...	10/4/2018 19:23	File	106 KB
2a12cf959413b1b9769b69b872d51ce17b...	10/4/2018 19:23	File	66 KB
2a17e6a5330755bd2cf3fe0c9dfc631514d...	10/4/2018 19:22	File	1,911 KB
2a28ea10bb6322be802a49d32adcbf47d...	10/4/2018 19:23	File	86 KB
2a39a13824fabbf56868bf748af554b02ee...	10/4/2018 19:33	File	116 KB
2a44c2255448b791b0eed24ddd0b89b11...	10/4/2018 19:23	File	60 KB
2a49e63c6e32a573d8c53a212c71513e7a...	10/4/2018 19:24	File	1 KB
2a51d7d371bb3ef222afb07932b9135886...	10/4/2018 19:28	File	126 KB
2a57f454690905935c1c606e1008a075fa4...	10/4/2018 19:28	File	403 KB
2a58f43ddda09d568cfe9a2a4e55252d7f...	10/4/2018 19:23	File	62 KB
2a70dd85742ca02546af83bc69ee1df553...	10/4/2018 19:22	File	13 KB
2a71ad570cd71a9a51127d58e06505c9f9...	10/4/2018 19:33	File	180 KB
2a80a0e0efb6e78fc1bf61883f0053f68bf5...	10/4/2018 19:22	File	1 KB
2a80ee1aa3b95a3c02fe2d768b8677fcd9...	10/4/2018 19:22	File	1 KB
2a92d2b2fd4314fe368008a224fbfbc6e19...	10/4/2018 19:23	File	1 KB
2a101bd7c018ebabd8703d9cff4419d06e...	10/4/2018 19:28	File	611 KB
2a109ef5154762a3d20080c61c6464b6fc1...	10/4/2018 19:22	File	18 KB
2a301c477244833c83f6d20802a74dcebb...	10/4/2018 19:22	File	267 KB

Figure 47. Snaps view.

By this type of acquisition, we get to know a basic info of what model of the phone the person was using and what iOS version was on it. We also get to know about the detailed view of whether the backup was encrypted or not and also about the last data when the phone was backed up to the system. This step of acquisition can be considered as the first step towards performing iPhone forensics.

Acquisition via logical methods. For acquisition via logical methods the tools we are going to use are iPhone Explorer, Elcomsoft phone breaker and iFunBox. These tools have their own set of features and interfaces which make them to stand out from rest of the tools. Now let's see the various tools that we use for Logical acquisition:

1. iPhone Explorer.

2. First, we open iPhone Explorer and see for interesting views on the left-side panel.

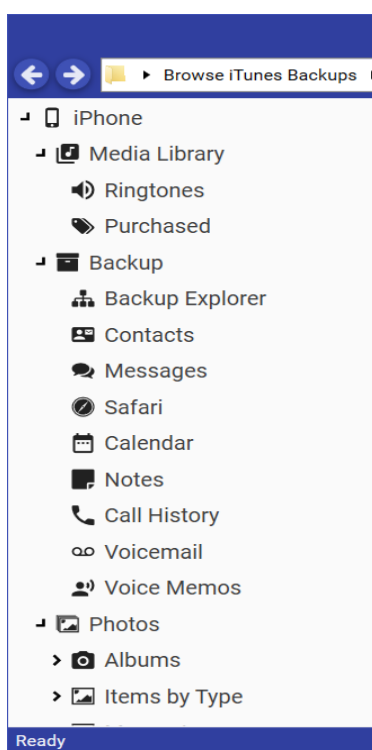


Figure 48. iPhone explorer view.

Then we see a whole list of actions available such as view messages, contacts, call history, photos and much more.

3. Now we need to explore all of them as all these are potential folders for finding and performing forensics.

1. **Checking for messages:** Now we click on Messages and get a window which lists all the messages. We can see the preview as follows:

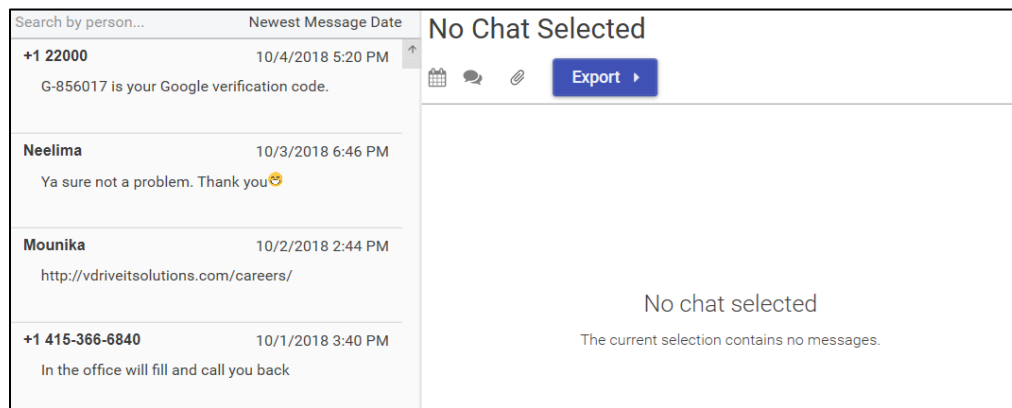


Figure 49. iPhone explorer messages view.

2. **Checking Call history:** Now we click on call history and we get to see all the recent calls that the person made, received and missed. We can see the preview as follows:

Contact	Date of Last Call	Count	Call Type	Contact
(All)	10/4/2018 10:28 PM	331	Outgoing Face Time	Mounika
Nikita	10/4/2018 10:28 PM	3	Incoming Face Time	Mounika
Mounika	10/4/2018 7:19 PM	86	Incoming Face Time	Subash Reddy Velimineti
Neelima	10/4/2018 3:07 PM	7	Canceled	Mounika
Rebtel Local Call	10/4/2018 4:29 AM	37	Outgoing Face Time	Shoban Kandala
Aditya Anna	10/3/2018 11:44 PM	6	Outgoing Face Time	Shoban Kandala
			Incoming Face Time	Mounika
			Incoming Face Time	Mounika

Figure 50. iPhone explorer call history view.

3. **Checking for photos:** Now we check for photos as this folder also plays a key evidence in forensics. We see the time stamps and the location where the photo was taken. This is a crucial information. We see the preview as follows:








Name	Date Modified	Type	Size
 Jan 01	1/1/2018 7:23:16	Folder	
 Jan 01 (2) - 49th Ave SW, May, MN	1/1/2018 5:23:58	Folder	
 Jan 01 (3) - St. Cloud, Home	1/1/2018 8:50:33	Folder	
 Jan 02	1/2/2018 5:00:33	Folder	
 Jan 02 (2)	1/2/2018 11:01:59	Folder	
 Jan 03 - St. Cloud, Home	1/3/2018 3:21:17	Folder	
 Jan 03 (3) - St. Cloud, Home	1/3/2018 3:42:58	Folder	
 Jan 03 (2) - W Division St, West End, MN	1/3/2018 9:08:06	Folder	

Figure 51. iPhone explorer photos view.

- 4. Checking for contacts:** Now we look for contacts as this is also the main file of interest for performing forensics. We see that we find all the contacts that are saved on the phone. We can see preview of the contacts as follows:






Groups	Contact
(All)	 Abhinav +919002000000
	 Abhinav Scl +919002000000
	 Abhishek 310 +91 9002000000
	 Abhishek Chintapatla
	 Abhishek Vangala +919002000000

Figure 52. iPhone explorer contacts view.

