12-2019

The Apple of the World: Extracting Evidential Data through IPhone

Rakesh mangalamapalli
rakesh.mangalampalli@gmail.com

“The Apple of the World’s Eye”: Retrieving Data from iPhone using Various Methods

by

Rakesh Mangalampalli

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

December, 2019

Starred Paper Committee:
Mark Schmidt, Chairperson
Lynn Collen
Sohn Changsoo

Abstract

The data storage system has changed timely manner. As we have been seeing in the past data used to be saved in hard drives, solid state drives and computers. It used to be easy to retrieve data from those drives, but it was very difficult to maintain them as they had very small storage space and it was very difficult to carry them. Smartphones have been introduced in the recent past and they have over crossed old devices as they are fast in the process and have multiple features when compared to computers. Apple has introduced most powerful smartphones called Apple iPhones in 2007.

iPhone forensics is used to acquire data from iPhones like images, text messages, contacts and call library. I would be using iPhone for my forensics investigation. In my further investigation process, I would be extracting data using various methods. Apple has built its own software called iTunes which is used to save and protect its data security. iTunes software has been licensed and provided by Apple.inc. To connect iPhone we need a lightning cable. We would also be using Dell laptop for our forensic investigation.

As per my research on various methods to extract data from iPhone. I have come across a number of software applications but from which I would like to use iTunes and iMyfone D-Port software applications in my starred paper.

Figure 1: Apple iPhone5, front side.

Figure 1.1: Apple iPhone5, back side.

Acknowledgements

I thank professor Mark Schmidt for giving me an opportunity to write starred paper on iPhone Forensics under his guidance. I also thank my committee members Professor Sohn Changsoo and Professor Lynn Collen for accepting my invite and joining with me on my starred paper.

Table of Contents

Chapter Page

List of Table

List of Figures

Figure Page

Figure Page

Figure Page

Chapter 1: Introduction

Introduction

According to my research on the cellphone industry, Apple iPhone is the most commonly used smartphones in today's digital world. Apple.inc was been established by Steve Paul Jobs. Apple not only produces cellphones it also produces iPods, iPads, Mac book Computers and it recently started to produce Apple smartwatches. Apple has not restricted itself to hardware devices (Apple-iPhones, 2018). They have created software's like iTunes and iPhone Operating Systems (iOS) as these phones perform N number of futures at a reasonable price. Due to the appropriate cost and futures on these phones, people are showing more interest towards buying these phones. Forensics on iPhones has become more important in the recent years.

In today's world iPhones are nothing less than a small satellite. There are is some valuable information stored in smartphones like Media (photos, video) Text messages (SMS, MMS), Contacts and Call library (favorite contacts, recent, voice Mails,). In addition to it we cannot just copy data from the iPhone as the data is encrypted and the IOS would not allow us to use any application that is not been in contract with Apple. Innovation of iPhones and tablets is progressing at a Fast Pace. With every new iPhone that has been released Apple has introduced some new advancement.

In the recent past forensics on iPhone has become more popular as each and every person is using iPhone. I believe that if we are able to retrieve images, text messages, and contacts and call history from iPhone through iPhone forensics, then we would be able to catch hold of criminals and put them the behind bars. There are many tools and technologies for iPhone forensics like iPhone backup extractor, iMyFone D-port, iPhone transfer recovery and many

more. If these software's help forensics experts in recovering data from iPhone than many innocent people can be saved from false legalization (imyfone-Backup Application, 2018).

Problem Statement

One of the primary reasons, why everyone are interested to buy Apple iPhone is because of its "Data Security and Data Intelligence". Apple tries to improve its security on a day to day bases and closing all its loop holes. In this process of closing its loop holes Apple is improving its software as well as hardware, this improvisation has become a big issue to the forensics investigators as they need to keep updating their forensics software's and hardware's to examine Apple devices.

- How are we applying forensics on Apple iPhone?
- What data needs to needs to be extracted?
- What are the Tools and Technology need to perform Forensics on iPhone?
- What are the Challenges faced by forensics investigators while examining iPhone?
- What are problems faced while retrieving data from iPhone?

Nature and Significance of the Problem

Tools and technology used to examine Apple iPhone needs to updated on the bases of Apple updates, Apple updates its software for every 6 months and also sometime for every 3 months as well. This updating of software is to fix bugs in software and add more features to growing software.

This makes it difficult to the forensics investigators to examine Apple iPhone, as they need to update their software whenever there is an update on Apple's software. This one of the biggest challenges faced by forensics team.

Objectives of the Project

The objective of this study is to understand the challenges faced by forensics investigators while performing iPhone forensics. In this procedure I would provide the different methods used to extract data from data from iPhone. Extraction data from iPhone would be very useful method to forensics investigators. This study will also compare various data extracted by various software applications.

Study Questions

The study of questions may contain questions as to what the challenges are faced by forensics investigators while examining an iPhone for evidence. What data has to be extracted? Where should we search for evidence? How data needs to be extracted? What are the different methods to recover data? How extracted data needs to be segregated? Where should the evidence need to be kept? And how should they be protected from destroying?

Limitations of the Study

The main objective of this paper is to study how different applications help in collecting data from iPhones. This study does not make any kind of changes to the methods of examining data or extracting data, but this study helps in understanding the limitations of these methods. It then relates to current methods of recovering data from iPhones and helps for future works.

Definition of Terms

Apple iPhone: The revolutionary smartphones introduced to make human life easy are called as Apple iPhone. These smartphones have been released by Steve Paul Jobs in the year 2007.

Software Application: Software applications are nothing but a path or mode of importing and exporting date form devices. They also provide security and store different kinds of data.

iPhone Forensics: Examining iPhone to recover data such as Photos, Text Messages, Contacts and Call History is called as iPhone Forensics. Usage of iPhone has increased rapidly in recent years and due to which forensics on Apple iPhone has also increased.

iTunes: iTunes is a software developed by Apple. It is used to store data like music, App's, personal information, etc.

iMyFone D-Port: iMyFone D-Port is third-party application that I would be in my further study to extract data from iPhone.

Summary

In Chapter 1 we have learned what is iPhone and why have they become so popular in recent years, also we have seen what products are being released by Apple. We have learned what are different kinds of data that is been stored in iPhone and what methods are we going to use in future to extract data. What are the problems faced by forensics officers while examining iPhone? We have discussed limitations and objectives of this study. Definitions for better understanding about the hardware and software tools used in our study.

Chapter 2: Background of iPhones and its Literature Review

Introduction

Forensics investigators resolve most of the cases by collecting proofs from computers and laptops. As in the recent year's usage of smartphones have increased and nobody wants to save their data in computers or laptops. Smartphones provide as much as speed and storage space as a computer. So everyone is showing more interest towards cell phones. Smartphones like iPhone have not only developed its hardware as well as its software.

Background Problems

Apple released its first iPhone in the year 2007 and since then it has been improvising its hardware and software according to the growing technology. Apple uses Copper, Cobalt and Lithium metals for creating its hardware and for the front screen it uses Dragon glass which is strong and touch sensitive. When is come to the software development, Apple releases two software updates every year? The current software update that’s running in apple iPhone is IOS 12.1.4 Forensics investigators while examining an apple iPhone its will be very difficult for them to find out on which software version is the phone running on and its hardware is also so hard that it makes difficult for them to explore the iPhone. As apple improves its software every six months its becomes difficult for the forensic investigators to develop their technology according to the new software. Forensics investigators must develop a new software or make changes according to the new upgraded software (Phone.html, 2018).

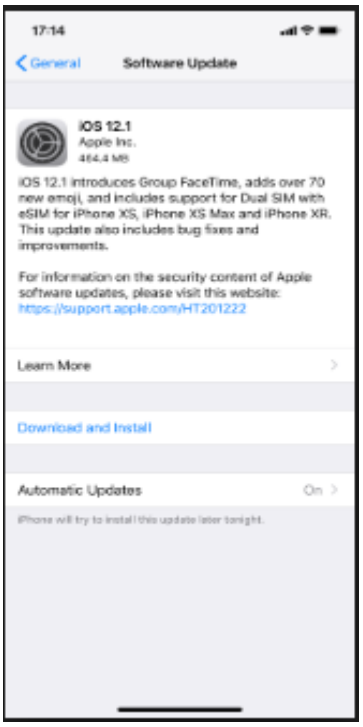


Figure 2: iOS software.

Figure 2.1: iPhone hardware.

Literature Related to Problem

Forensics. Forensics is the method of studying of criminal evidence. The forensic details are then handed over to the court of law as to take its decision on the crime incident. To deliver a consistent evidence, it involves three steps. The first one is Chain of Custody, Admissibility of test, testimony, Export witness and many more (Digital forensics.com, 2018).

iPhone forensics. Utilizing logical methodologies for recovering information from mobile phone (iPhone) for legitimate purposes. Mobile phone investigation is a branch of computerized forensics recognized with the recovery of advanced confirmations from cell phones. The main principle for forensic examination of digital evidence is that the original evidence must not be modified (Digital forensics.com, 2018).

NAND flash memory. NAND flash memory is used to store data in iPhone. NAND flash memory contains floating gate transistor. it is developed to decrease the cost per bit to improve memory chip capacity to its best. The very good advantage of this memory is that it does not require power to restore data. NAND flash memory can sustain a large import and export of data (Ttechtarget-NAND flash memory , 2018).

Digital Forensics Procedure Analysis

The procedure of digital forensics can be explained in six different stages (Digital forensics, 2018), explained below:

Identification. This is the first stage to start Forensics process starts by Identify where crime seen has occurred and look around the surroundings of the crime act for an evidence.

Collection. The next stage is the collect all the evidences from the crime location. This is very crucial stage because most of cases of forensics depend on collection of evidences.

Preservation. Preserving is also one of the most important stage in Forensics, as the evidences collected are very sensitive like Hair, Peace of cloth, Blood samples. They are very delicate evidences that give very crucial proof of crime.

Examination. This is the fourth stage, once all the evidences are preserved at a secured location. Examination of those evidences would begin, Each and every evidence will be reviewed very carefully without damaging any of the evidences.

Analysis. After the examination has been completed, in this stage analysis of examined evidence would be conducted and record is created according to it.

Presentation. This is the last and final stage where all the evidences and report that has been created according to the analysis is been presented in front of the court for decision.

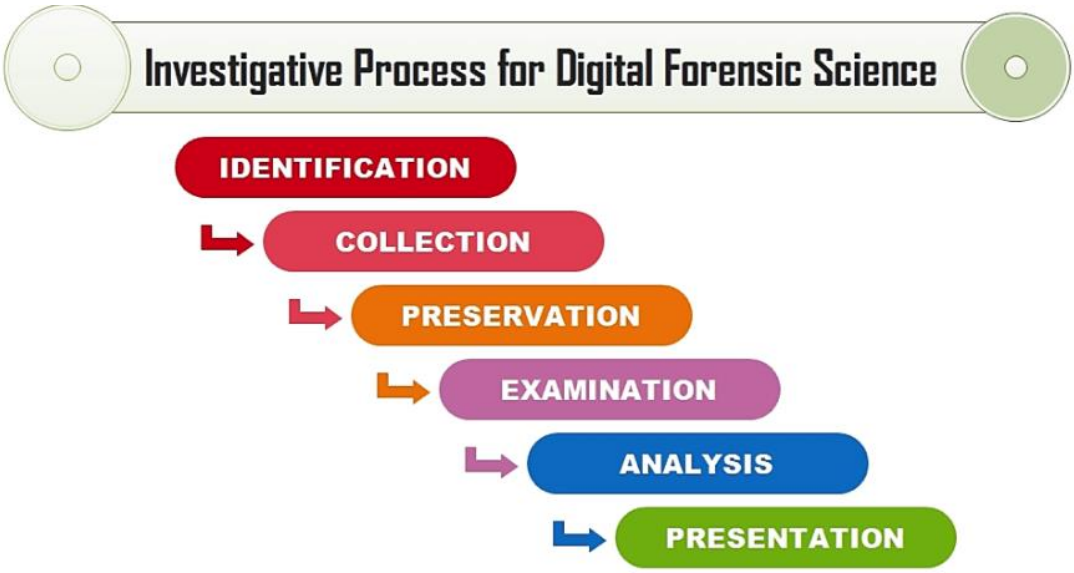


Figure 3: Digital forensic procedure.

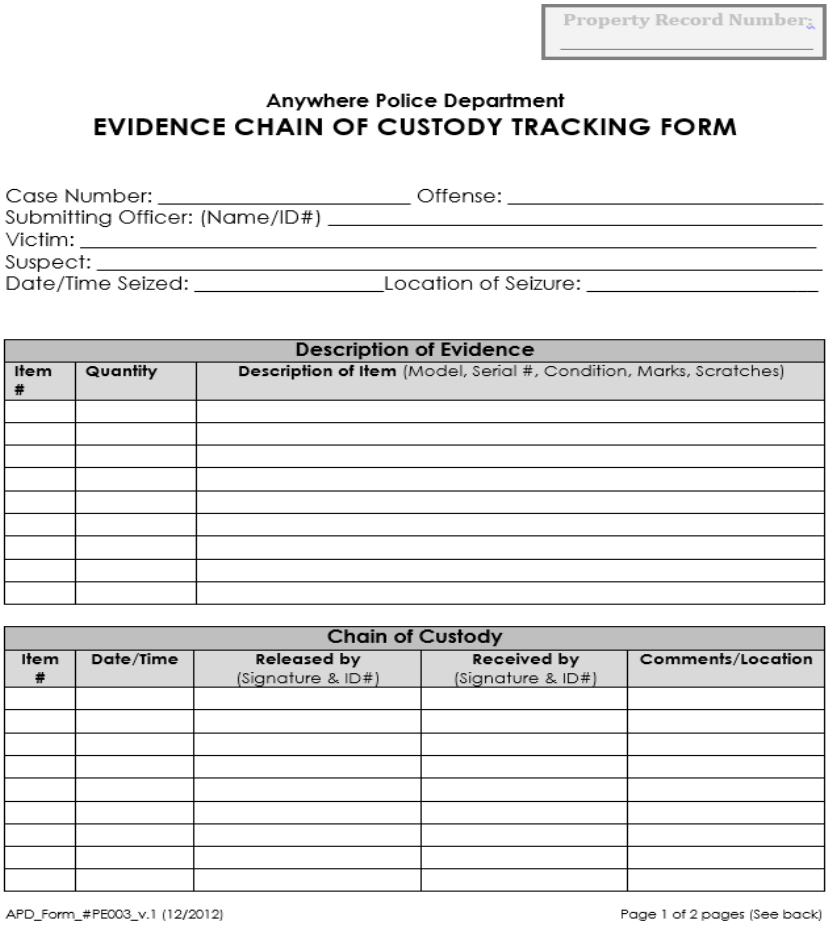
The portable legal sciences process is divided into three fundamental classifications which are Hardware, Software, Knowledge and tools / technology (Kandidatuppsats, 2013).

- Hardware. Hardware is the important tool in iPhone forensics. If we do not have hardware devices like iPhone, Computer, Cable and forensics tools, then it would not be possible to perform forensics on iPhone (Kandidatuppsats, 2013).
- Software. Software is the second most important requirement for forensics. Software is necessary for any kind of forensics. Some software's are developed in such a way that they can handle a board of data and some other software's are designed to perform particular tasks (Kandidatuppsats, 2013).
- Knowledge. As we have hardware and software, the individual should also have the knowledge to use not only hardware but also software as well. It is also necessary to have the technic to perform forensics.

- Technology/Tools. Forensics implementation procedure is completely depended on the tools and technology, in today's world technology is changing every day and every month, Digital forensics investigators also need to improve their tools and technology for investigation (Kandidatuppsats, 2013).

Literature Review Related to the Methodology

Chain of custody. Chain of Custody is a procedure that used for tracking evidences. To follow this procedure there is (below images) form that is maintained by forensics investigators. This tracking procedure keeps the evidences intact and any examinations made to the evidences will be recorded into the chain of custody.



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**

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

Figure 4: Chain of custody.

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

Authorization for Disposal

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)
☐ Return to Owner ☐ Auction/Destroy/Divert
Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:_____ in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

Figure 4.1: Chain of custody-page 2.

Data Extracting

Forensics completely depends up the Data Extraction. Once the evidences have been collected from the crime sight. The first and foremost things that forensics investigators do is to analyze what data needs to be extracted through the evidences. As we all know that now a days

each and every one is use phone and saving its private information in his/her phone. Below are the list of data extraction methods.

- Data Extraction through Hardware;
- Data Extraction through software;
- Data Extraction through knowledge;
- Data Extraction through technology.

Data extraction through hardware. Hardware of iPhone has its own uniqueness, every part of iPhone is very useful in processing of Apple iPhone, extracting data from hardware of iPhone is one of the difficult challenges. We can find lots of data stored in memory of iPhone. Forensic investigators can find evidences on iPhone hardware like finger prints.

Data extraction through software. Extracting data using software is one of the more crucial tasks to forensics investigators, as 90% of evidences can be found inside iPhone like Photos, Messages, Browsing history and many more. Forensics investigators needs to have upgraded versions of software's to extract data from iPhones.

Data extraction through knowledge. Data in Apple iPhone is saved with a tight security and safety. Extracting data from Apple iPhone is not a easy task. So forensic investigators need to be well knowledge to extract data from one or another way.

Data extraction through technology. Apple iPhones are known from its technology and processor used in their performance. Data from iPhones cannot only be extracted from software, hardware and knowledge. It also needs to be extracted using best technology. Forensics investigators develop new technologies to find evidences while examining Apple iPhone.

Data of Interest

As a forensic investigator, we need to find which information is necessary for investigation and to come to know the people behind the incident. As a basic function of smartphones is to have connected and been in contact with people you are related with, this is the main goal of a mobile phone (Kandidatuppsats, 2013).

In a smartphone, there is loads of information that can be extracted but we are only interested to extract information that is useful for us for forensics. Data that I would be chosen for investigation are as follows.

- Call history. Call history contains recent incoming and outgoing calls from a mobile phone. This will help the forensic investigator to know with whom the suspect has been in contact with at or before crime scene (Kandidatuppsats, 2013).
- Contacts. Contacts contain a list of members with whom suspect is in contact with. It also contacts email and fax contacts. Most of the fraud evidence would be found in email connections.
- Messages. Messages contain chat history which tells forensic investigator with whom the suspect is chatting with. Apart from normal text messages now a day we also see third part text messengers like WhatsApp, Facebook Messenger, Instagram, Snapchat, etc. All these third part messengers run of 2G and 3G data connections
- Media. Most of the smartphone are purchased for good camera clarity as it can click good pictures. These smartphones can also record videos and audio as well. Pictures and video recording can be the key evidence for a crime scene (Kandidatuppsats, 2013).