- 5. Checking for Safari history:** Checking for search history also plays a key role in forensic activity. We can see what webpages the user bookmarked and also the history of websites what the user has visited. We can see the preview as follows:

Bookmarks	Page Title	URL	Visits	Last Visited
History	iPhone User Guide	https://help.apple.com/iphone/guide/		
	My Sprint Mobile	http://www.sprint.com/?ECID=iPhoneOS:Spr		
	Apple	https://www.apple.com/		
	Bing	https://www.bing.com/		
	Google	https://www.google.com/?client=safari&char		
	Yahoo	https://yahoo.com/		
	iClarified - Apple News and Tutorial	http://www.iclarified.com/		
	Home - YouTube	https://m.youtube.com/		
	BGR – Tech and entertainment new	https://bgr.com/		

Figure 53. iPhone explorer history view.

- 6. Checking for Notes:** Notes also plays a vital role in forensics. It might contain vital information about the user's data as they might save certain information in them. We can see the preview of notes as follows:

iCloud	Notes
Recently Deleted 7	8a 8/3/2018 11:49 AM
Notes 2	A 8/3/2018 11:48 AM
Notes 63	New Note 7/14/2018 2:40 PM
All iCloud 65	New Note 11/15/2017 6:57 PM
	New Note 10/12/2017 5:49 AM
	New Note 10/1/2017 8:07 AM
	New Note 9/19/2017 8:30 PM

Figure 54. iPhone explorer notes view.

7. Checking for applications: Now we can see what all applications are installed on the phone if we go to the Apps folder. We can see the preview as follows:

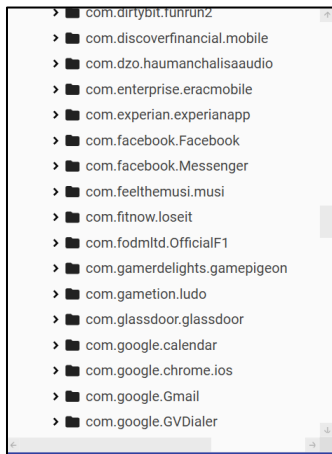


Figure 55. iPhone explorer applications view.

2. Elcomsoft Phone breaker. First, we open Elcomsoft phone breaker and we see the preview as follows:

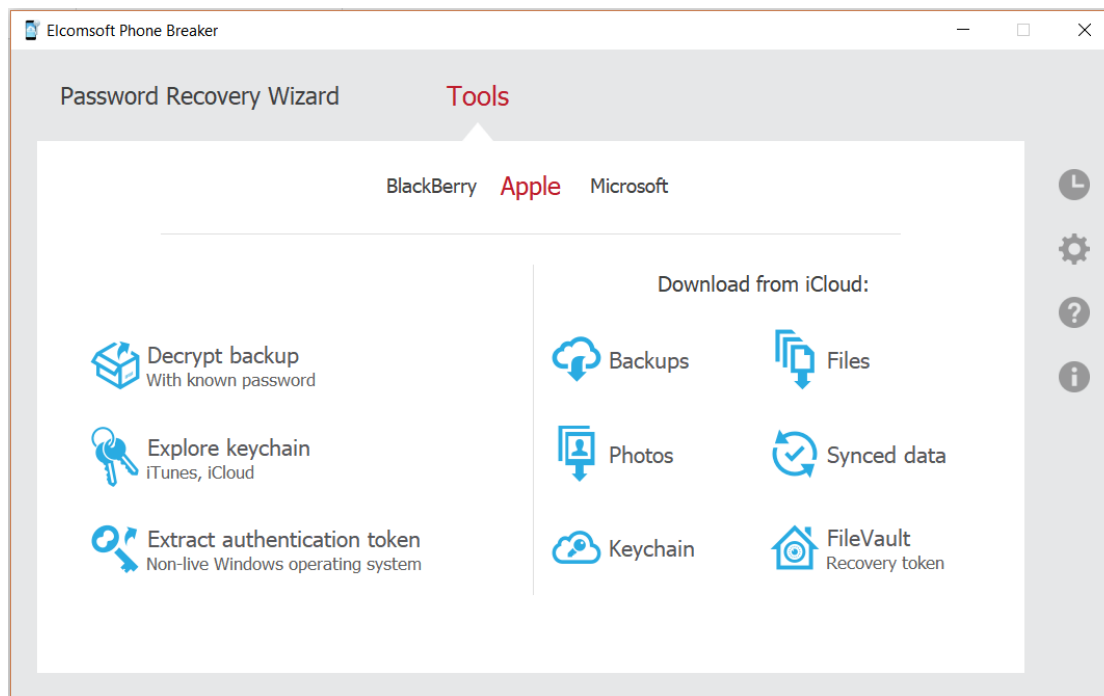


Figure 56. Elcomsoft phone breaker preview

1. Exploring tools: In this we can find a way to get all the keychain passwords stored on the iPhone. The only necessity is that we need to specify a path for the backup. After we go to tools we then go to explore keychain so that we get to know the various saved passwords on the iPhone. Once we click on open keychain, we see the preview as follows:

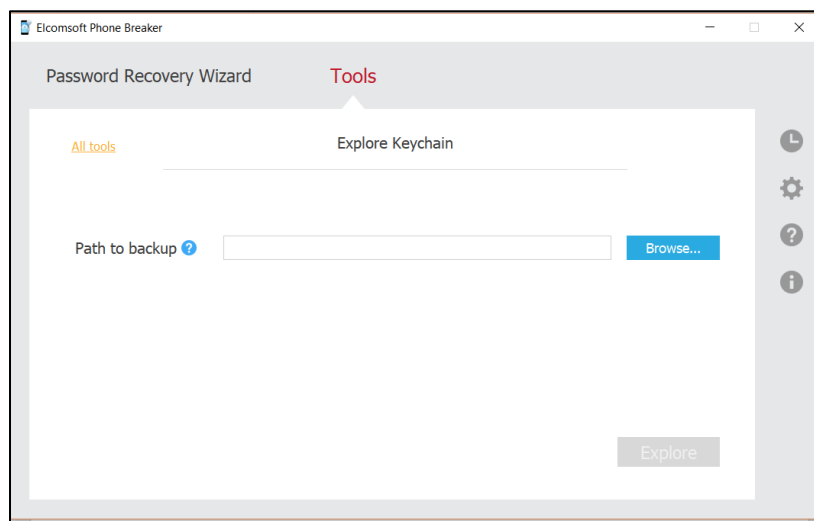


Figure 57. Elcomsoft phone breaker tools.

We can clearly see that we need to specify the path for the backup. Once we have specified it we can see the passwords for various kinds as follows:

Apple IDs (5) Wi-Fi accounts (6) Mail accounts Browser passwords (27) Credit cards DSIDs & Tokens (82)						
Name	Creation date	Modification date	Address	Account	Account	Password
com.intsig.keychain (ISUniq...	2016.11.22 22:36:23	2016.11.22 22:36:23	0://com.intsig.keychain	ISUniqueGlobalDeviceIdentif...		2d*****...
com.intsig.keychain (ISUniq...	2016.11.22 22:36:24	2016.11.22 22:36:24	0://com.intsig.keychain	ISUniqueDeviceIdentifier		0a*****...
rso.stcloudstate.edu (ki134...	2017.05.08 07:27:03	2017.06.19 04:45:41	https://rso.stcloudstate.edu	ki1349kk		\$6*****
rsoconnect.stcloudstate.ed...	2017.05.08 07:27:25	2017.06.19 04:45:41	https://rsoconnect.stclouds...	ki1349kk		\$6*****
huskynet.stcloudstate.edu ...	2017.05.09 16:41:13	2017.06.19 04:45:41	http://huskynet.stcloudstat...	ki1349kk		\$6*****
stcloudstate.ims.mnscu.edu...	2017.05.10 23:53:14	2017.06.19 04:45:57	https://stcloudstate.ims.mn...	ki1349kk		\$6*****
192.168.101.1 (omc_sande...	2017.06.22 03:49:37	2018.08.03 09:38:14	http://192.168.101.1	omc_sandeep		12**
www.services.irctc.co.in (go...	2017.07.06 06:53:12	2017.07.06 06:53:12	https://www.services.irctc.c...	gopicsr		gj****
huskynet.stcloudstate.edu ...	2017.09.13 17:50:25	2017.09.13 17:50:25	https://huskynet.stcloudsta...	ki1349kk		\$6*****
www.linkedin.com (chinhap...	2017.09.15 15:01:17	2017.09.15 15:01:17	https://www.linkedin.com	chinhapatlasandeep95@g...		De*****

Figure 58. Elcomsoft phone breaker passwords.

From the above image we can clearly see that we have passwords saved for Apple ID's, Wi-Fi accounts, browser passwords and DSID's and Tokens. We can clearly investigate each of the accounts so that we can find some evidence in them.

- 2. Exploring Password recovery wizard:** In this process we go through how we can recover passwords using Elcomsoft password breaker. We can perform two types of attacks mainly dictionary attack and brute force attack. Dictionary attack as the name suggests attacks the system by passing words as passwords in the same way how the words are in the dictionary.

Similarly, a brute-force attack is a trial and error method in which we pass in various passphrases until we find a correct match to unlock.

In the below image you can see that I have started attacking the backup file by first doing a Dictionary attack and then a Brute-force attack.

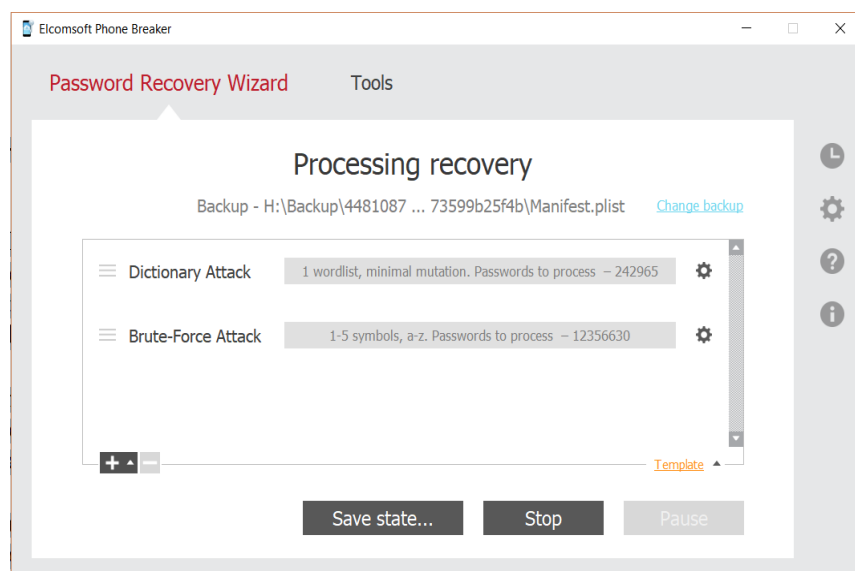


Figure 59. Elcomsoft phone breaker password recovery wizard.

After performing this process, we finally get the password for the iTunes backup. This process takes a whole lot of time and processor utilization.

3. **iFunBox.** First, we open iFunBox and we can see the preview below. We clearly see that we can see the product model along with the serial number and phone number.



Figure 60. iFunbox preview.

1. **Checking for photos:** On the left panel we have an icon which contains a folder named photos. When we click on it, we get all the photos in chronological order.

We can see it as follows:

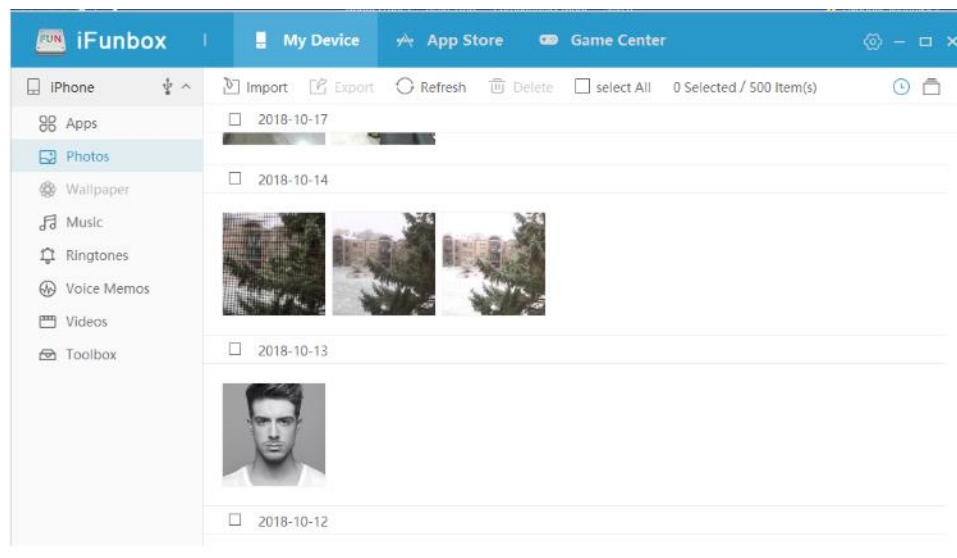


Figure 61. iFunbox photos.

2. Checking for applications: Now with the help of iFunBox we can also see what all the applications the user has installed. As these might also play a key evidence in performing forensics. Here is the image which shows all the applications that the user has installed on the phone.

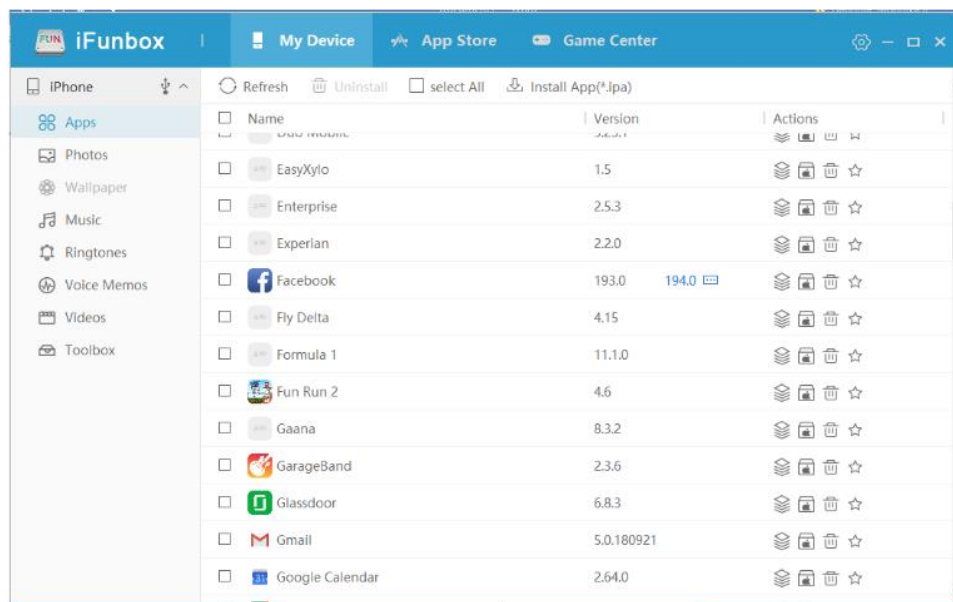


Figure 62. iFunbox applications view.

iFunBox also has a special feature called toolkit which consists of various options such as we can use the phone as a general storage too. The main key thing we need to identify is the “User file system”. It acts as a file explorer so that we can dive in deep and look for all the files stored in the iPhone storage.