- Deleted files. Deleted files are the darkest secrets of any suspect as now body was to save any information that can harm them, as they delete any kind of evidence so as a forensic investigator, we have to check each and every part of the cell phone for any kind of proof or evidence.
- Location tracker. Location helps us locate where the suspect was and at what time. Location data can be tracked by Google maps and WIFI location settings (Kandidatuppsats, 2013).

Summary

In this chapter, we have discussed on the literature related problems and different ways and procedures of extracting data from iPhone. There has also been discussion on chain of custody and how evidences need to maintain.

In this lesson we have also discussed methods of extracting data, these approaches are very useful and effective in current world of forensics. These extraction methods will help forensics investigators to know what data needs to be extracted. What are the different methods to extract data and what is data of that is in our interest to extract?

Chapter 3: Methodology

Introduction

In this chapter we are going to discuss on how we are going to perform digital forensics on Apple iPhone using different tools and technology. We would also be discussing on hardware and software applications that we are going to use in extracting our data of interest from Apple iPhone.

Design of Study

The study of this chapter in the paper is quantitative. To start with we would be using iPhone with IOS operating system. The main objective of this study is to learn and understand how we extract evidential data from iPhone using various methodologies. To perform these forensics act we need different hardware and software tools that have been discussed in previous chapters, once we extract our required data we would be formatting the files and documents for reporting purposes.

Data Collection

In this section of study, we would be going to collect all the data we require for forensics examination purposes like Photos, Videos, Notes, Messages, Emails, Google Maps, etc.

Once we extract all the required information, we would be examining them using forensics tools and technologies. The main aim of this study is to extract data from iPhone using various methodologies and compare them with each other and suggest the best method to forensics department.

Hardware and Software Requirements

To perform forensics on iPhone we require different kinds of software and hardware tools, below are the list of tools we would be using.

1. iPhone – 5S
2. Lighting cable (iPhone Charger)
3. IOS Operating System
4. iTunes
5. iPhone Extractor
6. iMyFone D-Port
7. Dell laptop
    - Windows 10 Operating system
    - RAM – 5GB
    - HDD – 500GB
    - Processor – i5 5200U @ 3.0 GHZ
    - Dell Charger

Budget

In the study of iPhone forensics, we require Apple iPhone and software and hardware tools that we are going to use for extracting data, the estimated budget that we would be using for this study are as follows,

1. iPhone – 5S: $250 to $400
2. Software and Hardware Tools: $150 to $200 (Most of the tools that I have used are basic version which are free to download)

Timeline

See the following table for the timeline.

Table 1

Timeline

Start Data	End Date	Task Performance	Time
10/05/2018	10/19/2018	Referring to the topic documents	2 Weeks
10/22/2018	11/05/2018	gathering information	3 Weeks
11/12/2018	11/26/2018	Comparing referred documents and finalization	2 Weeks
11/27/2018	12/04/2018	Collecting files for implementation	1 Week
01/02/2019	01/09/2019	Gathering data using various sources	1 Week
01/14/2019	01/28/2019	Analyzing all the gathered data	2 Weeks
01/28/2019	02/01/2019	Performing forensics on collected data	1 Week
02/5/2019	02/12/2019	Examining forensics results	1 Week
02/12/2019	02/18/2019	Comparing extracted results	1 Week
02/18/2019	02/25/2019	Reviewing results of comparison	1 Week
02/25/2019	03/04/2019	Completing Defense document	1 week
03/07/2019	03/10/2019	Review of complete document	3 days

Chapter 4: Data Presentation and Analyzation

Introduction

In this chapter, we would be discussing about what are the different software we are using to extract data from iPhone and its installation procedures. We would also be comparing data extracted from different software's with each other and advise which is the best software method to extract data for forensics.

Data Presentation

Data that is been extracted in this process would in different forms like images, messages, Emails, etc. Data which has been extracted has a key informative evidence that helps forensics investigators to catch hold of the criminal.

Installation process of iTunes. We would first go to website link https://www.apple.com/itunes/download/ to download iTunes. Then choose the version of iTunes according to your computer. My computer is running on Windows 10, So I am downloading below iTunes for my computer.

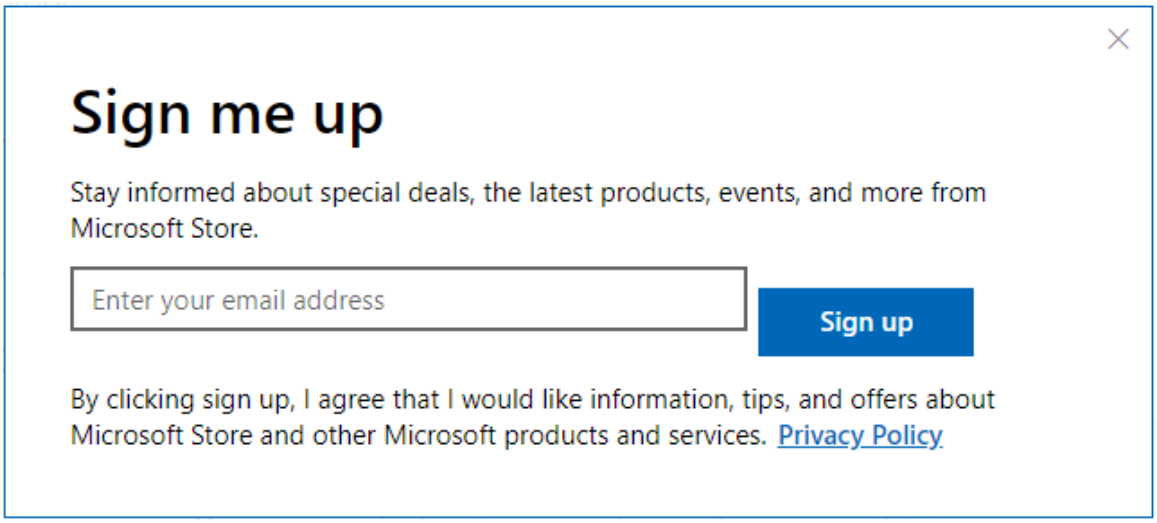


Figure 5: iTunes sign in screen.

Apple iTunes would ask you to create a unique Apple ID for security purposes, once we provide Apple ID it would divert us to the below screen.

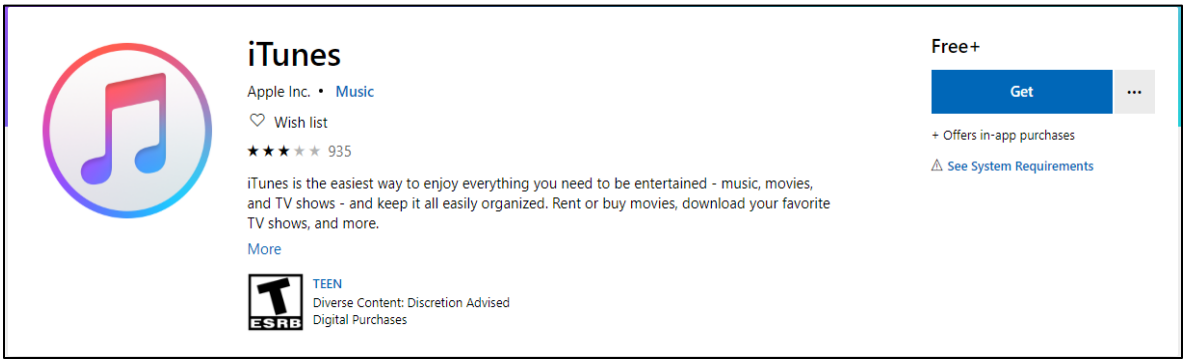


Figure 5.1: iTunes description screen.

Once the above screen pops up, hit on click and iTunes would be downloaded onto your computer.

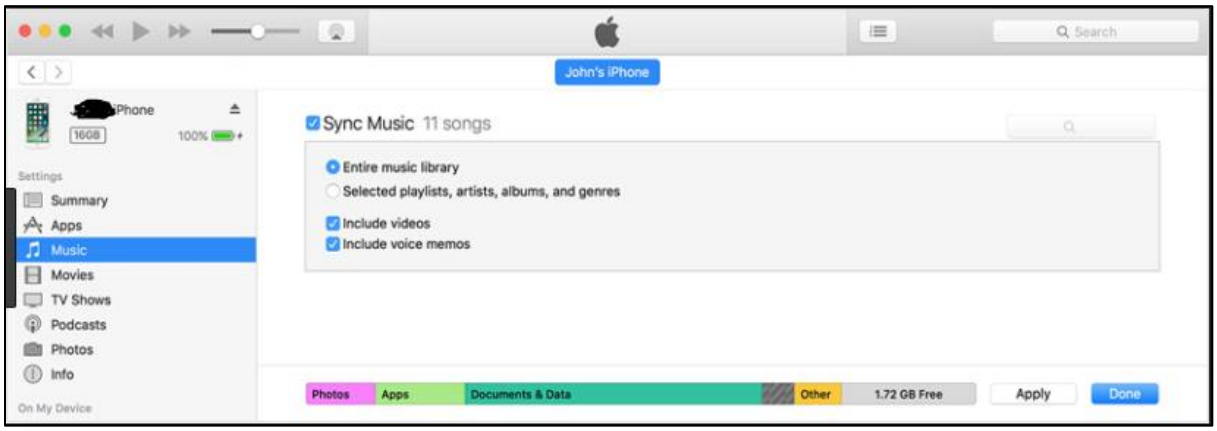


Figure 5.2: iTunes home page.

Once the iTunes has been downloaded on to your computer, It will take few minutes to sync the phone that is connected and above screen would appear with name, Storage capacity and break down of the storage. Once this screen appears which means iTunes has been successfully downloaded and installed.

Installation process of iPhone backup extractor. We first need to get on to its website link: https://www.iphonebackupextractor.com/ and once you get on to the below screen will appear.

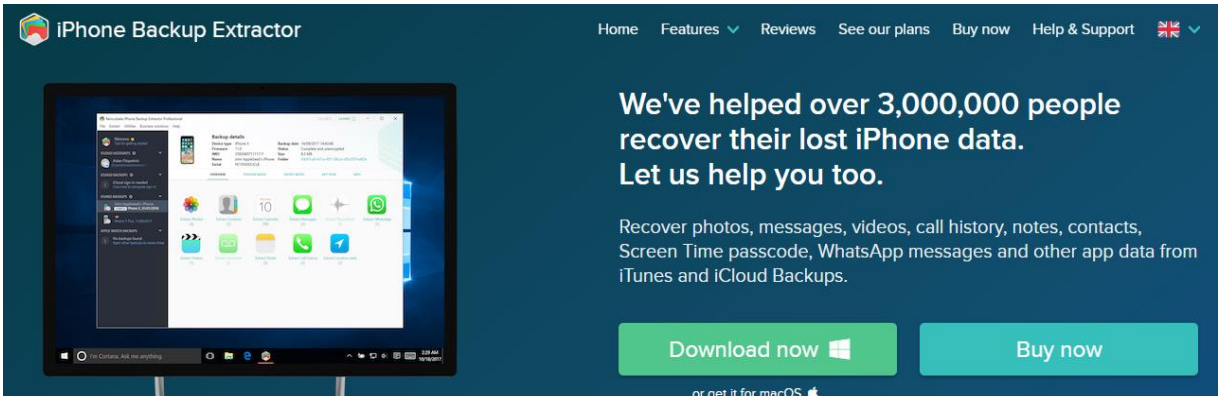


Figure 6: iPhone backup extractor download page.

As I am using Windows 10, I would be selecting Download now windows option. Once the downloading process has been completed, below screen appears.

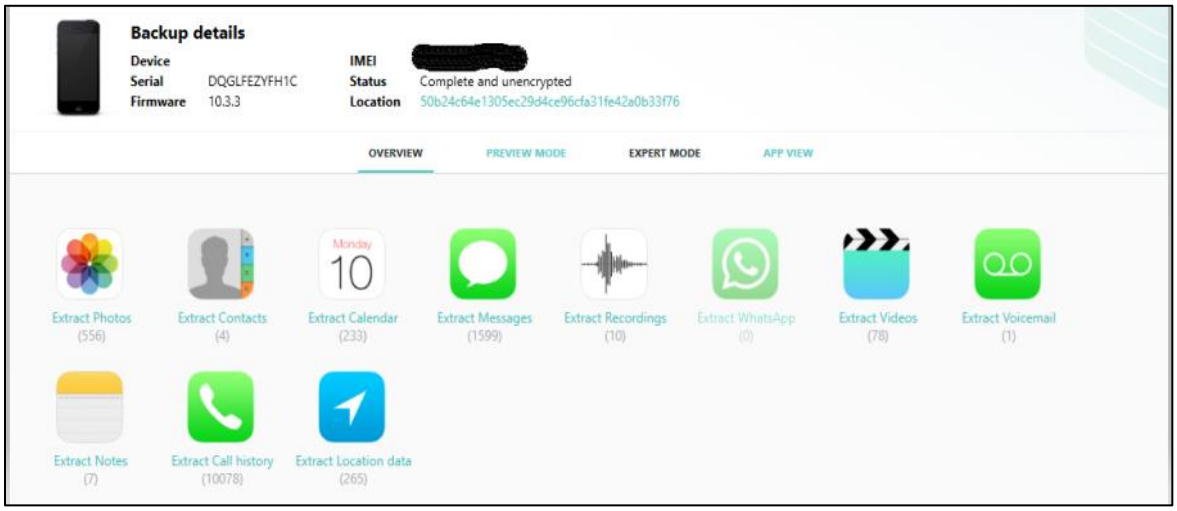


Figure 6.1: iPhone backup extractor home page.

In the above screen we can see that what all data is stored in the different applications with numbers.

Installation process of iMyFone D-Port. To install iMyFone D-Port application we need to get on to website link: https://www.imyfone.com/iphone-data-exporter/guide/ and download.

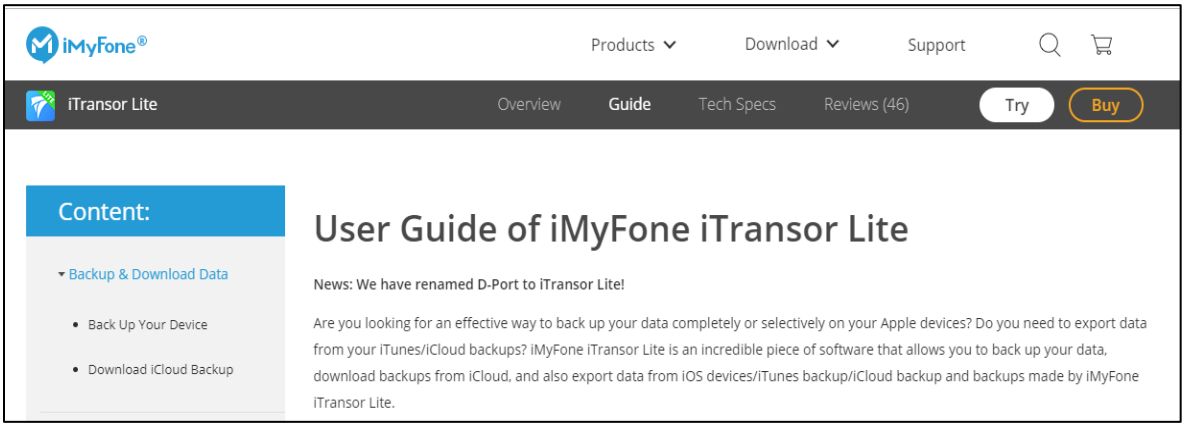


Figure 7: iMyFone D-port download page.

Then download the application version according to our windows version.

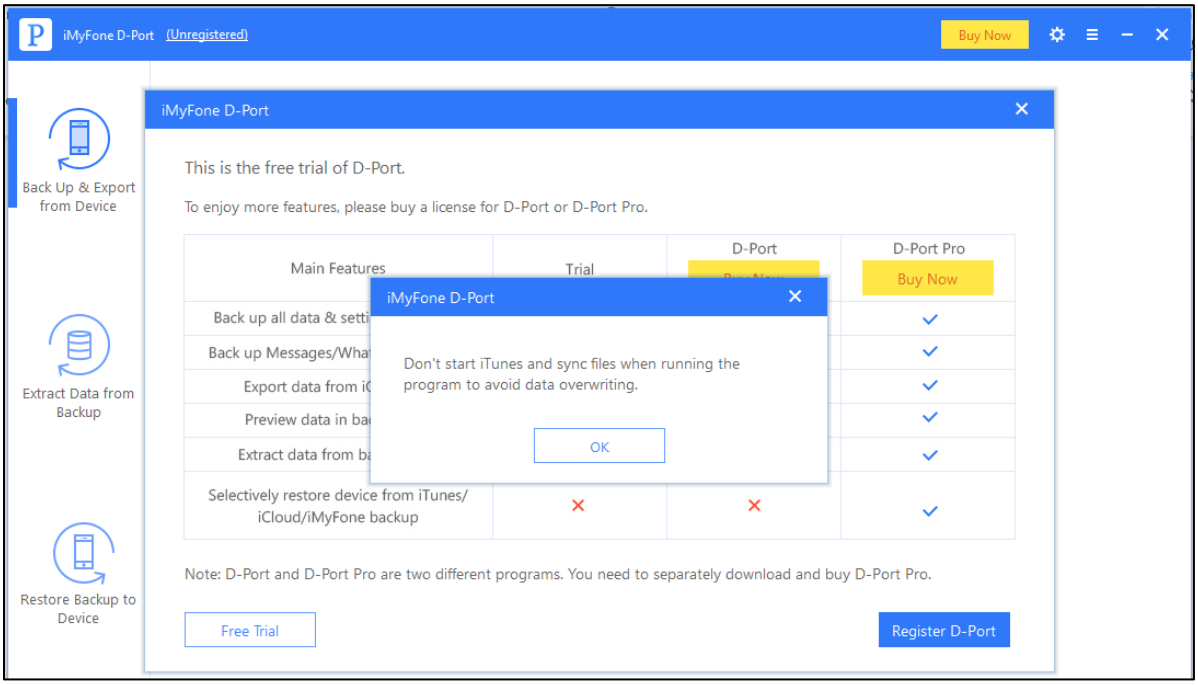


Figure 7.1: iMyFone D-port download process.