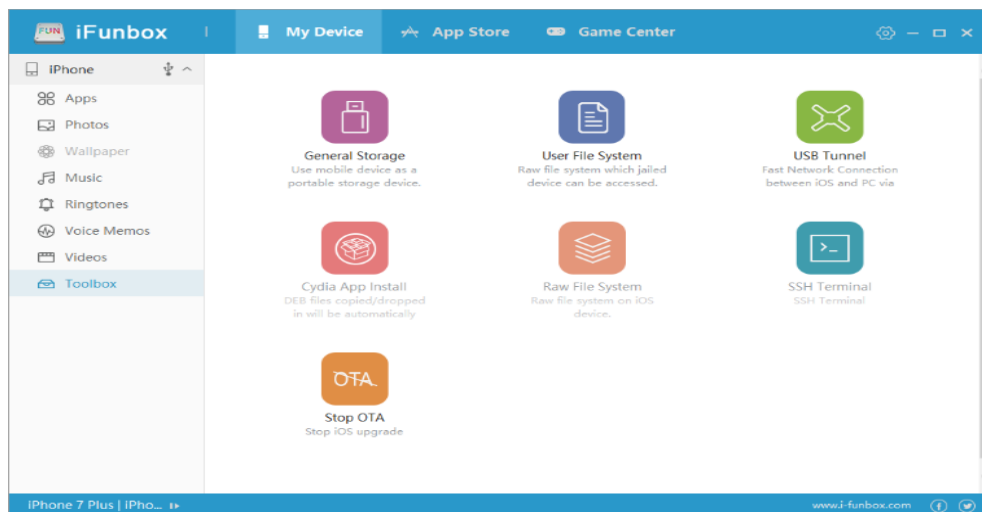


Figure 63. iFunbox toolbox.

Now if we go inside the user file system, we can see the DCIM folder which contains all the photos which are stored in folder based on the time when they were clicked in the system. We can see the preview of it as follows:

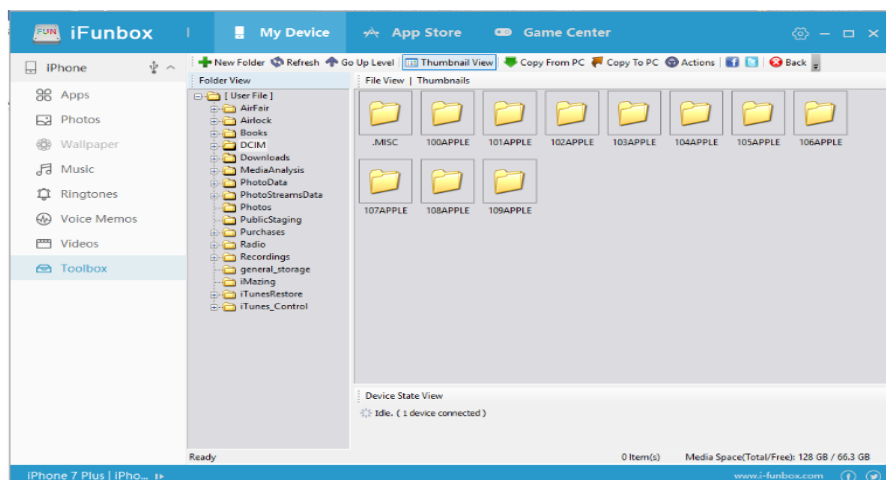


Figure 64. iFunbox toolbox view.

If we open any of this folder, we can see the images lined as follows:

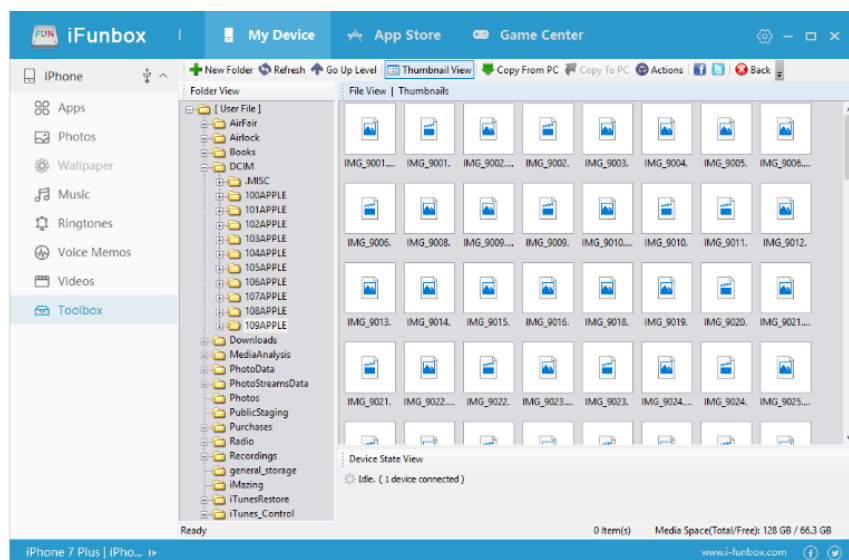


Figure 65. iFunbox toolbox insight view.

Acquisition via physical methods. First, we open iOS forensic kit which is downloaded from Elcomsoft website. We can see the preview of it as follows:

```

C:\WINDOWS\system32\cmd.exe

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 3.0/Win

(c) 2011-2018 Elcomsoft Co. Ltd.

Please select an action:
I DEVICE INFO - Get basic device information
B BACKUP - Create iTunes-style backup of the device
M MEDIA - Copy media files from the device
S SHARED - Copy shared files of the installed applications

1 ENTER DFU - Help putting device into DFU mode
2 LOAD RAMDISK - Load tools onto the device
3 GET PASSCODE - Recover device passcode
4 GET KEYS - Extract device keys and keychain data
5 DECRYPT KEYCHAIN
6 IMAGE DISK - Acquire physical image of the device filesystem
7 DECRYPT DISK
8 TAR FILES - Acquire user's files from the device as a tarball
9 REBOOT - Reboot the device

0 EXIT

>:

```

Figure 66. Elcomsoft iOS forensic toolkit preview.

This toolkit has various options that we can perform on a device. This tool helps a lot in performing physical acquisition as this has all the key features that are required by a forensic investigator.

Now let's begin the physical acquisition of iPhone. For this experiment I am going to use an iPhone SE which runs on iOS 10.3.3



Figure 67. iOS version.

Now let's connect the phone to the laptop using a USB cable as follows:

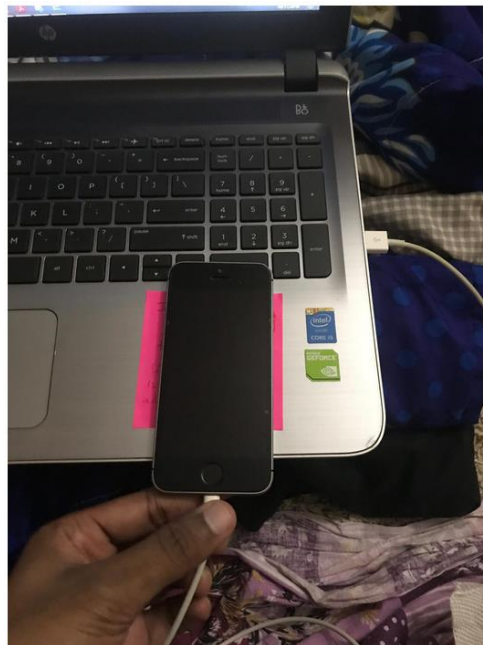


Figure 68. iPhone connected to laptop.

Now from the Elcomsoft iOS forensic toolkit command line lets perform the physical acquisition. But for acquiring the image we need to first turn the phone off and put the phone in DFU mode. For entering the DFU mode we first hold down both the home button and lock button and then after 8 seconds we release the lock button while continuing to hold the home button. We can see the preview as follows:



Figure 69. iPhone DFU mode

Then we open the Elcomsoft command line and from the set of commands we need to give number 6 as input and press enter to extract the image from the iPhone. We can see it as follows:

```

Please select an action:
I DEVICE INFO      - Get basic device information
B BACKUP           - Create iTunes-style backup of the device
M MEDIA           - Copy media files from the device
S SHARED          - Copy shared files of the installed applications

1 ENTER DFU       - Help putting device into DFU mode
2 LOAD RAMDISK    - Load tools onto the device
3 GET PASSCODE    - Recover device passcode
4 GET KEYS        - Extract device keys and keychain data
5 DECRYPT KEYCHAIN
6 IMAGE DISK      - Acquire physical image of the device filesystem
7 DECRYPT DISK
8 TAR FILES       - Acquire user's files from the device as a tarball
9 REBOOT          - Reboot the device

0 EXIT

```

Figure 70. Kit preview.