This application would not sync if iTunes software is in running.

The final screen of iMyFone D-Port looks like below.

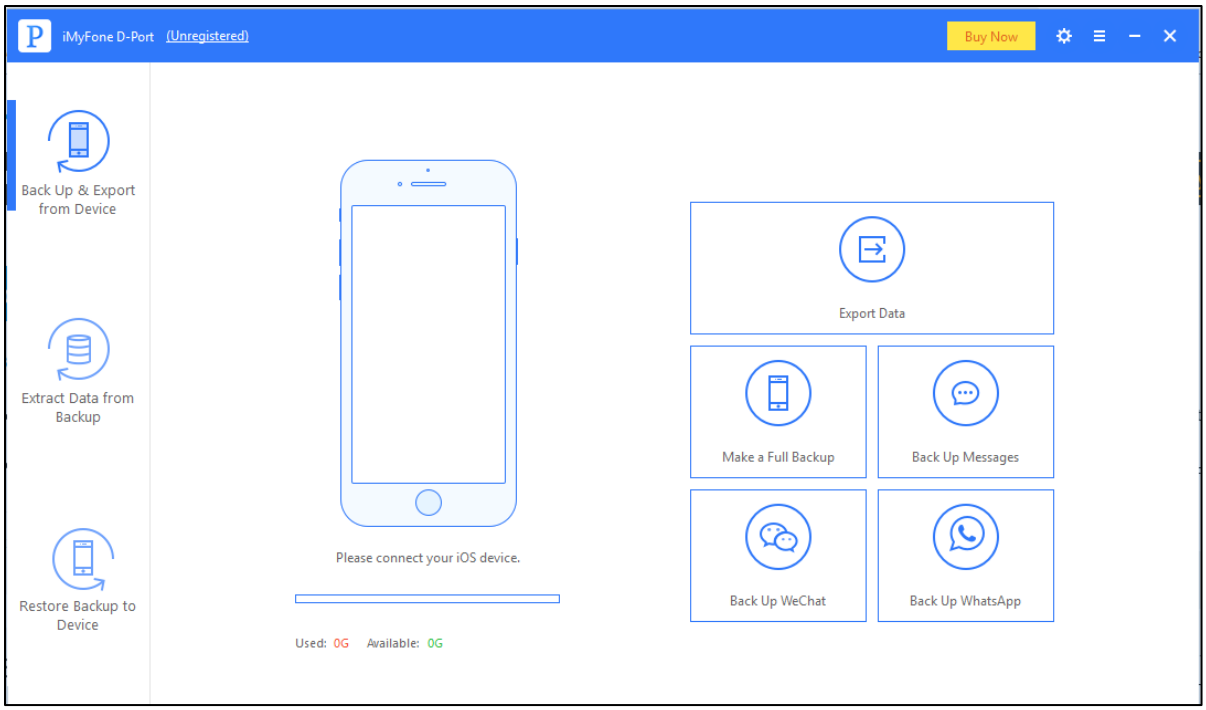


Figure 7.2: iMyFone D-port home page.

Source of interest

Apple iPhone is very secured device with strong firewall, and it contains source to its back folder which stores all the phones internal data like, Photos, Notes, Videos and many more. We need to look very carefully in to all the backup files to check if there is any valuable information that can be useful as a evidence.

When we connect the iPhone, we are examining to the computer, System will detect the device and it will pop the below screenshot.

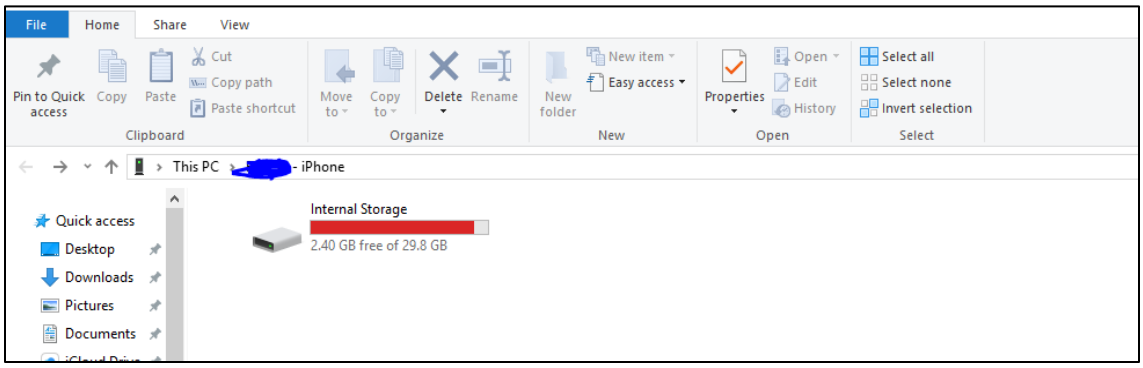


Figure 8: iPhone backup folder.

Below is the internal folder that contains information that is valuable for forensics.

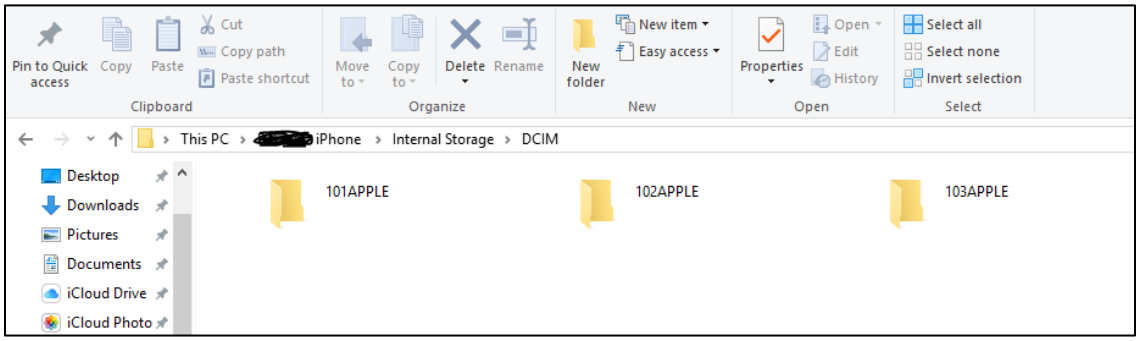


Figure 8.1: iPhone backup sub-folder.

The image below shows us the information we are looking for our forensics investigation.

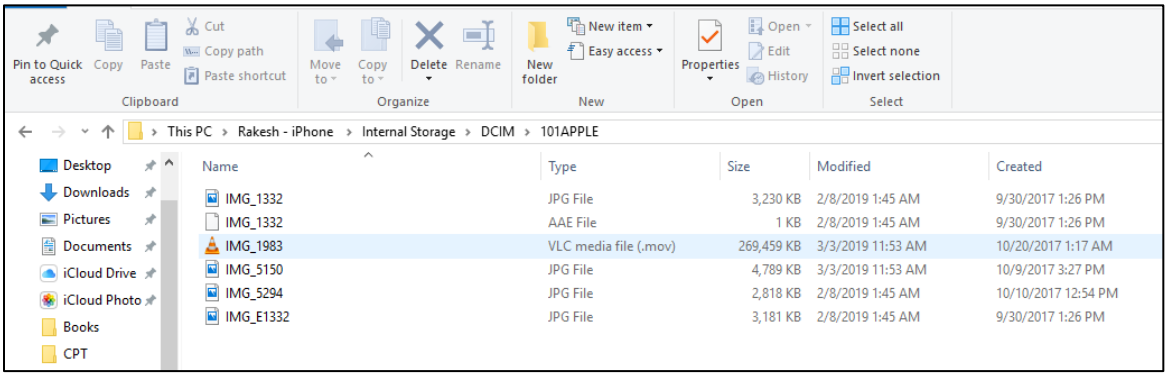


Figure 8.2: iPhone backup internal folder.

Data Analyzation

In this part of the section we would analyze all the evidences we have gathers using different methods of extracting data (“What Do iPhone Forensic Investigations Reveal?”, 2018).

Extracting data using iTunes. In this procedure we are going to learn how extraction of data can be made through iTunes. To perform this extraction we require an Apple iPhone, laptop and a lighting cable. In the first place we connect iPhone to the computer with help of lighting charger, as we connect Apple iPhone to computer will detect the device and it will popup below image. This image is an indication to us that computer is trying to detect the iPhone device connected to the respective computer. Once we hit Trust than the actual process of syncing of iPhone to the computer will begin, iTunes application will sync with the detect iPhone and it starts reading the iPhone.

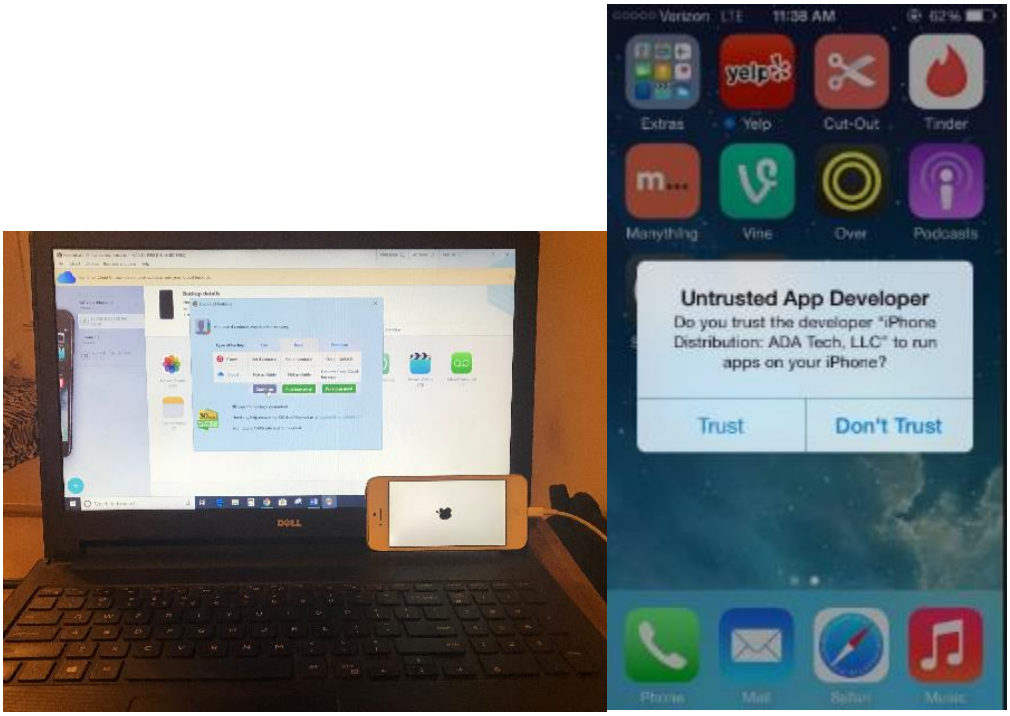


Figure 9: iPhone trust.

As soon as the sync process is competed than folder gets populated with all the backup files in it. Below is the image of the path where all the backup files and documents are saved of Apple iPhone.

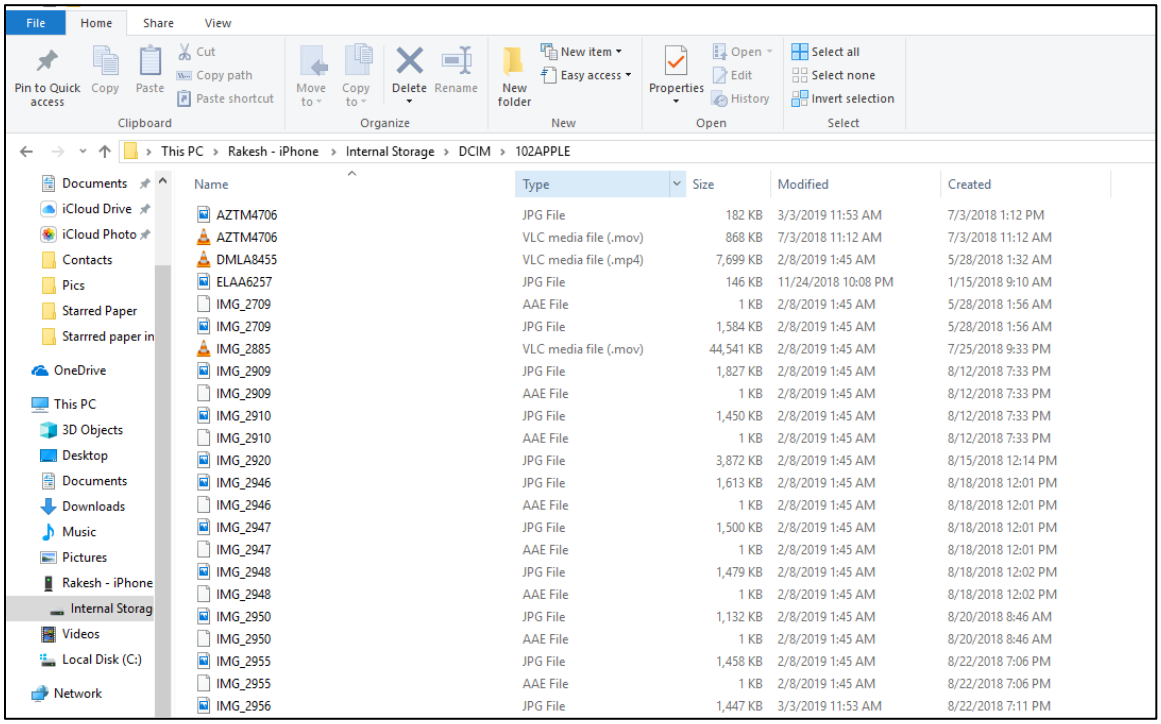


Figure 10: iPhone storage folder.

As the iPhone is connected to the computer and iTunes has detected the iPhone it will populate the below image, this image is called the home page of iTunes. In this image you can only view very basic information like, who is the owner of the phone and what are the recent applications the iPhone user has reviewed. This information is not much useful for forensics examination purposes, but it is very good start for examining iPhone. This image is very perfect start for extracting data from iPhone using iTunes. If you see in the below image you will see that there is phone like small image that is the key part in this image. This image will take us to

the person information of the iPhone user like Photos, Videos, Notes, Applications used and may more (iTunes, n.d.).

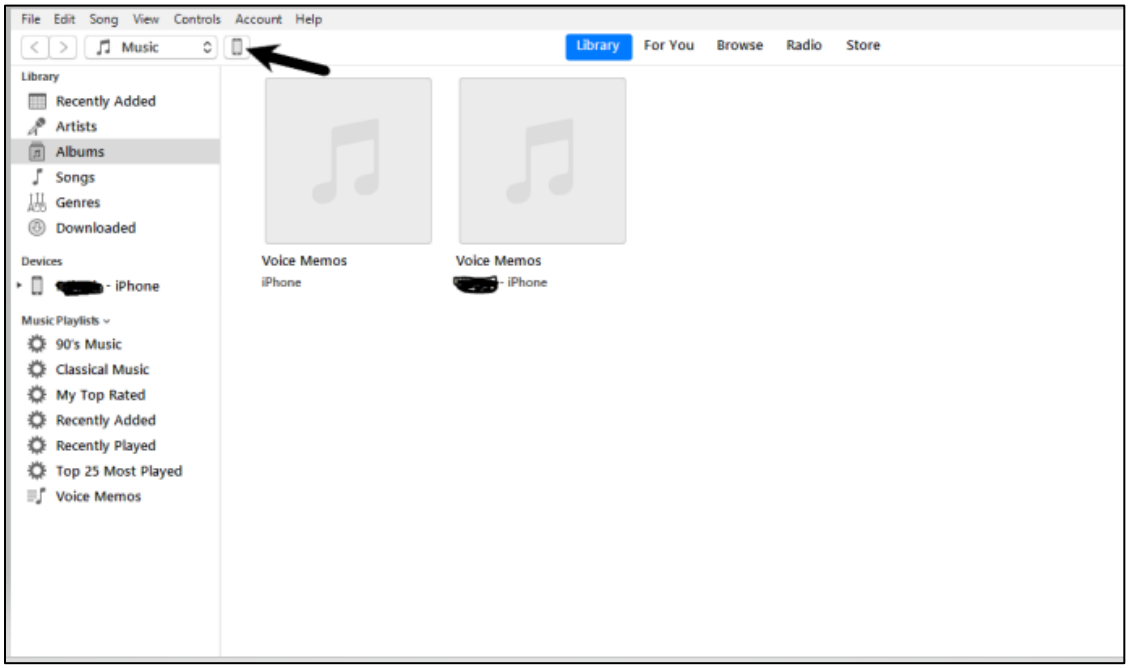


Figure 11: iTunes home page (selecting of iPhone).

Once you click on the small phone image you will see below screen, this screen gives us the information we are looking for forensics' examination purposes. I will go through each and every detail information we can find for forensic in this below image. I have divided the below image in to four different sections for easy explanation.

Section 1. In section 1 contains some of the valuable information like which model is the phone, like in this image we can see that model of the phone is 7. Phone number (For privacy reasons I have colored) is another key information we can find in this section. This section also tells us with what the serial number of this phone number is. This number is provided by apple as a service number, this number helps iPhone owners to track their phone in case of lost or theft. In

this section we can also see the software that is running on the iPhone connected to iTunes (imore-files in iPhone and iTunes, 2018).

Section 2. This section provides us with the backup information such as automatically back-up which means when the iPhone is connected to iTunes that data that needs to be extracted would that needs to be backed on to the computer or to the iCloud. We can also see the information like when the last backup was done on this phone.

Section 3. Section 3 is the very important section as this provides us with the valuable information like Photos, Videos and personal information and files (applications) stored in the iPhone connected.

Section 4. This part of the section does not provide much valuable information this section provides us with the Movies, Music and TV Shows stored in the phone. This information can help us to understand what kind of person is the one who is using this iPhone.