Then it asks for the partition for creating image and we select the appropriate partition that is User. We see the screenshot as follows:

```

Please note that to obtain device disk image you need to load ramdisk
on the iOS device first. If you haven't done this yet, please return
to previous step and use corresponding menu item.

Please select partition to image:
 1 System (rdisk0s1s1) -- this one is NOT ENCRYPTED
 2 User (rdisk0s1s2) -- this one is ENCRYPTED

 0 Back

>: 2

```

Figure 71. Partition selection.

This process usually takes a lot of time and we can see that the imaging has been done.

```

>: 2
Save image to file <user.dmg>: userfiles.dmg

rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

28,958M
0+926506 records in
0+926506 records out
28958+1 records in
28958+1 records out
30365065216 bytes (30 GB) copied, 5019.23 s, 6.0 MB/s

Imaging done.

Press 'Enter' to continue

```

Figure 72. Image completion.

Analysis on Physical image acquired: Now we go into the folder where the physical image is stored. We need to analyze it using FTK imager.

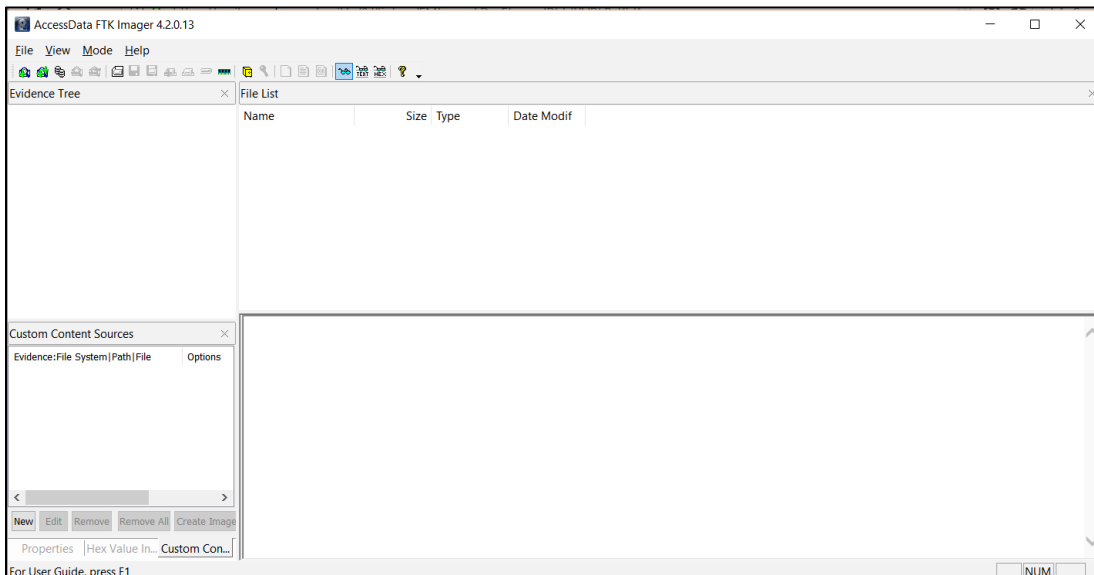


Figure 73. FTK imager preview.

Then we go to file and click on add evidence and we select the image file as follows:

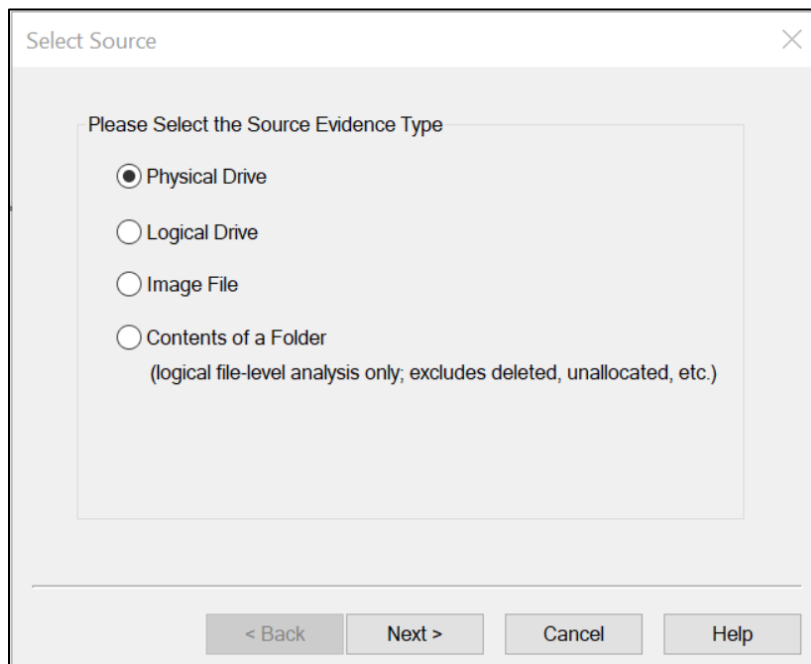


Figure 74. Evidence type selection.

Then we open the image file from the folder as follows:

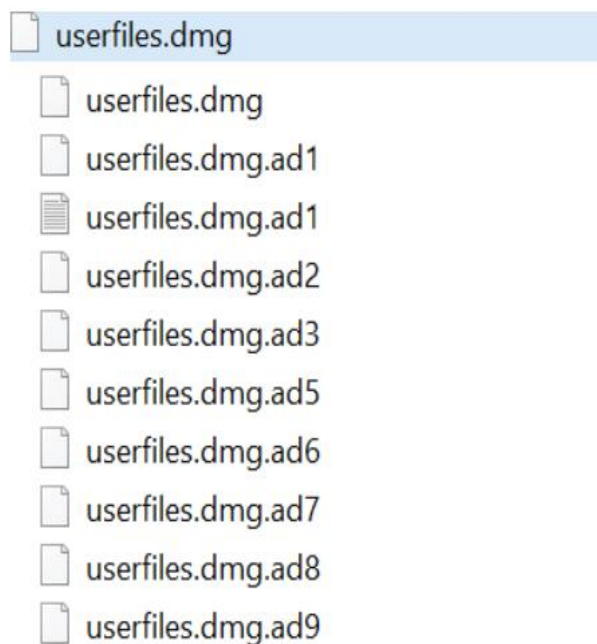


Figure 75. Image files.