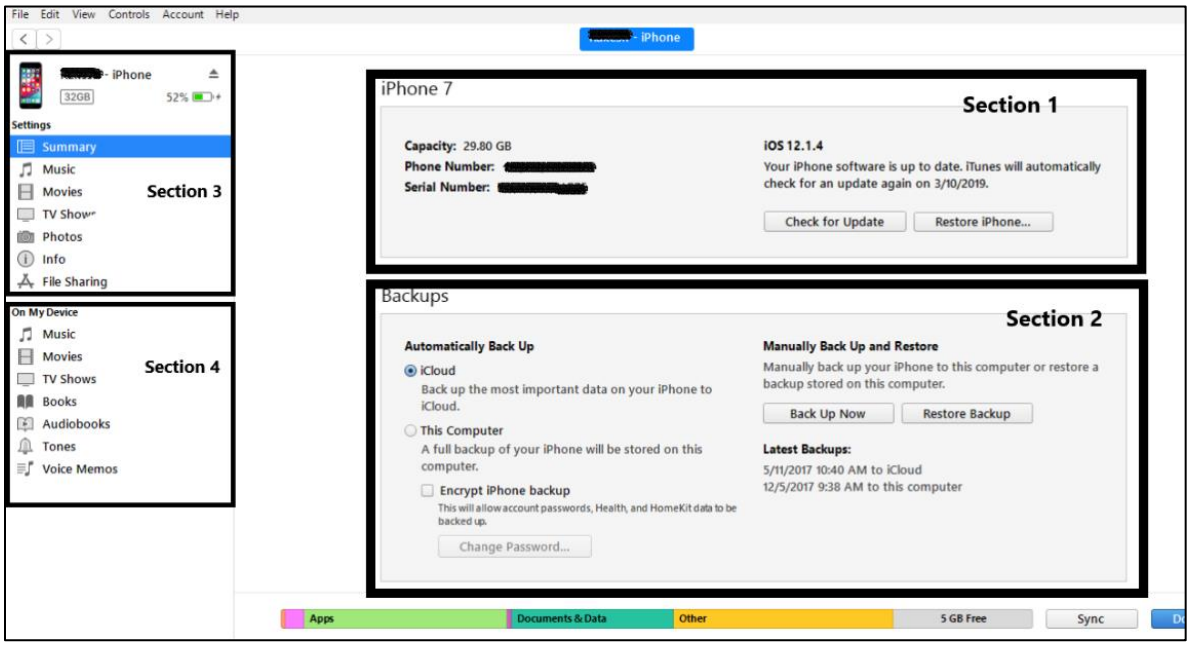


Figure 11.1: iTunes section wise description.

Information what we are looking for our examination can be found in Section 3. Let's start looking in to this section.

Data extraction process–iTunes (Apple.com).

Extracting photos and videos through iTunes. As we select photos tab and select Sync Photos and include videos and select the location when you want to save this picture then all the photos, videos in the phone will come into the selected folder.

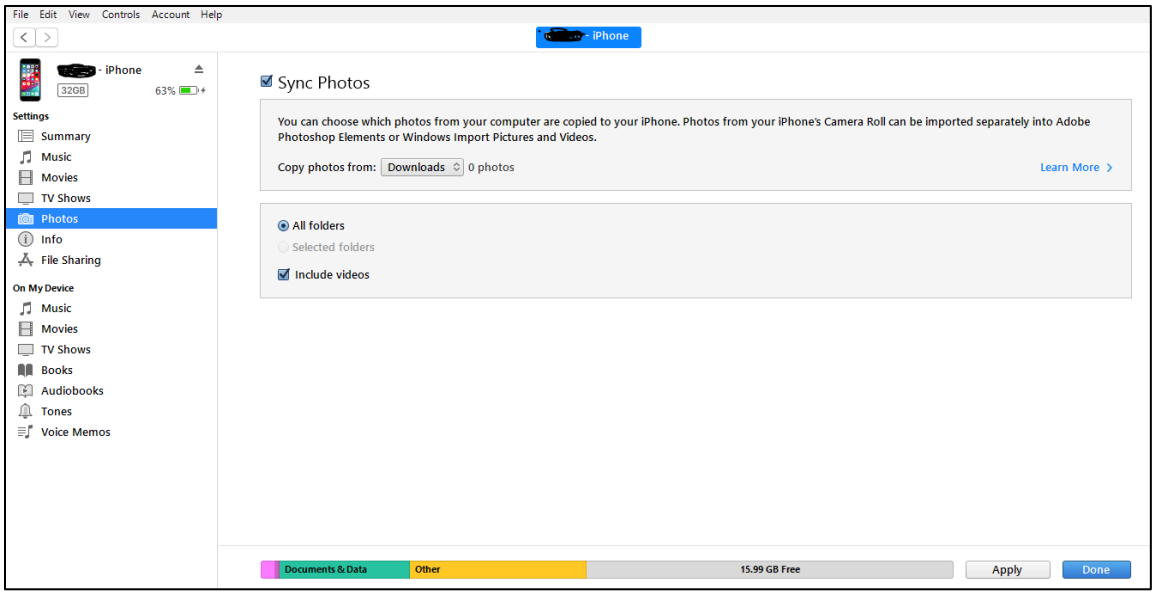


Figure 12: iTunes photo and video file.

Below screen shows us the photos and videos that are stored in the iTunes connected iPhone. This is a very valuable information that we have extracted now. Photos and Videos are the very valuable proof of evidence in the court of law. Photos and Videos gives us the explanation about the suspect and with whom has been meeting and his target has well (iTunes, n.d.).

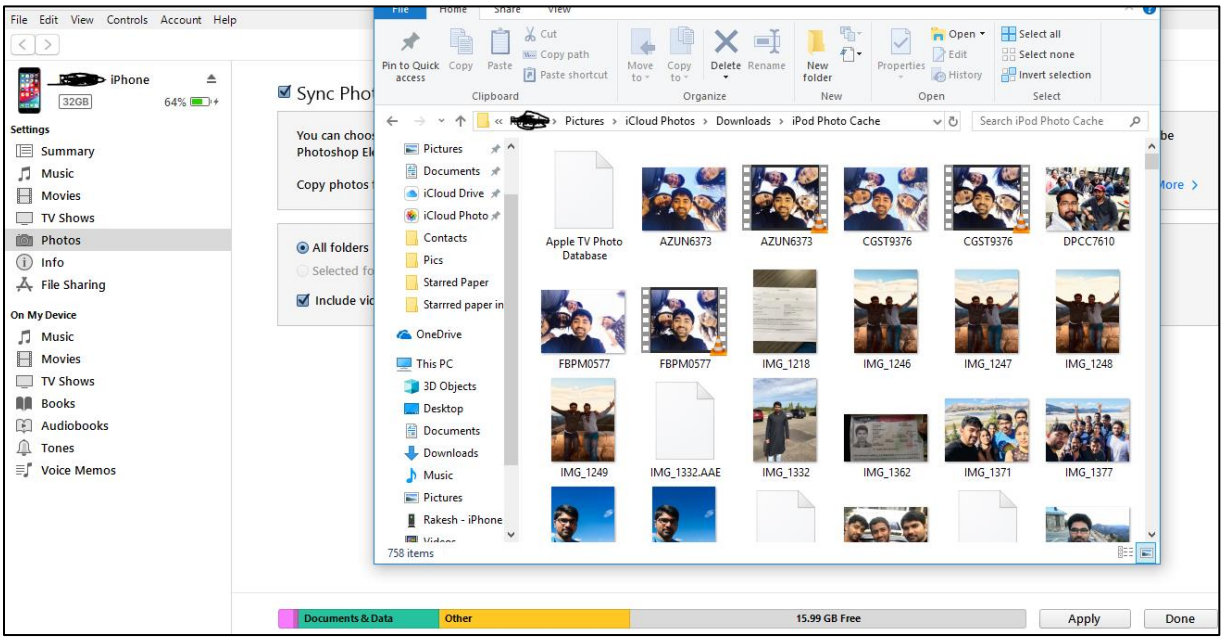


Figure 12.1: iTunes photo and video folder in local computer.

Extracting contacts through iTunes. In section 3 of iTunes we can also see a column with **info,** as we select the info option we can see below screen, this screen tells us to sync contact into the iPhone connected laptop, we only need to do is to select the info option and hit apply at the bottom right side of the screen.

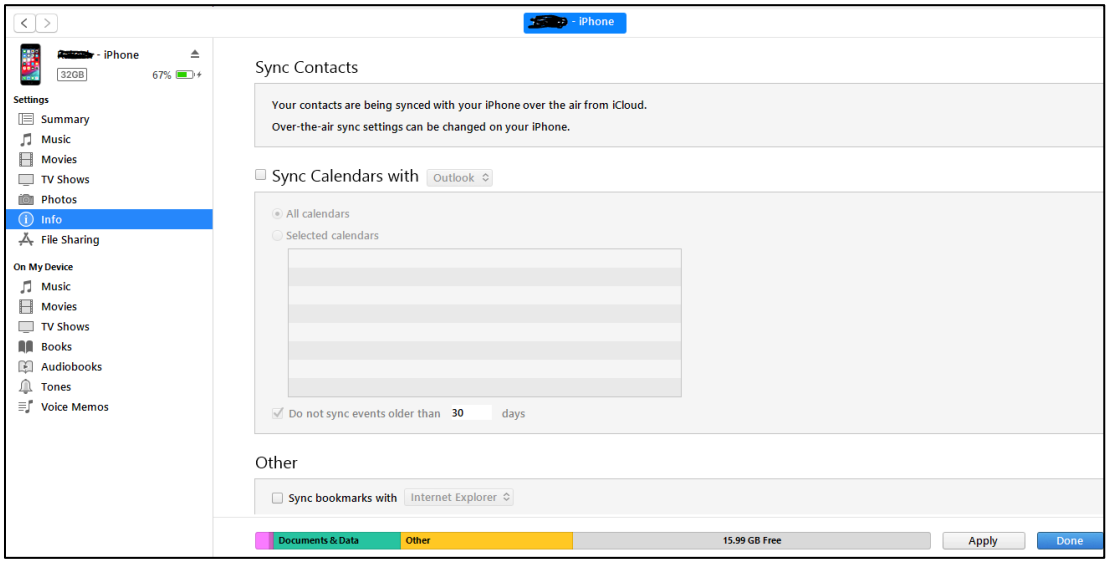


Figure 13: iTunes contact information.

Once we select sync option and apply the required changes to iTunes this would direct us to the location where contacts are being saved. Below is the screen that explains us about the contacts saved in iPhone.

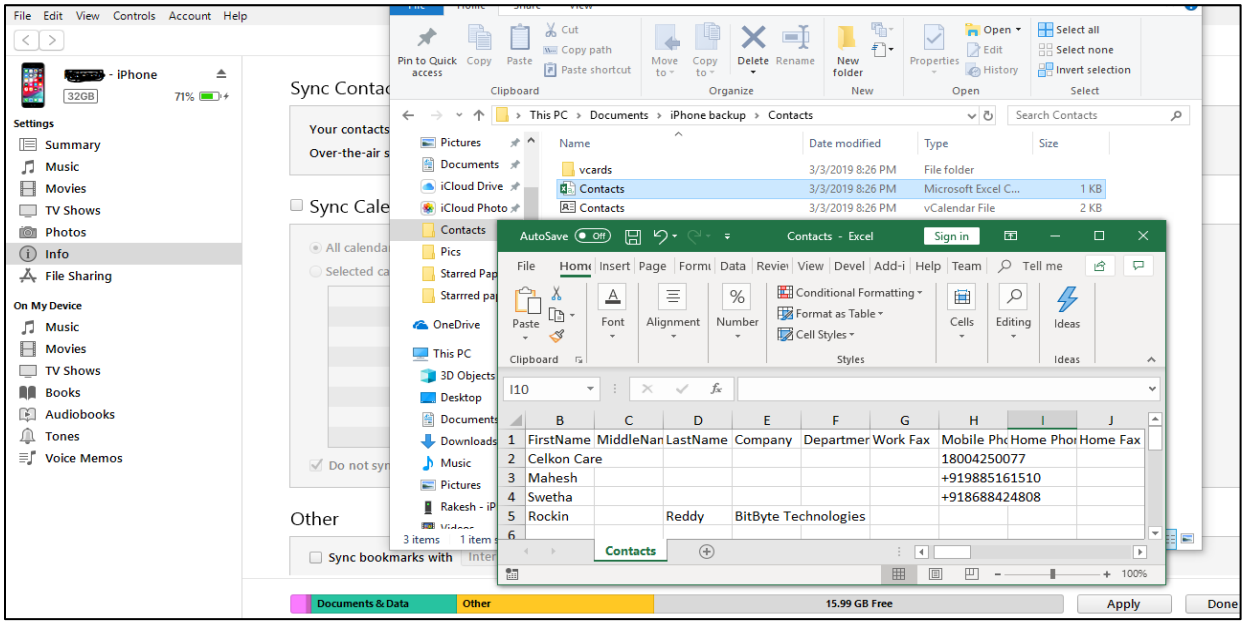


Figure 13.1: iTunes contact list (Excel).

Extracting application through iTunes. In section 3 of iTunes we can also see a column name with **File Sharing,** as we select the file sharing option, we can see below screen this screen show us the list of applications used in by the suspect.

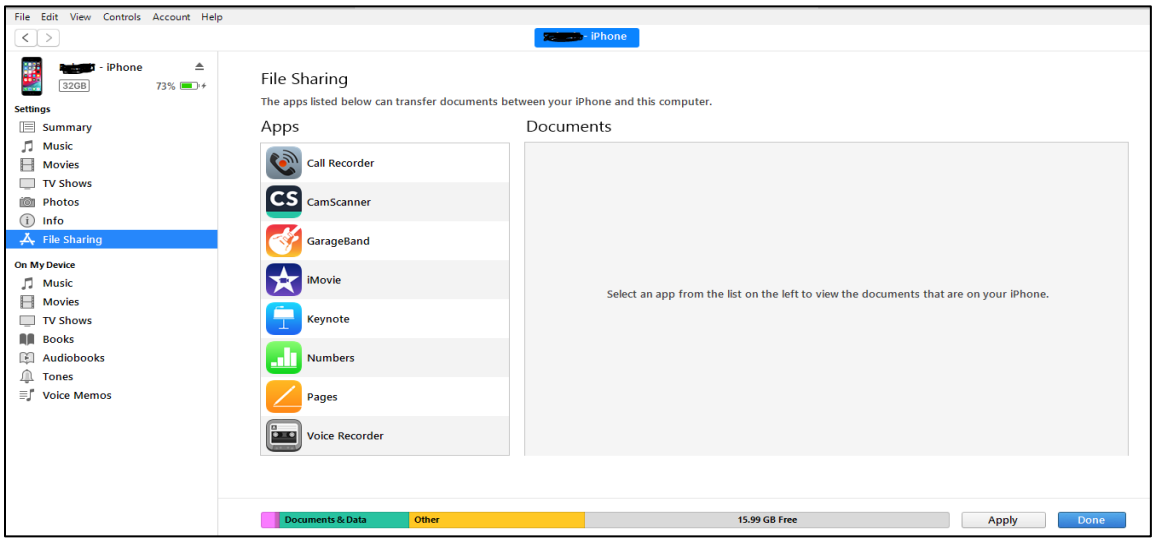


Figure 14: iTunes application screen.

As we can see in the below image that the suspect is using some suspicious applications like Phone Recorder and Voice Recorder. We can also see the list of call recordings of the phone.

Figure 14.1: iTunes call recording.

As we can see in the below image that the suspect is using some suspicious applications like Phone Recorder and Voice Recorder. We can also see the list of voices recordings of the phone (“Cell Phone and Tablet Forensics”, 2018).

Figure 14.2: iTunes voice recording.

This is some of the most valuable evidences we could collect through iTunes. We have tried to collect more information like Email, Deleted files, Call history and Messages bur however we could not collect. Let us see if we can collect this information in other two applications that we are going to use in this paper for extracting evidential forensic data.

Extracting evidential data through iPhone backup extractor. iPhone Backup Extractor is a third-party application which is quite famous application used to extract data. I have chosen this application is because this is quite handy software application to extract data from iPhone. This software application can extract more evidential information then iTunes has extracted is my feeling. Let’s go ahead and start the process of extracting data using iPhone Backup Extractor.

To start with the procedure of extracting evidential data using iPhone backup extractor, we need to install the iPhone backup extractor on to the computer as show in previous chapters. First let's start with the connection procedure by connecting iPhone that we are examining with a lighting cable to the computer in which the software is installed. As we connect the phone and select iPhone backup extractor software application, we can see that software starts to read the connected iPhone (imore-files in iPhone and iTunes, 2018).

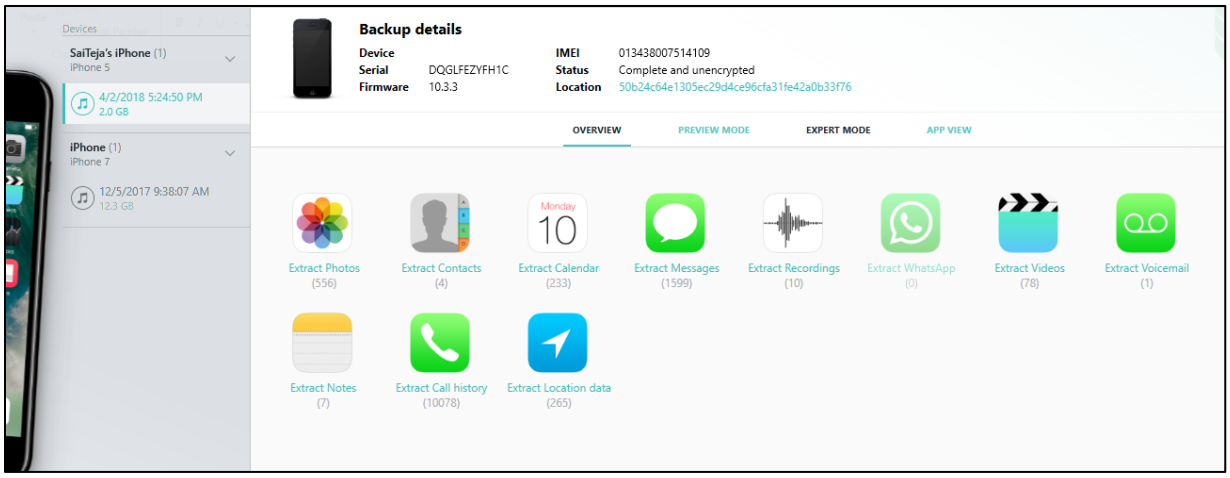


Figure 15: iPhone backup extractor (home page).

The above image is the home screen of iPhone backup extractor. I am going to divide this screen in to 3 sections for easy understanding and explanation. Let's is go ahead and look in to the explanation process of the software application.

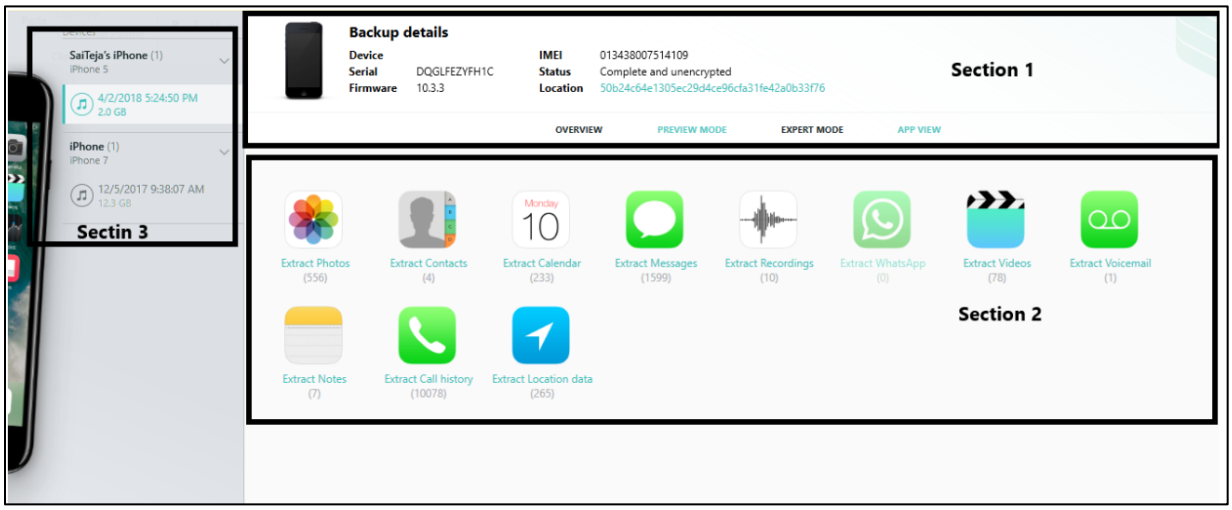


Figure 15.1: iPhone backup extractor (home page split into sections).

As we can see in the above image, we have divided it in to 3 sections. Let's go ahead and discuss about these sections and what kind of valuable forensic evidential information we can find through the application. All the 3 sections of this application are very useful for forensic investigators (Extractor, B. E., 2018).

Section 1. As the name in section 1 suggests that it is a back-up section. It contains some of the valuable information that would be very useful for our experimental purposes. Evidences that need to look at first is the backup location. As we select the backup location in the application. It would navigate us to the location where all the backup files of the software are going to get collected.

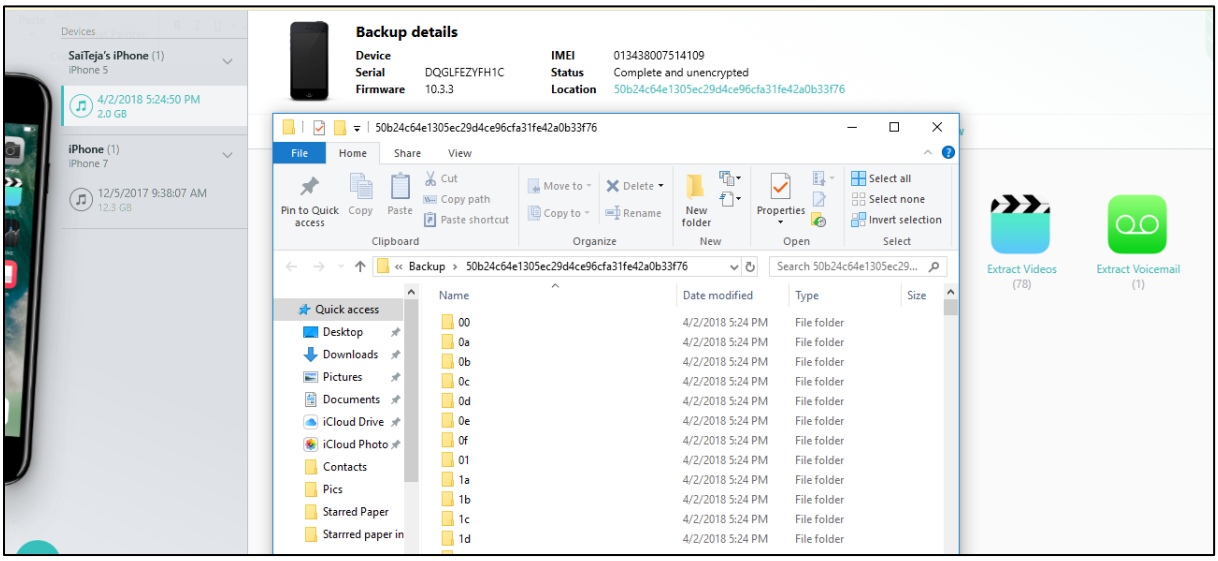


Figure 15.2: iPhone backup extractor (backup file).

Serial and IMEI number are also few internal valuable information providing number, as discussed in the previous chapters if an Apple iPhone is lost using Serial and IMEI number we can track the lost or theft iPhone. Firewall provides us information about that software version that is being used on iPhone.

Section 2. In section 2 we can find the list of software applications that have been stored iPhone like Photos, Contacts, Messages, Notes, Call History and Location Data. These are the valuable information that we are looking for extracting evidential data for our forensic purposes.

Section 3. In section 3 we can see the previous devices connected to iPhone backup extractor software. this section does not provide us with much informative information but just only the count of devices connected to the software. let us start with data extraction and analyzation.

Data extraction process–iPhone backup extractor.

Extracting evidential contact information through iPhone backup extractor. As we can see in the section 2 there is an icon named with Extract Contacts, we need to select that icon and it would navigate us to the folder into which we would like to store the data.

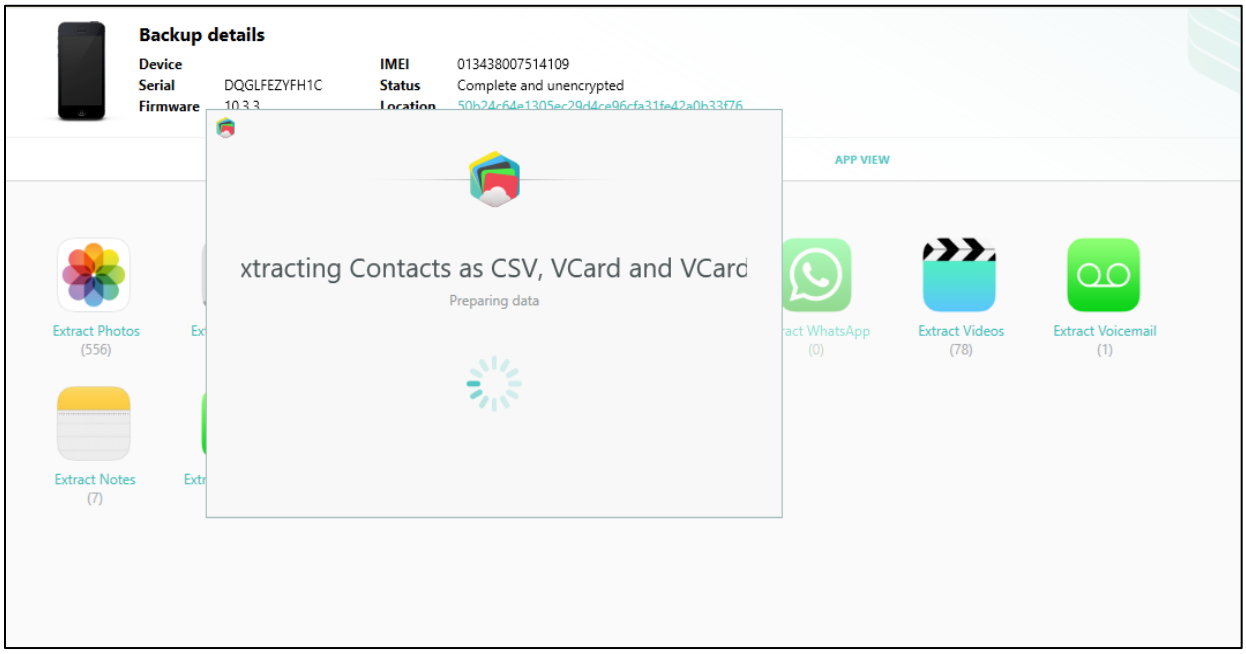


Figure 16: iPhone backup extractor (contact Information).

Once the folder in which data needs to be stored is selected the below popup screen would reflect and this screen would ask us to select the level of backup we would like to choose, as we are using this paper for internal purposes, I am selecting lite version and it would help to extract only few contacts from the iPhone (Extractor, B.E., 2018).

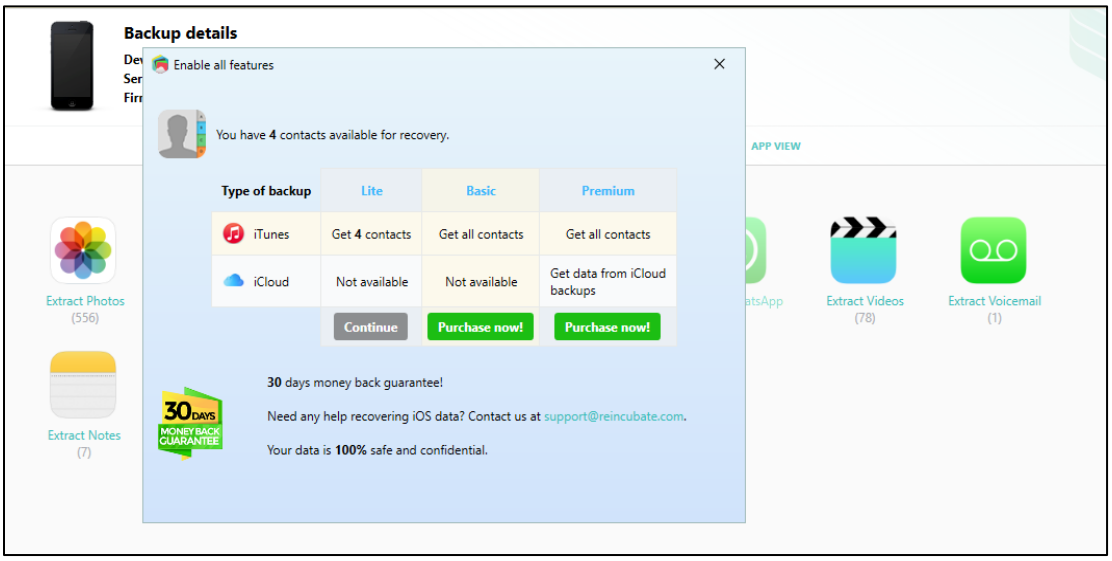


Figure 16.1: iPhone backup extractor (backup selection)

As we can see in the below image folder contacts have been exported to the selected location on to the laptop and this is a very valuable information for forensic investigators to get the list of contacts saved in the iPhone. By tracking these contact details, we can easily track the suspect and punish him under the court of law (Extractor, B.E., 2018).

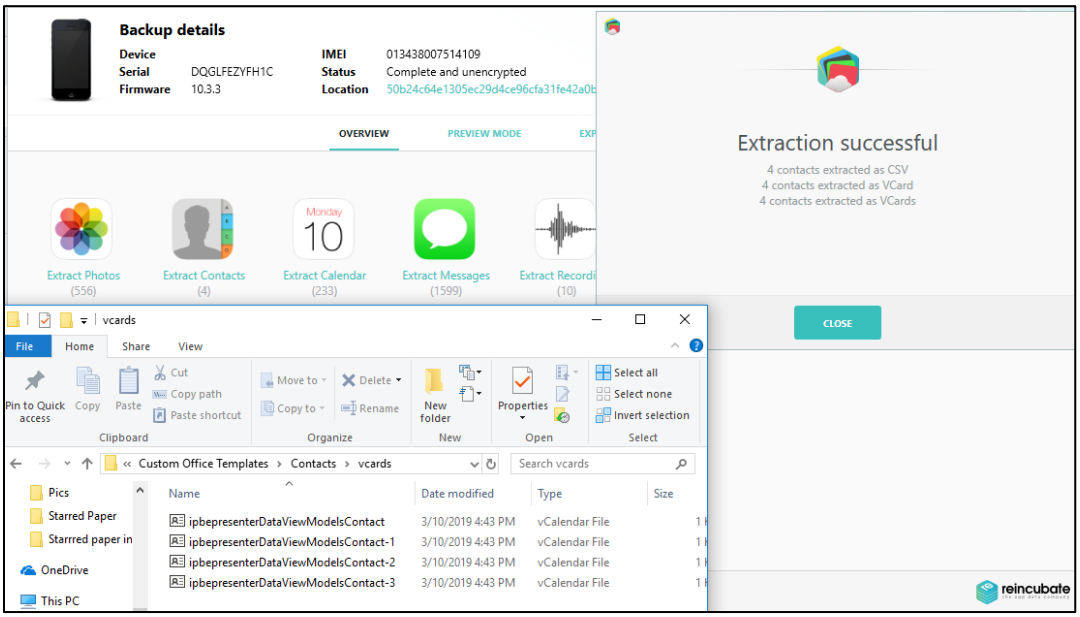


Figure 16.2: iPhone backup extractor (contact information details).

Extracting evidential messages information through iPhone backup exporter. In the section 2 we can see an icon named under Extract Messages, this is Extract Messenger software will read all the messages in the phone and save them on to the software, once we select the icon it will ask for the messages to be saved as CVS file, HTML file or PDR file. I would select PDF file and hit continue under lite. Let's see what data would be extracted.

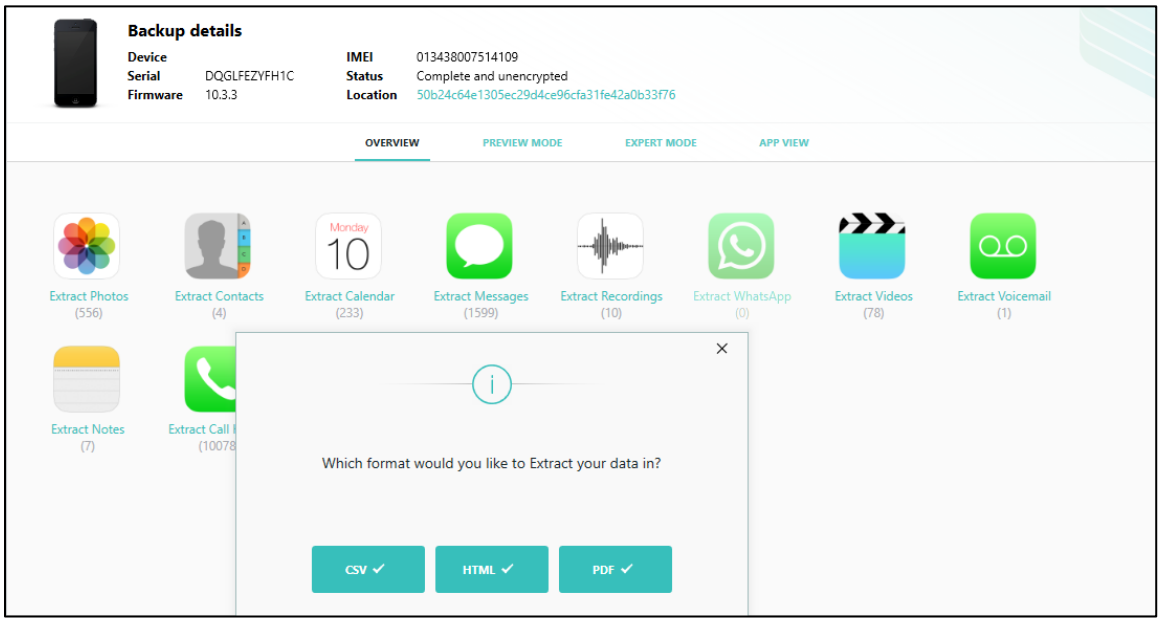


Figure 17: iPhone backup extractor (messages)

As I have selected messages to be extracted as PDF file, in the below image you can see that messages have been extracted successfully in to the computer just by few clinks and path selections.

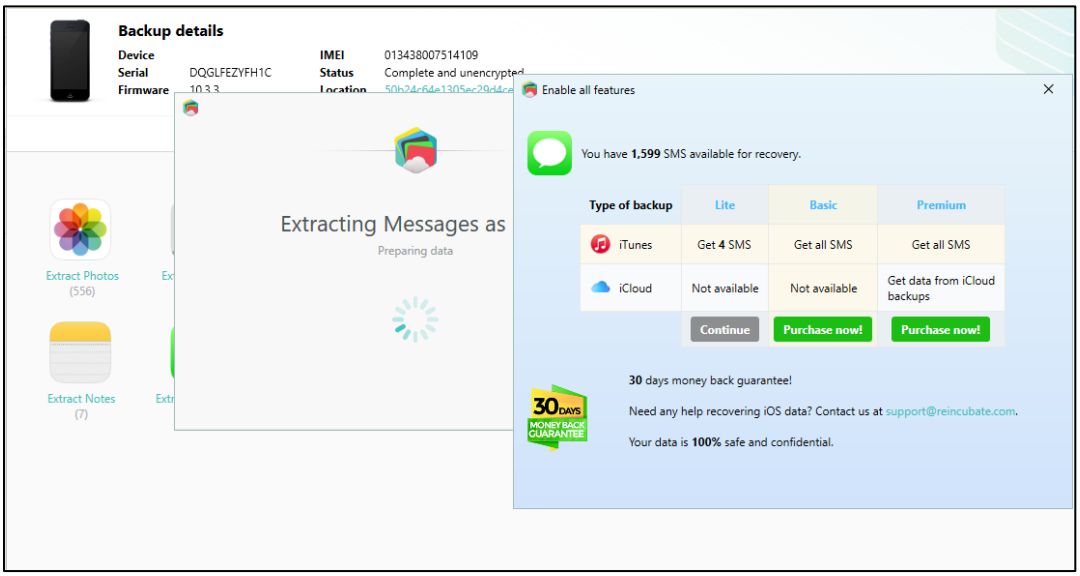


Figure 17.1: iPhone backup extractor (messages type selection).