Now we go to the left-side panel and try to analyze it using hex editor as follows:

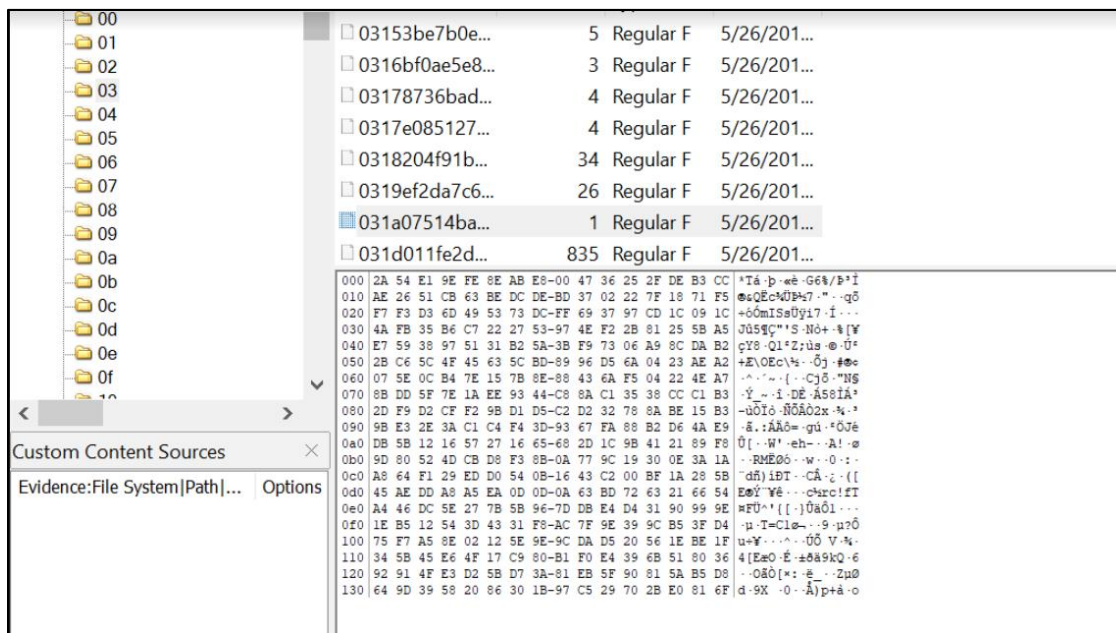


Figure 76. Hex viewer.

Now we see some of the hex format as follows:

10 7F 2F 76 61 72 2F 63 6F 6E 74 61 69 6E 65 72	../var/container
73 2F 42 75 6E 64 6C 65 2F 41 70 70 6C 69 63 61	s/Bundle/Applica
74 69 6F 6E 2F 36 34 31 31 43 31 35 31 2D 45 31	tion/6411C151-E1
37 43 2D 34 45 41 41 2D 39 37 37 33 2D 46 38 39	7C-4EAA-9773-F89
36 31 45 43 31 41 42 30 43 2F 46 61 63 65 62 6F	61EC1AB0C/Facebo
6F 6B 2E 61 70 70 2F 50 6C 75 67 49 6E 73 2F 4E	ok.app/PlugIns/N
6F 74 69 66 69 63 61 74 69 6F 6E 53 65 72 76 69	otificationServi
63 65 45 78 74 65 6E 73 69 6F 6E 2E 61 70 70 65	ceExtension.appe
31 31 5F 10 5D 2F 76 61 72 2F 63 6F 6E 74 61 69	11_./var/contai
6E 65 72 73 2F 42 75 6E 64 6C 65 2F 41 70 70 6C	ners/Bundle/Appl
69 63 61 74 69 6F 6E 2F 36 32 32 36 30 43 39 30	ication/62260C90
2D 34 43 43 44 2D 34 31 36 46 2D 38 41 42 34 2D	-4CCD-416F-8AB4-
46 39 37 46 41 41 30 35 30 31 33 46 2F 44 69 73	F97FAA05013F/Dis
63 6F 76 65 72 46 69 6E 61 6E 63 69 61 6C 2E 61	coverFinancial.a
63 6B 75 70 4B 65 79 42 61 67 57 56 65 72 73 69	ckupKeyBagWVersi
6F 6E 54 44 61 74 65 5F 10 14 53 79 73 74 65 6D	onTDate ..System
44 6F 6D 61 69 6E 73 56 65 72 73 69 6F 6E 5B 4D	DomainsVersion[M
61 6E 69 66 65 73 74 4B 65 79 5E 57 61 73 50 61	anifestKey^WasPa
73 73 63 6F 64 65 53 65 74 58 4C 6F 63 6B 64 6F	sscodeSetXLockdo
77 6E 5C 41 70 70 6C 69 63 61 74 69 6F 6E 73 5B	wn\Applications[
49 73 45 6E 63 72 79 70 74 65 64 4F 11 05 6C 56	IsEncryptedO..lv

Figure 77. Hex code inspection.

We clearly see the highlighted text as the Passcode set lockdown and application is encrypted. In this way we can analyze a whole lot of hex codes and try to get much information as possible which helps in gathering a lot of key information.

Acquisition via jail breaking. As Apple made security tightened over the years it has become difficult to perform jailbreaking. I have tried a method to perform jailbreak and it was partially successful. The way I performed is using Pangu and I did it virtually on an iPhone running iOS 12 beta 4. We see the details as follows:

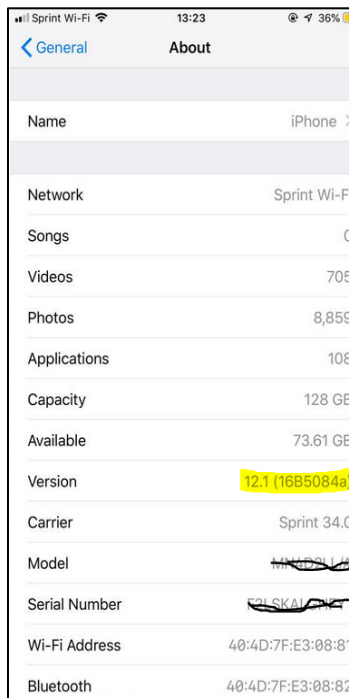


Figure 78. iOS version inspection.

Steps for jailbreaking:

1. First, we visit pangu8.com in the Safari browser on the iPhone and click on iOS 12.1.

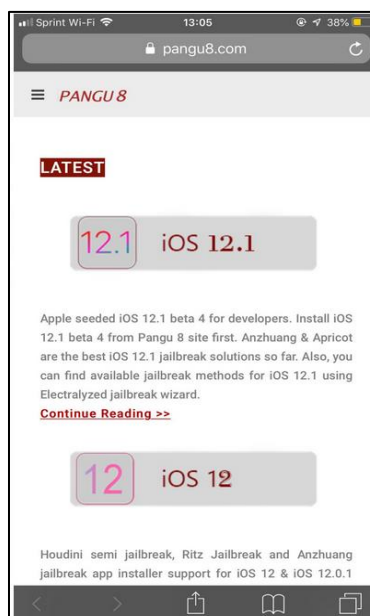


Figure 79. Pangu website.

2. After that we click on Electralyzed jailbreak wizard

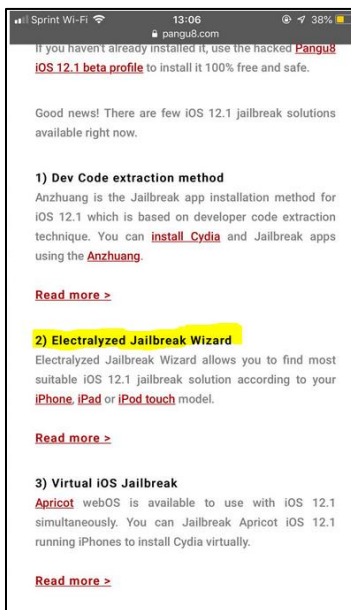


Figure 80. Electralyzed jailbreak wizard.

3. Then we choose the model and the iOS version the iPhone is running on.

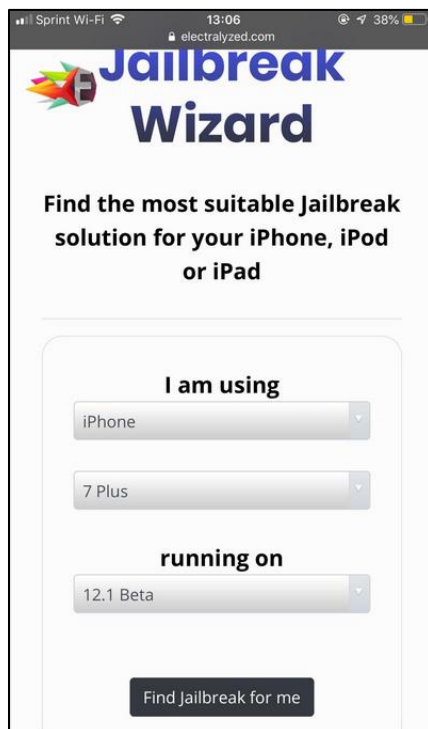


Figure 81. Jailbreak wizard.