As I select the lite continue version in the type I can see folder gets populated with the messages downloaded in to it. iPhone backup Extractor is one of the best and easy extraction tools used for extracting messages data from iPhone. These messages are one of the key evidences in the court of law to find out who is the suspect of the incident.

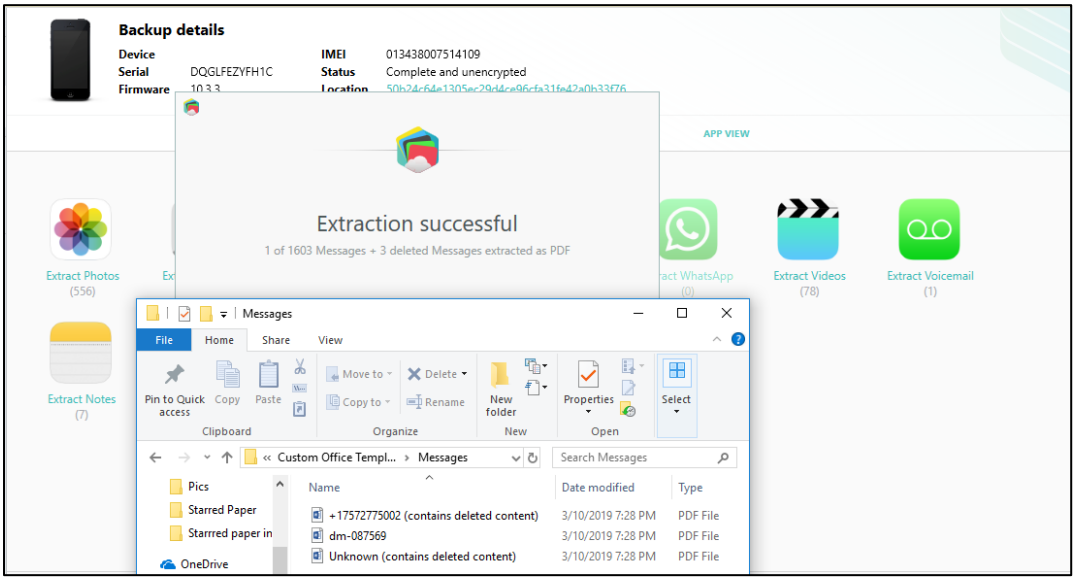


Figure 17.2: iPhone backup extractor (messages details).

Extracting evidential iPhone recordings through iPhone backup extractor. iPhone Recordings are also one of the important evidences in finding out who is the suspect. Let's go ahead and extract Recordings using iPhone backup Extractor. In the section 2 of the iPhone backup extractor there is an icon with the name of Recordings.

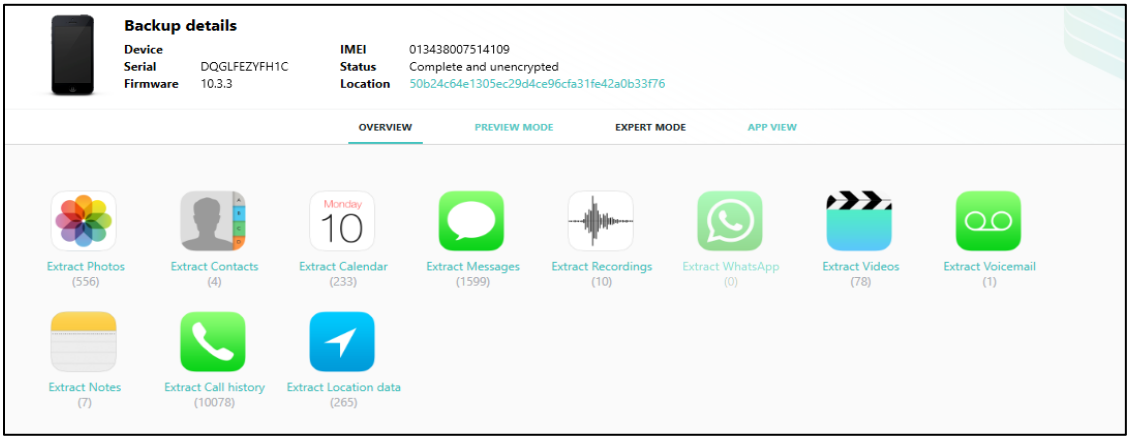


Figure 18: iPhone backup extractor (iPhone recordings)

As we find out the extractor software application in the section 2, we need to select the application and the application will start reading the recordings in the iPhone that has been backed up iPhone backup software and it will ask us to select the type of backup do we need and as we are using lite, I would hit continue under lite and let's see what we find.

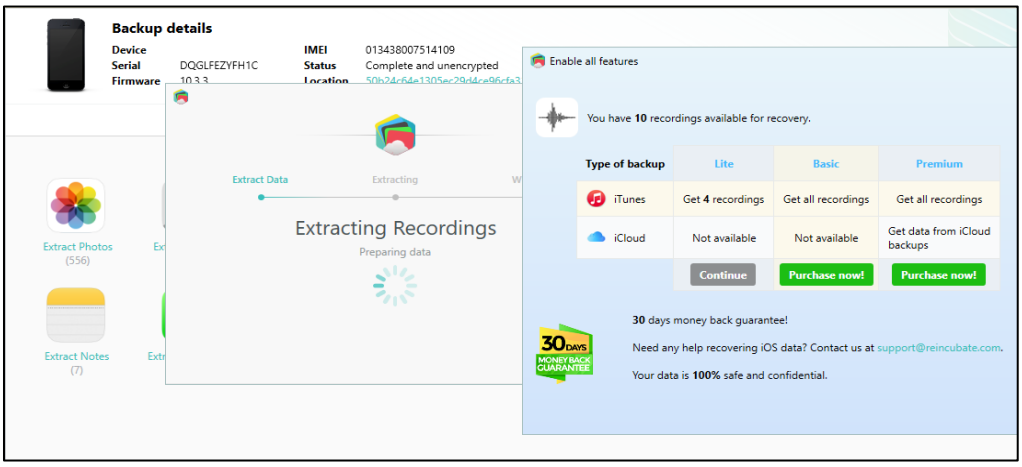


Figure 18.1: iPhone backup extractor (iPhone recordings type of selection).

As we hit continue under lite iPhone backup extractor would export phono recordings in to the backup folder into the computer as we can see in the below image. These Phone recordings are very valuable information in the eyes of law as evidences as they cannot be emended. IPhone backup extractor is the best and easy accessible application that it can been used my common man as well (Extractor, B.E., 2018).

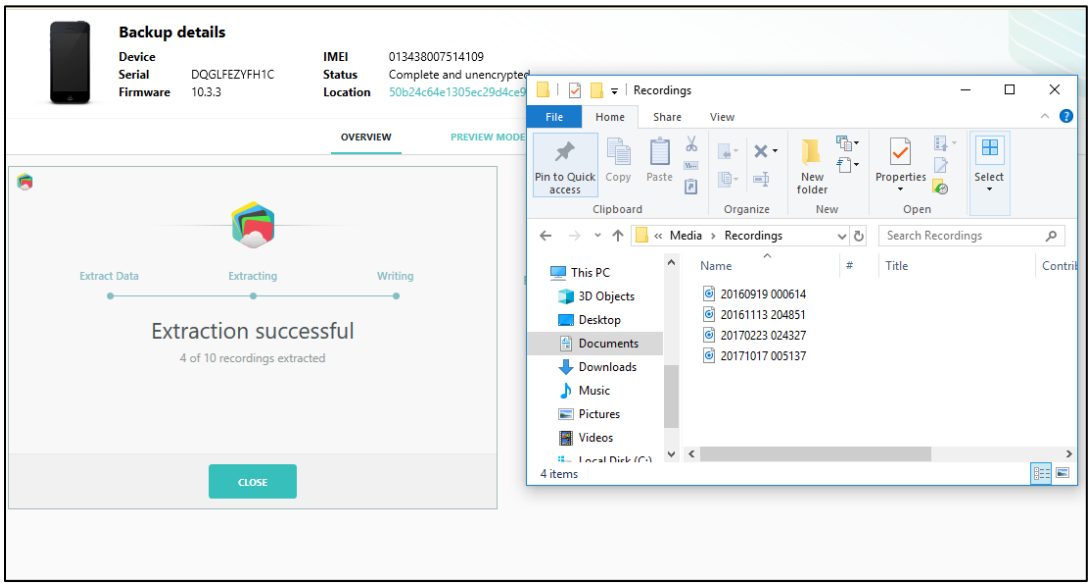


Figure 18.2: iPhone backup extractor (iPhone recordings details).

Extracting evidential whatsapp (messenger) through iPhone backup extractor.

WhatsApp is a third-party call, text and photo sharing application. This third-party application is weirdly used messenger in the world. This software application contains very informative and valuable data stored in it. As there is no WhatsApp data in the phone, I am examining I am using iPhone 7 for extracting data from WhatsApp messenger.

Let's start the process of extracting WhatsApp data through iPhone Backup Extractor from iPhone 7.

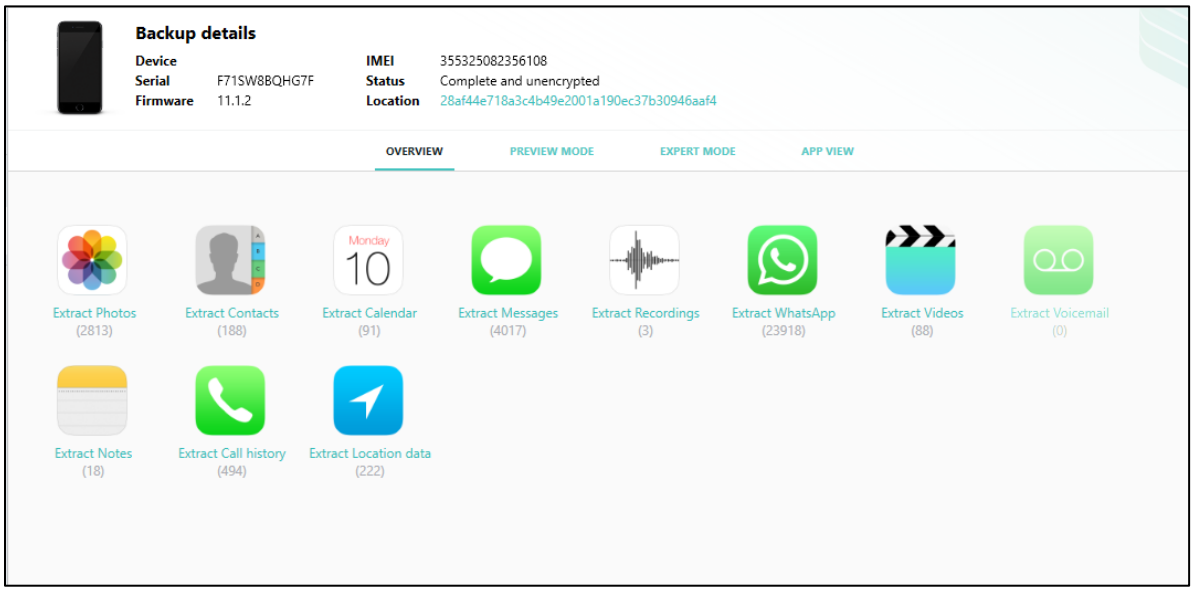


Figure 19: iPhone backup extractor (whatsapp messenger).

As we can see in the section 2 of the iPhone backup extractor, we can see WhatsApp third-party application, In the first place we would select the WhatsApp application.

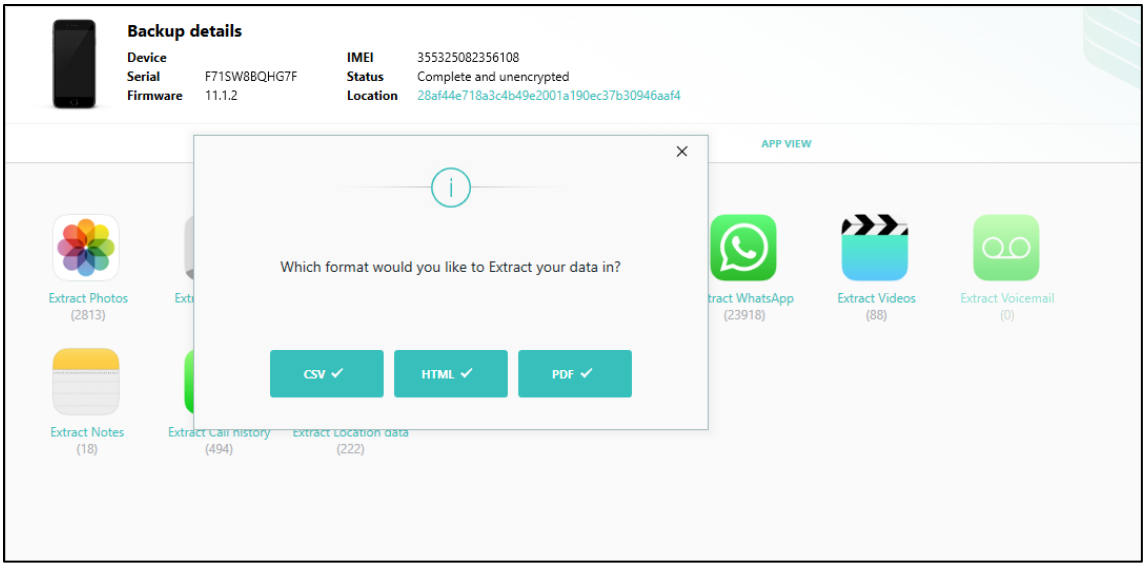


Figure 19.1: iPhone backup extractor (whatsapp messages save format).

As we selected WhatsApp application it give me a popup asking in which format would we like to save the data, I would select PDF file format.

As I selected the option of PDF format to be used to save the data. It next gives me a popup asking what kind of backup data recovery I would like to use, I would like to use the lite version as this paper is for internal purposes (Extractor, B.E., 2018).

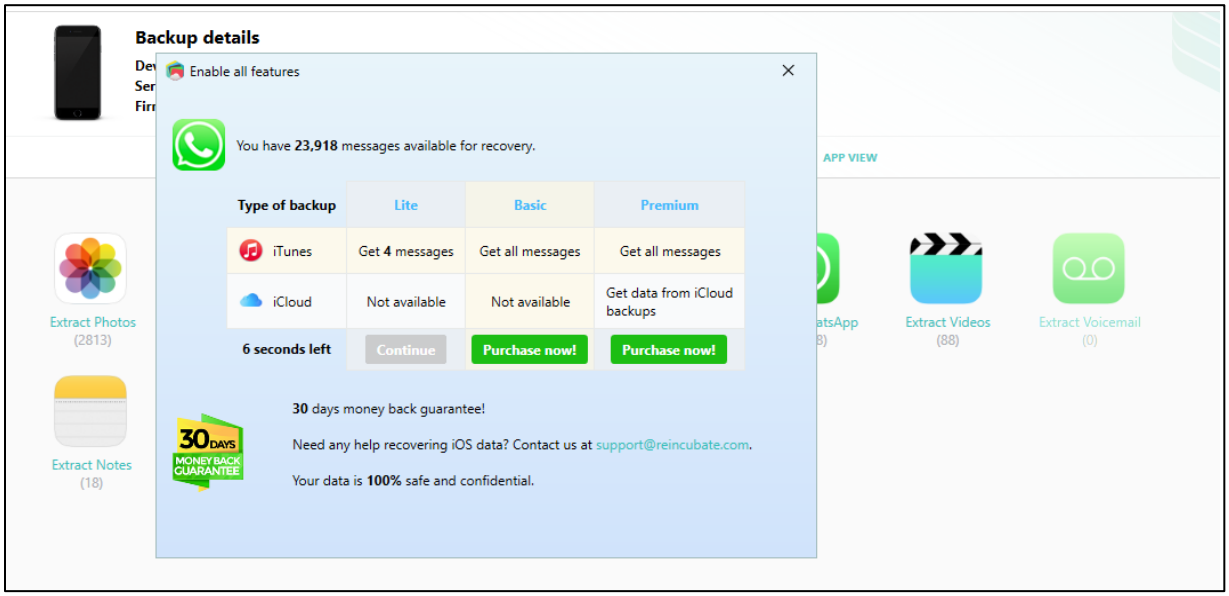


Figure 19.2: iPhone backup extractor (whatsapp messages save type).

Once we have come to this step of selecting the type of backup, lets us see what data from WhatsApp can be extractor. As soon as I have selected the type of backup it took me to a next stage of data form WhatsApp has been extracted and saved safely into the WhatsApp messenger files. These WhatsApp data are very valuable information in the eyes of law as evidences as they cannot be emended. iPhone backup extractor is the best and easily accessible application that it can been used by a common man as well.

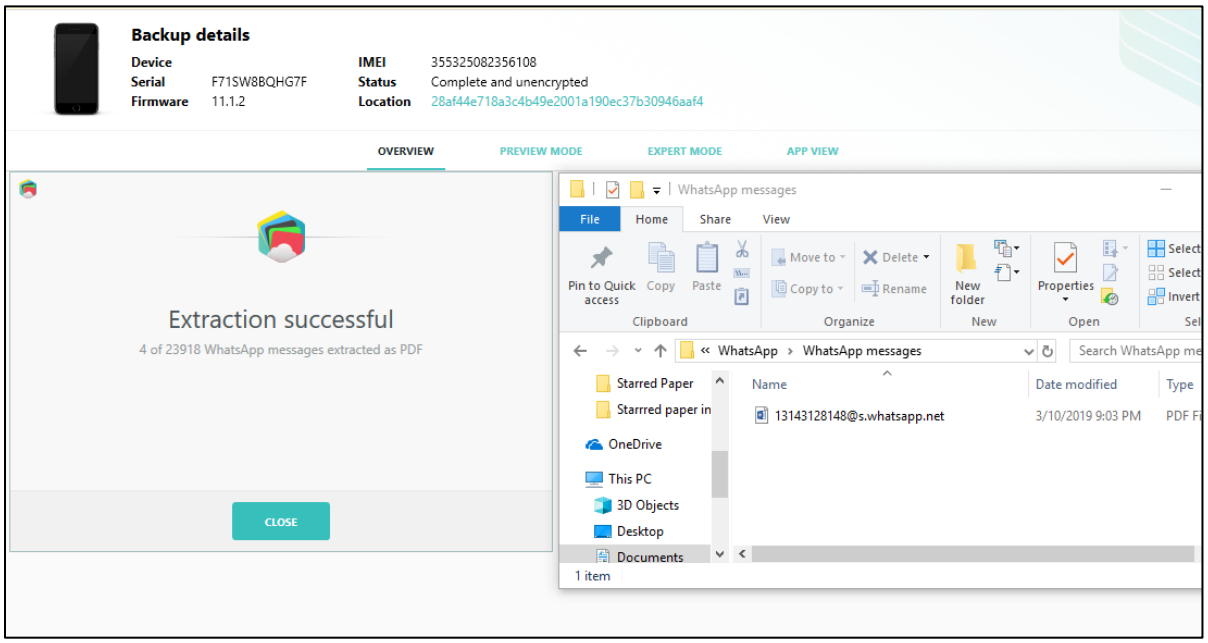


Figure 19.3: iPhone backup extractor (whatsapp saved folder).