4. Then we click on Anzhuang for further process as:

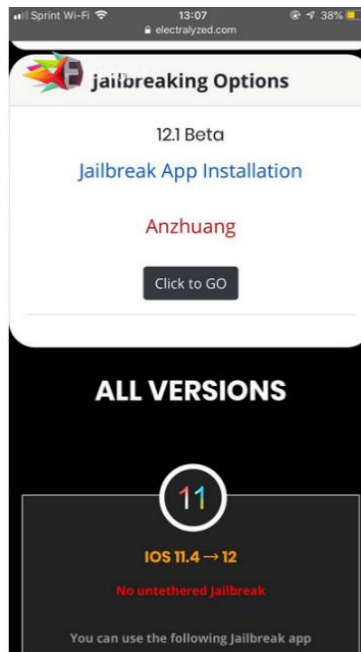


Figure 82. Jailbreak options.

5. We can see the brief description about Anzhuang as follows:

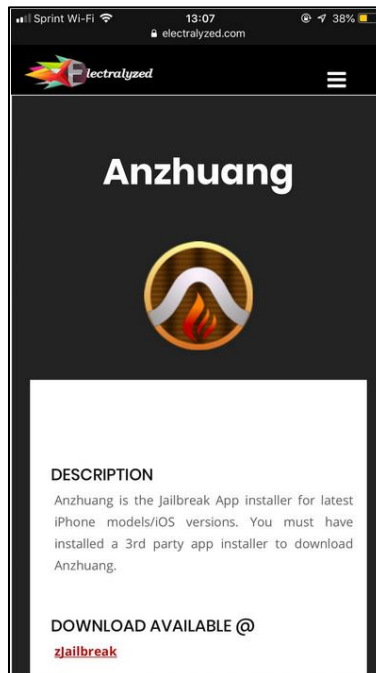


Figure 83. Jailbreak description.

6. Then we click on Install now and we see the screens as follows:

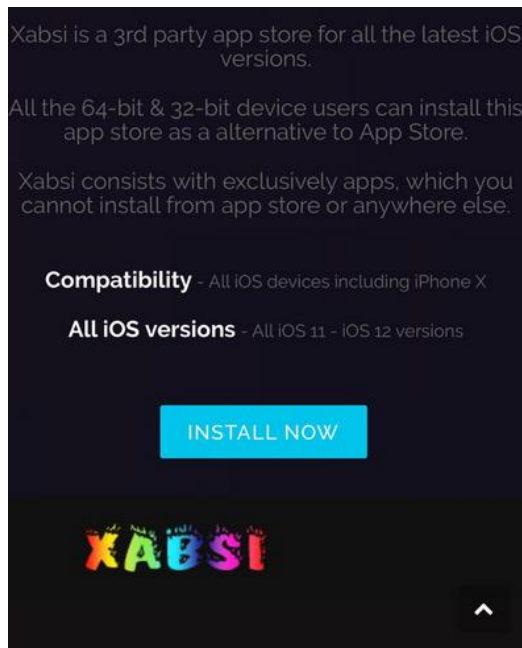


Figure 84. Installation compatibility.

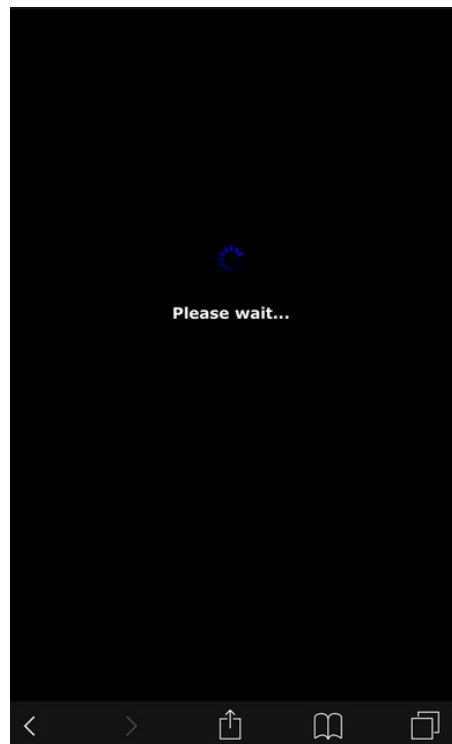


Figure 85. Installation step for pangu

7. Then we get a popup which asks for permission to install profile and we need to click on allow so that the profile gets installed. We can see the screenshot as follows:

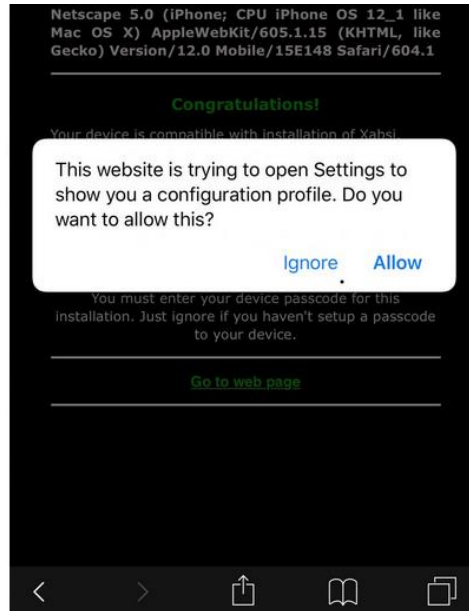


Figure 86. Installation popup.

8. After that we are taken to the settings folder where we need to install the profile and we can see the preview of it as follows:

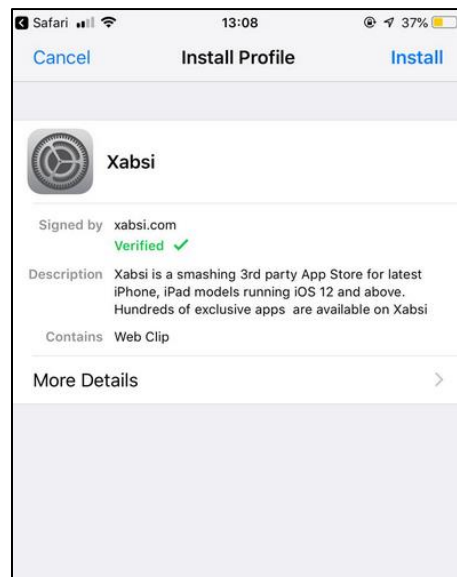


Figure 87. Profile view.

9. Once the profile is installed, we need to restart the phone and once we turn the phone on the phone will be jailbroken.
10. We can see the preview of the app after the device is turned on as follows:

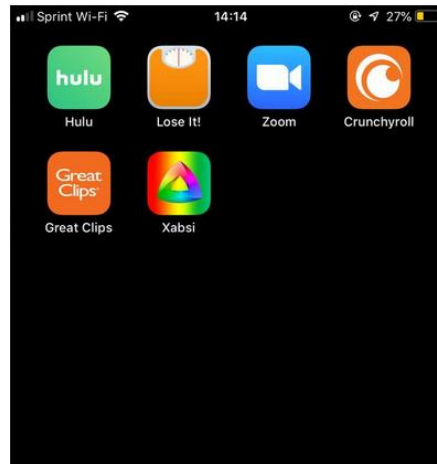


Figure 88. Launchpad view.

11. Once we open the app, we can see the preview as follows:



Figure 89. App view.

The only disadvantage is that we can install third party apps and make some tweaks but there is no way that we can retrieve data or fetch out data for performing forensics.