Extracting evidential notes through iPhone backup extractor. Notes in iPhone can be saved in two forms, one form of saving Notes in iPhone is in the iCloud data storage and the second is in the iTunes backup. iCloud data can be accessible from anywhere in the world just by the iCloud User ID and Password. The most important point I need to mention here is that we can extract deleted iCloud Notes data through iPhone Backup Extractor software application. Let's begin with the process.

First the process of extraction of Notes data from iPhone starts from section 2 in iPhone Backup Extractor.

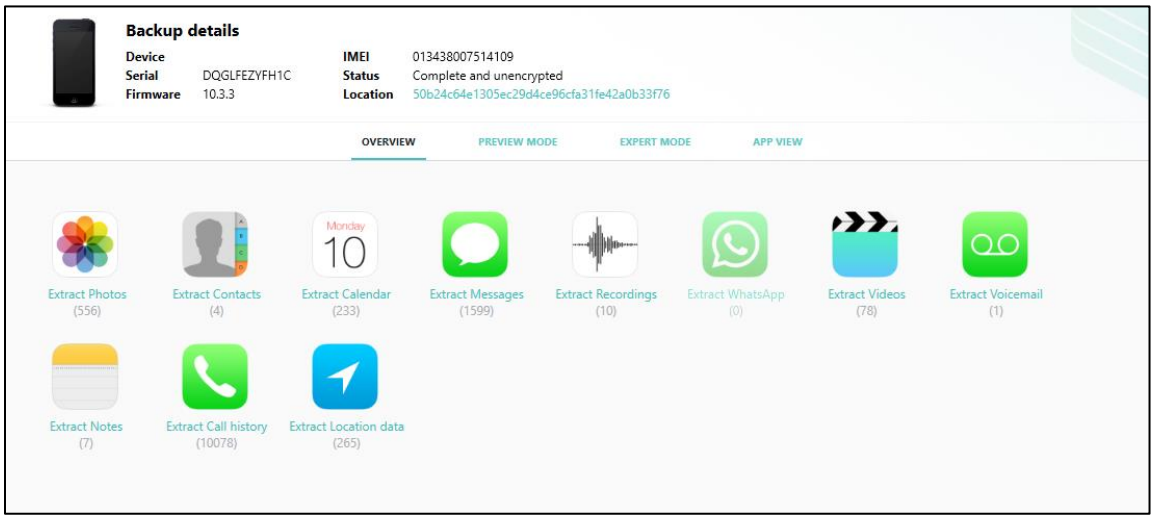


Figure 20: iPhone backup extractor (notes).

In the next step we select the notes icon in the section 2 of iPhone Backup Extractor and it would navigate us to type of data that we would like to select. As we are using the lite version and free software applications to extract data from iPhone (Extractor,B. E., 2018).

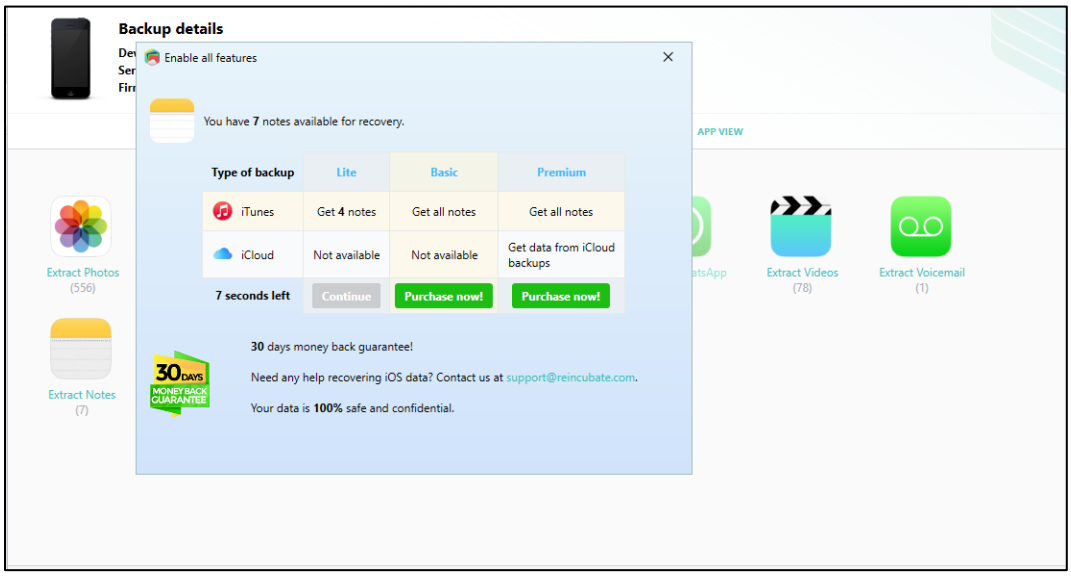


Figure 20.1: iPhone backup extractor (notes backup type).

After selecting the type of backup, we could see in the below image notes data has been extracted. In the below image we can see iPhone Notes and also iPhone Recently Deleted Notes.

These notes and recently deleted notes are very valuable data for forensic investigators for catching hold of the suspect.

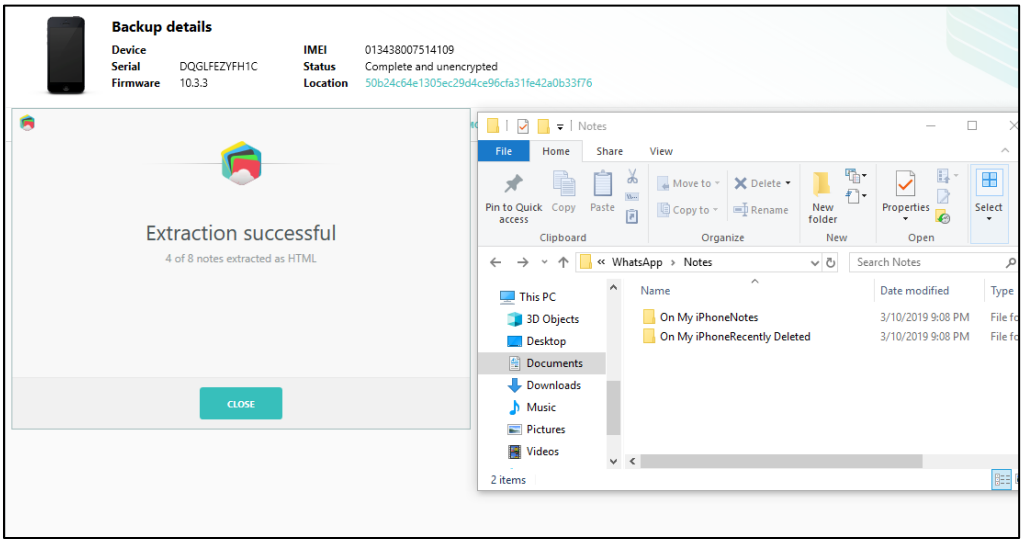


Figure 20.2: iPhone backup extractor (notes backup details)

Extracting evidential call history through iPhone backup extractor. Call history is a is nothing but the calls data like calls received, calls made and missed calls. This information can also ben extractor using iPhone backup Extractor software. let us go ahead and start with the process.

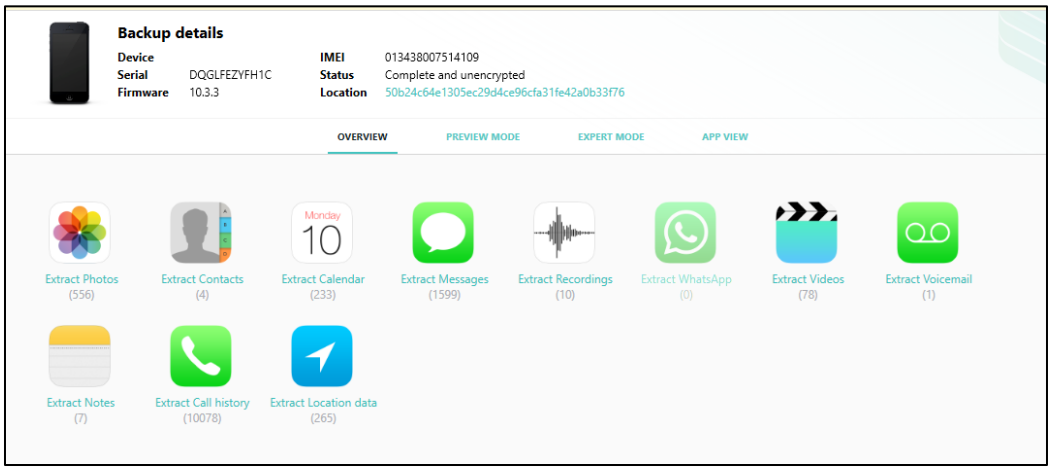


Figure 21: iPhone backup extractor (call history home page).

As we can see in the section 2 for iPhone Backup Extractor, we can find an icon with Call History. As we all know the call history is a very important data that we require to know if the suspect is in contact with any other person or how many people where involved also to know since when this planning was happening. Let us start the process of extracting call data from Apple iPhone (Extractor, B.E., 2018).

In the first place we need to select Call History icon in the iPhone Backup Extractor software application, this will take us to data backup screen.

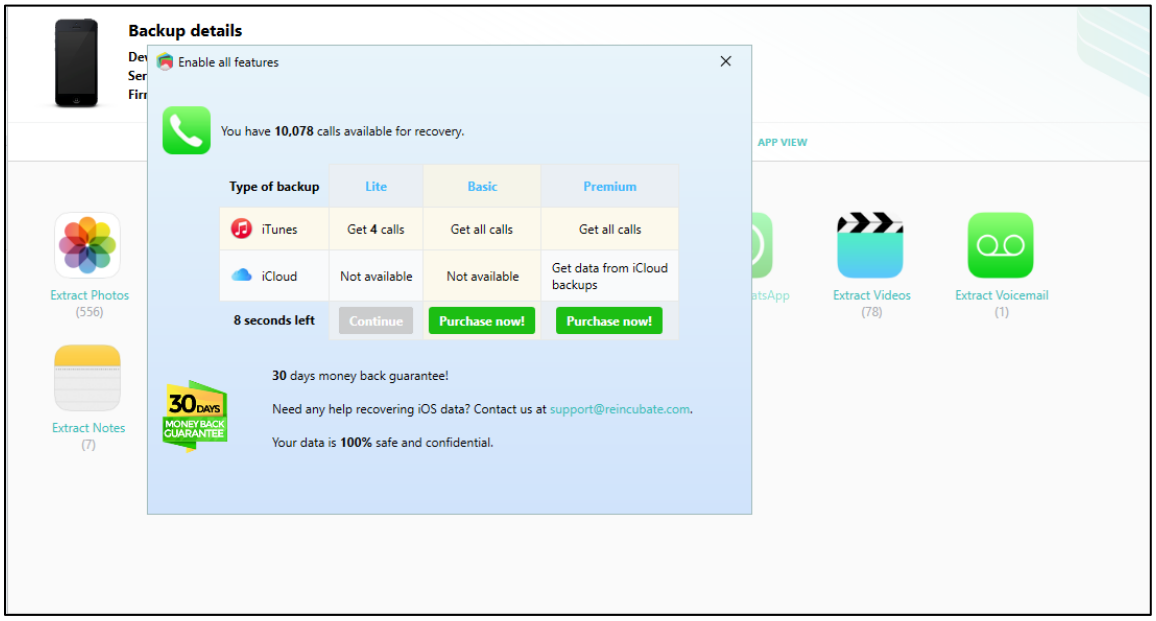


Figure 21.1: iPhone backup extractor (call history backup type).

In this step of data extraction we need to select the type of backup data we need to select, as we are using the lite version of data selection.

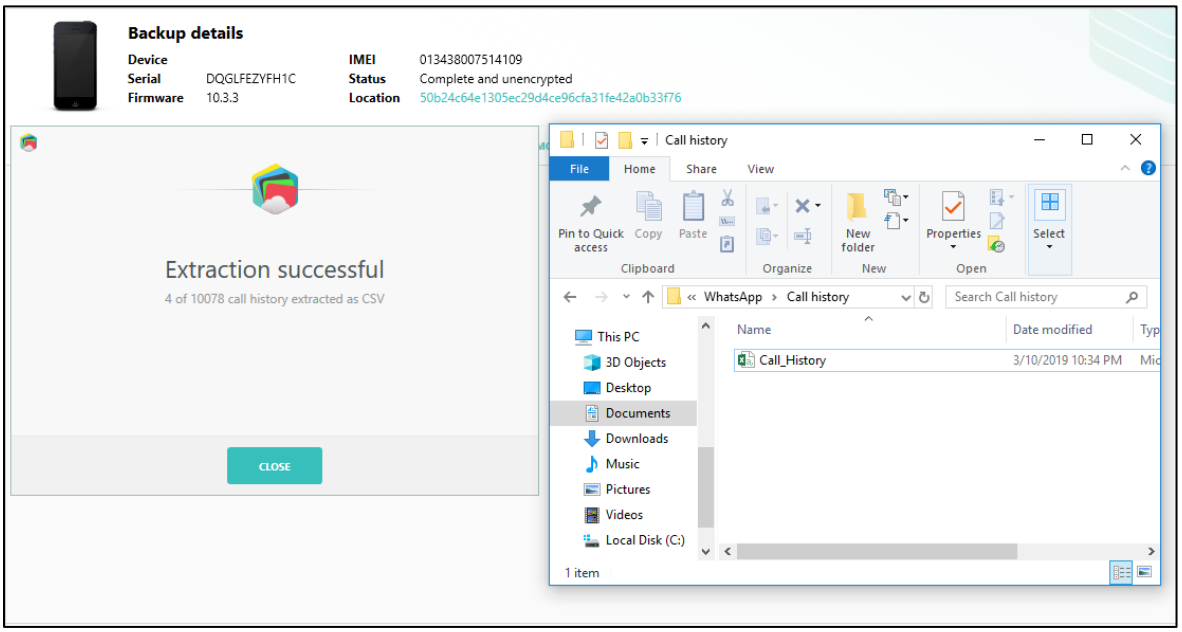


Figure 21.2: iPhone backup extractor (call history details).

In the above image we can see that data has been successfully extracted and it is also been saved in the backup files of iPhone Backup Extractor as an excel document (Extractor, B. E., 2018).

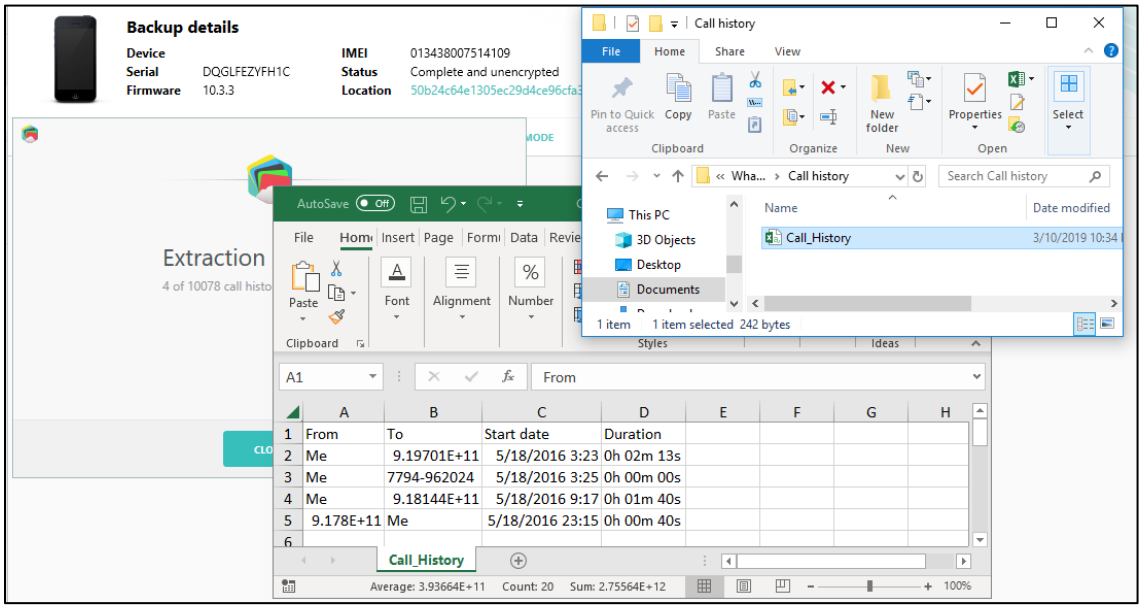


Figure 21.3: iPhone backup extractor (call history saved excel file).

As we can see in the above image how data has been stored in excel with from whom the call has been received (in this case it is me) and to which number also with date and time. This is very sensitive information to forensic investigators to catch hold of the suspect.

Extracting evidential location data through iPhone backup extractor. Location data is a valuable information that helps forensic investigators to catch hold of the suspect. We can extract location data through iPhone Backup Extractor. Let us go ahead and start the process of extraction of data.

Below is the home screen of iPhone Backup Extractor, let us go ahead and start the extraction process of Location Data.