Summary

In this chapter we have discussed, how we can acquire data using various types of acquisitions on an iPhone. There are both advantages and disadvantages for each method. Out of all the methods logical acquisition is the one which is the best because we can explore all the information that is contained on the device. The tools that are available in the market are also brilliant for performing logical acquisition and are mostly open-source and free to use.

Chapter V: Results, Conclusion, and Recommendations

Introduction

In this chapter we will discuss the results obtained by performing various types of acquisitions. We also compare which method gives us accurate and clear information when used and which is the best method to perform forensic analysis. There might be a variance in the data retrieved by performing various types of analysis, but we need to check which one fetches out data efficiently.

Results

For this project I have used two iPhones one running on iOS 12.1 and the other running on iOS 10.3.3. I have first performed the analysis on iTunes backup and found several key evidences which are crucial in determining key information.

In the later step we have seen how to perform logical acquisition and we have seen how we used three various tools as iPhone Explorer, Elcomsoft Phone breaker and iFunBox. All these tools were successful in fetching out useful data and each had its own advantages and user interface.

Coming to the next step we have performed physical acquisition and for this we have used Elcomsoft iOS forensic toolkit. We were successful in extracting the image of the iPhone and exploring it using FTK imager to fetch out the data.

In the last step we have performed jailbreaking and we were partially successful in doing it. Jailbreaking has its own limitations and because of frequent software updates and enhancement of security from Apple it has become difficult to investigate the data.

Now let's look whether we have accomplished in overcoming the problem statement. The questions we had in the problem statement are as follows:

1. How do we perform a forensic analysis on an iPhone?

We have used mainly four methods to accomplish this process. They are acquisition using iTunes backup, logical acquisition, physical acquisition and jailbreaking an iPhone.

2. Which tools to use to perform the forensic analysis?

For each and every process of acquisition I have used various tools such iPhone Explorer, Elcomsoft Phone breaker, iFunBox, Elcomsoft iOS forensic toolkit.

3. What is the information that we need to examine?

The key sources of information that is valuable for forensic analysis are messages, safari history, call history, photos and contacts. If there is application information and geo location information, it would also play a vital role.

4. How many various methods can be applied to perform the analysis?

There are majorly four various methods to perform analysis.

5. How many types of approaches yield the same result?

Based on my research almost all approaches yield the same result. But logical acquisition had much detailed information than all the other approaches.

6. How effective will the approaches be?

Every approach has its own uniqueness and interface. We cannot say which one is more effective because it depends on the data and the situation where we perform the analysis.

Conclusion

All the approaches yield almost the same result. We have performed the research in four ways namely acquisition via iTunes backup, logical acquisition, physical acquisition and jailbreaking. Every approach had its own difficulties and the results yielded were different slightly. But some approaches were somewhat more efficient than the other approaches.

We got to know some of the issues faced during the jailbreaking process and how some new versions of iOS do not support jailbreaking. Out of all the approaches that we have done in performing forensic analysis logical acquisition gave us a whole lot of information more than other types of acquisition.

Mainly iPhone Explorer stood among all the tools in fetching out the data. It gave us deep and clear insights of the user data and had an easy user interface in doing so.

Based on all the results yielded it depends on situation in which we are performing forensics. If we have a passcode with us, then logical acquisition is the best way to go because we will have a whole lot of deep insight in the user information. On the other hand, if we do not have a passcode then we need to break it, and this circumstances mostly physical acquisition plays a major role.

Future Work

With this experiment we have understood how we can access and perform forensics on an iPhone. We learnt about various tools that can be used to perform forensics too. As faceID is now become a part of iPhones the next difficult task for forensic investigators is to unlock the iPhones with faceID's. Apart from this as new iOS versions release every year and new security enhancements are made, I would love to extend my research on how to bypass faceID and perform various types of acquisition.

References

- Apple*. (n.d.). Retrieved from File system. https://developer.apple.com/library/content/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html#//apple_ref/doc/uid/TP40010672-CH2-SW2.
- Apple business*. (n.d.). Retrieved from iOS security guide. https://www.apple.com/business/docs/iOS_Security_Guide.pdf.
- Apple library*. (n.d.). Retrieved from plist. <https://developer.apple.com/legacy/library/documentation/Darwin/Reference/ManPages/man5/plist.5.html>.
- Blackbagtech*. (n.d.). Retrieved from mobilyze. <https://www.blackbagtech.com/mobilyze.html>.
- Digital forensics*. (n.d.). Retrieved from Wikipedia. https://en.wikipedia.org/wiki/Digital_forensics.
- Elcomsoft*. (n.d.). Retrieved from. <https://www.elcomsoft.com/eppb.html>.
- Engman, M. (2013). *Forensic Investigations of Apple's iPhone*. Retrieved from. <https://www.diva-portal.org/smash/get/diva2:651693/fulltext01.pdf>.
- Handling iOS encryption in a forensic investigation*. (2011, July 19). Retrieved from UniversityVanAmsterdam. <http://www.delaat.net/rp/2010-2011/p26/report.pdf>.
- iFunbox*. (n.d.). Retrieved from. <http://www.i-funbox.com/>.
- iFunBox*. (n.d.). Retrieved from userchoose. <http://www.i-funbox.com/index.html?userchoose>.
- Interworks*. (2016, February 5). Retrieved from. What is digital forensics?: <https://www.interworks.com/blog/bstephens/2016/02/05/what-digital-forensics>.
- Katana forensics*. (n.d.). Retrieved from lantern. <https://katanaforensics.com/lantern.php>.
- Macroplant*. (n.d.). Retrieved from iExplorer. <https://macroplant.com/iexplorer>.
- Mallepally, R. (n.d.). Retrieved from. <http://sci.tamucc.edu/~cams/projects/371.pdf>.

Merriam Webster. (n.d.). Retrieved from. <https://www.merriam-webster.com/dictionary/forensic>.

Morrissey, S. (2011). *Wordpress*. Retrieved from iOS forensic analysis. <https://sensperiodit.files.wordpress.com/2011/04/ios-forensic-analysis-for-iphone-ipad-and-ipod-touch.pdf>.

National institute of standards and technology. (n.d.). Retrieved from. <https://www.nist.gov/document/sample-chain-custody-formdoc>.

Proffit, T. (2012, November 5). *San's Institute InfoSec reading room*. Retrieved from Forensic Analysis on iOS devices. <https://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092>.

Sourceforge. (n.d.). Retrieved from iPhone analyzer. <https://sourceforge.net/projects/iphoneanalyzer/>.

Tech republic. (n.d.). Retrieved from Filesystem comparison. <https://www.techrepublic.com/article/apfs-vs-hfs-which-apple-filesystem-is-better/>.

The Mercury news. (n.d.). Retrieved from All iPhone predecessors. <https://www.mercurynews.com/2017/09/13/slideshow-how-apples-new-iphones-stack-up-against-their-predecessors/>.

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

Wikipedia. (n.d.). Retrieved from Statistics of iPhone. <https://en.wikipedia.org/wiki/IPhone>.

Wikipedia. (n.d.). Retrieved from Smartphone. <https://en.wikipedia.org/wiki/Smartphone>.

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

Wikipedia. (n.d.). Retrieved from iOS. <https://en.wikipedia.org/wiki/IOS>.

Wikipedia. (n.d.). Retrieved from Encryption. <https://en.wikipedia.org/wiki/Encryption>.

Wikipedia. (n.d.). Retrieved from Chain of custody. https://en.wikipedia.org/wiki/Chain_of_custody.

Wikipedia. (n.d.). Retrieved from iOS jailbreaking. <https://en.wikipedia.org/wiki/>

IOS_jailbreaking.

Wikipedia. (n.d.). Retrieved from iOS jailbreaking. <https://en.wikipedia.org/wiki/>

IOS_jailbreaking.

Wikipedia. (n.d.). Retrieved from Forensic tool kit. <https://en.wikipedia.org/wiki/>

Forensic_Toolkit.