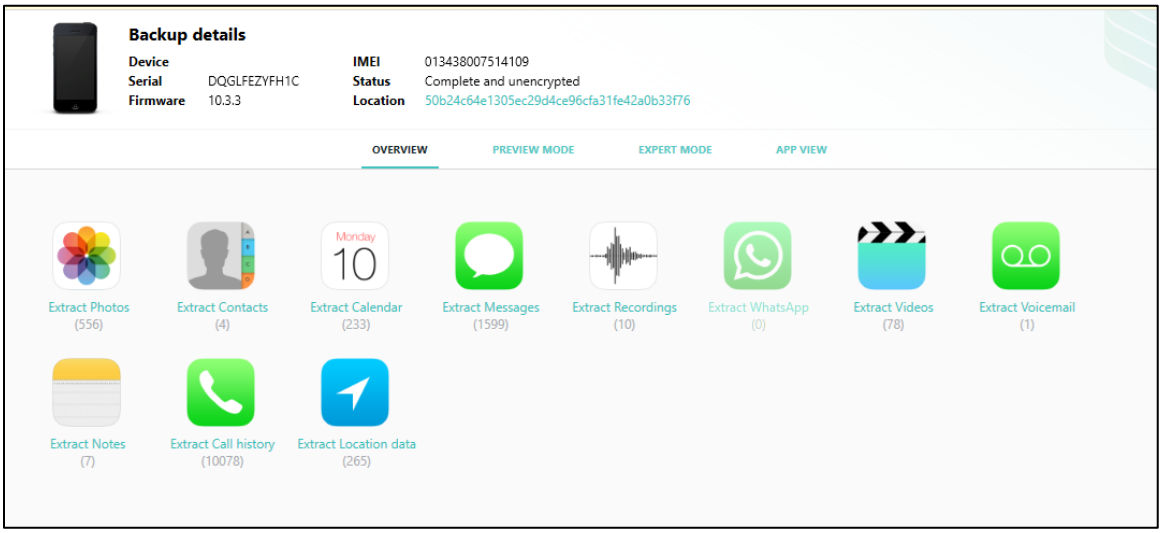


Figure 22: iPhone backup extractor (home page location data).

Above is the home screen of iPhone Backup Extractor and in the 3rd section of the application. We would find an application called Location Data and this will help us extract evidential data for location (Extractor, B. E., 2018).

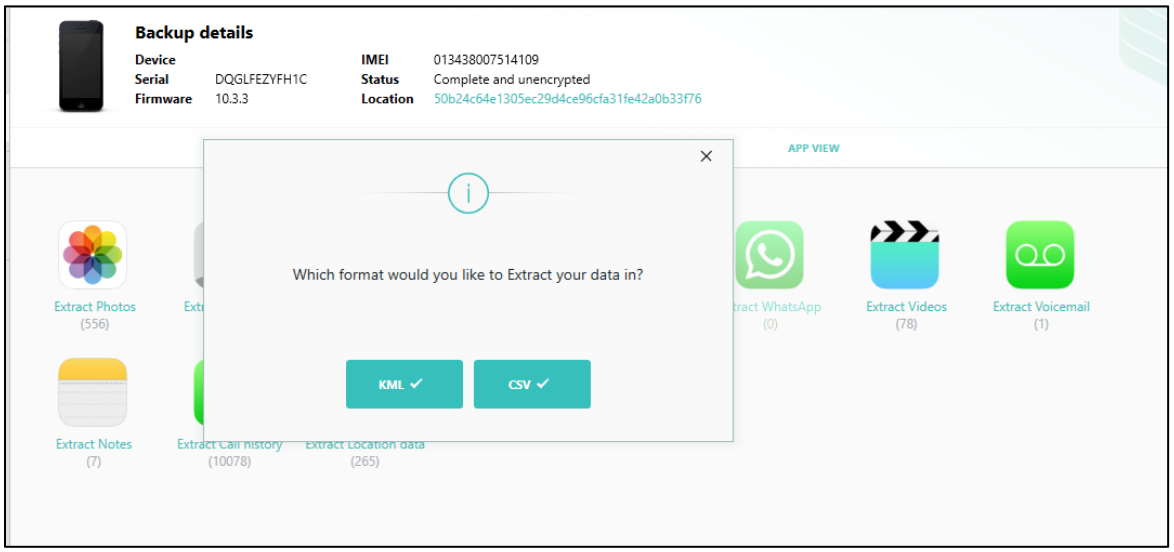


Figure 22.1: iPhone backup extractor (location data type of data format).

As we have selected location data application in iPhone backup extractor home page it will navigate us to the data saving method. In this way we can store the data according to our interest. I am using CSV method of saving data because it is easier to read and access.

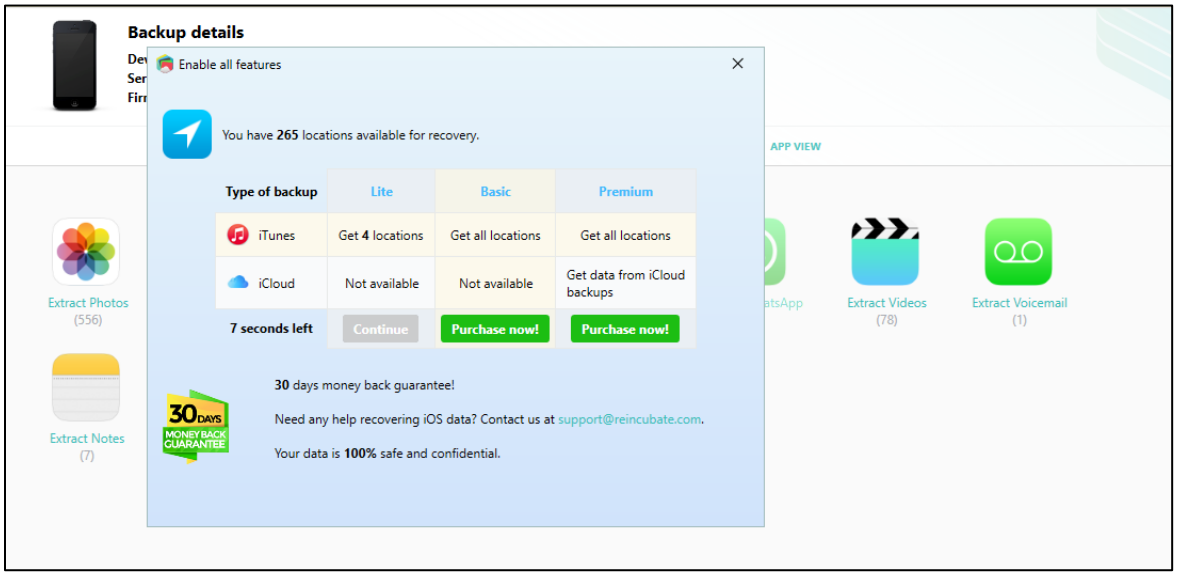


Figure 22.2: iPhone backup extractor (location data type of data storage).

In the above image we can see that iPhone Backup Extractor software application has the method of saving its extracted backup data. In this step we need to select the backup method. I am using lite and free method of data extraction for my paper (Extractor, B. E., 2018).

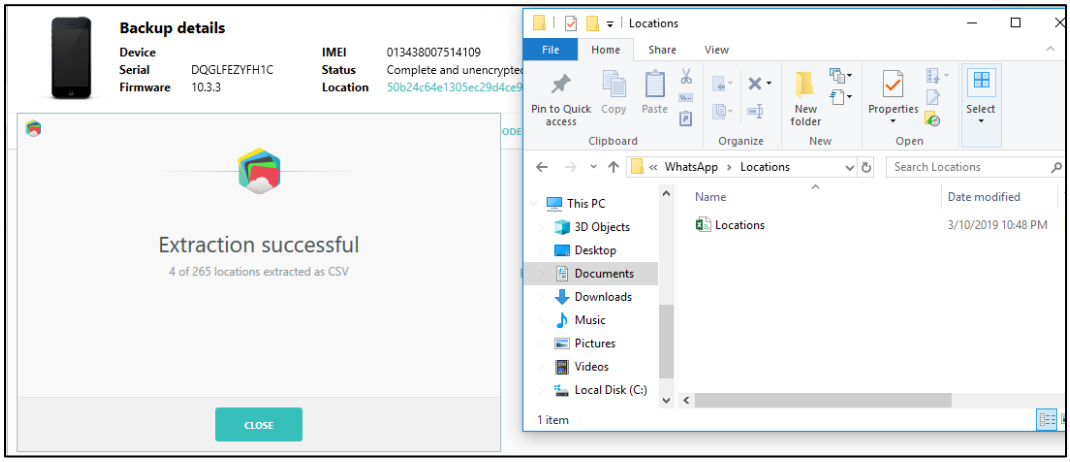


Figure 22.3: iPhone backup extractor (location data saved excel file).

As we select the type of backup we need it would scan the location data and it would start extracting data in to our local computer. Extracted data is been saved on to excel as show in the above image. Let us go ahead and open the excel sheet and see how location data looks like (Extractor, B. E., 2018).

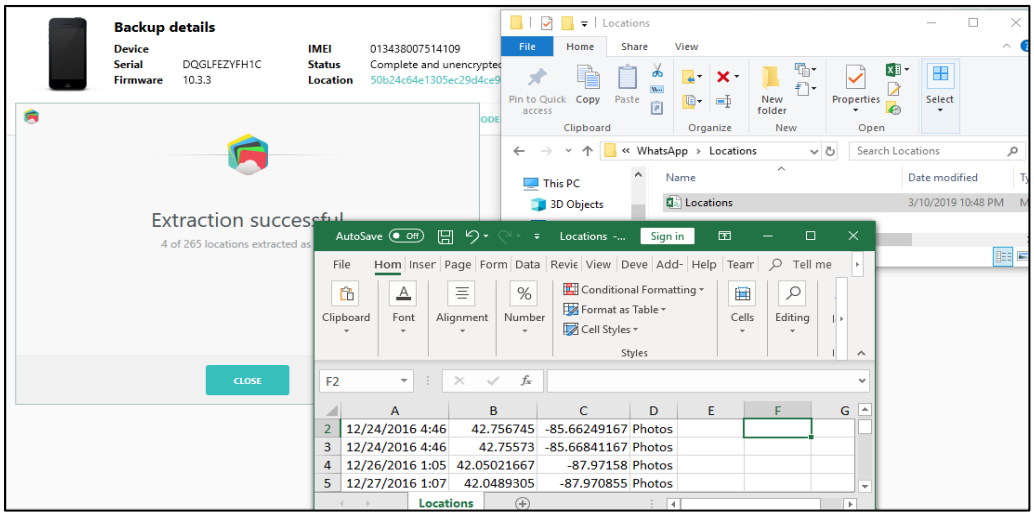


Figure 22.4: iPhone backup extractor (location data saved details).

This is the final and last step in location data extracting. As we can see in the above image how extracted location data looks like. iPhone Backup Extractor application is very user friendly as it can extract that is required for forensic data.

Data extraction process–iMyFone D-port. iMyFone D-Port is a third-party software application used for extracting evidential data for forensic examination purposes. This application is developed and maintained by third-party. As soon as I log in to the application, I see below application image to register or use free trial version.

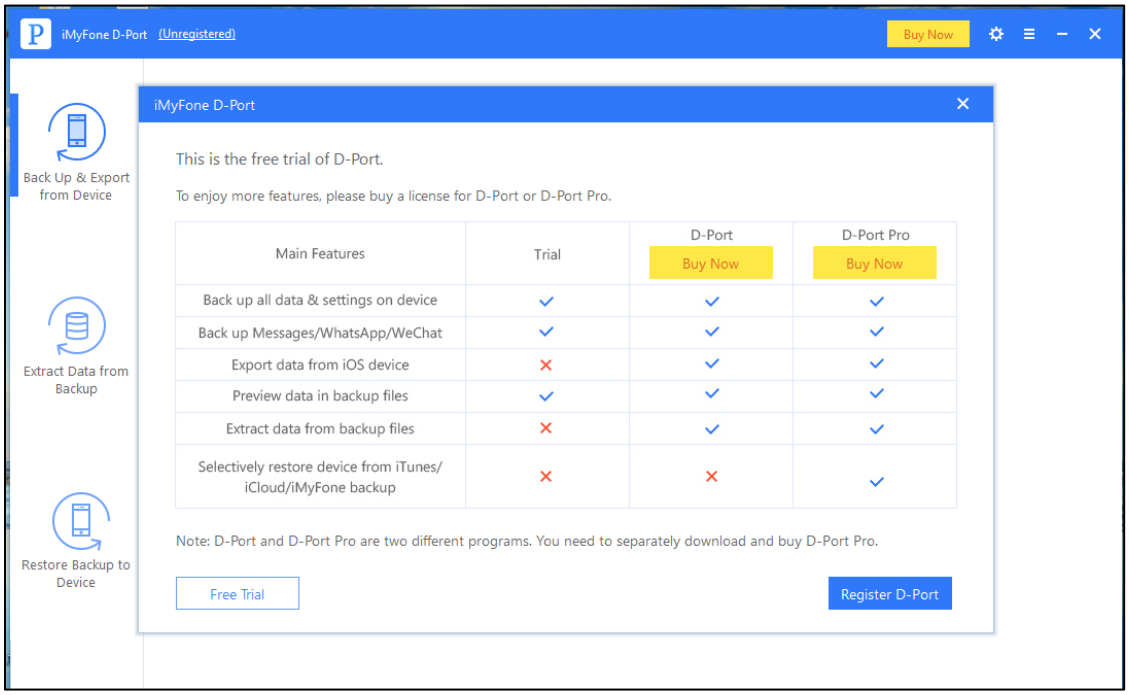


Figure 23: iMyFone backup extractor (free trail).

As I am using free trail version of iMyFone D-Port software for extracting evidential data. Let us go ahead and start the process of extracting data.

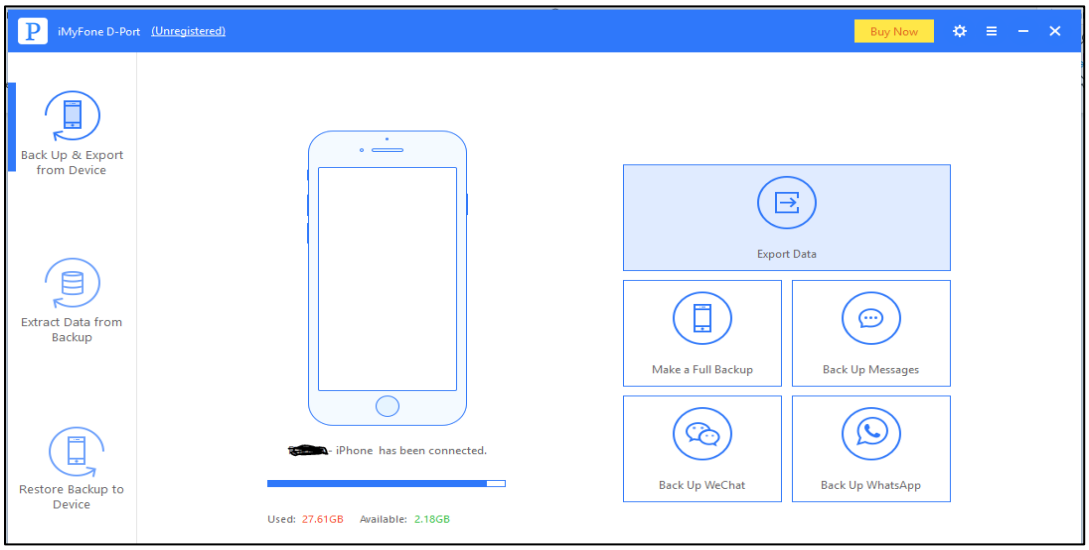


Figure 23.1: iMyFone backup extractor (home page).

As I connect Apple iPhone to the computer, I see software application has detected the phone and downloaded backup files. In the above home screen, we can get some basic information on what kind of backup's we can do and how much data is stored in the phone also its free space. Let us start the process of extraction (imyfone-Backup Application, 2018).

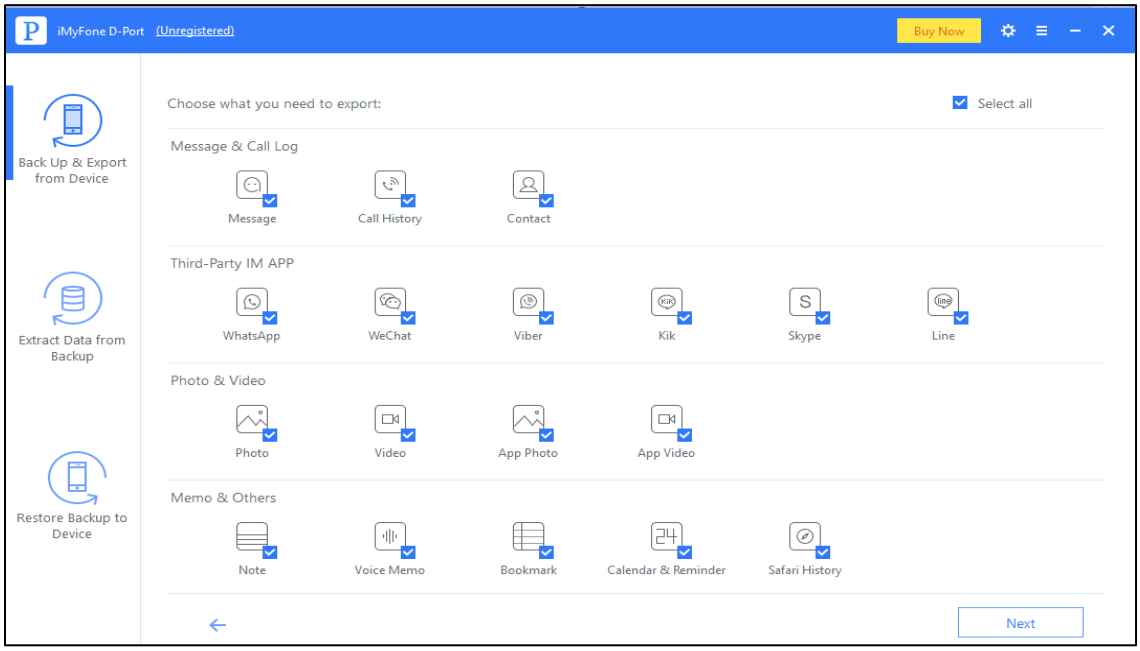


Figure 23.2: iMyFone backup extractor (data extraction screen).

From the above image we can see that there is lot of data that we can extract at a time just by selecting that information what we require. Lets us start with the data extraction of call logs (imyfone-Backup Application, 2018).

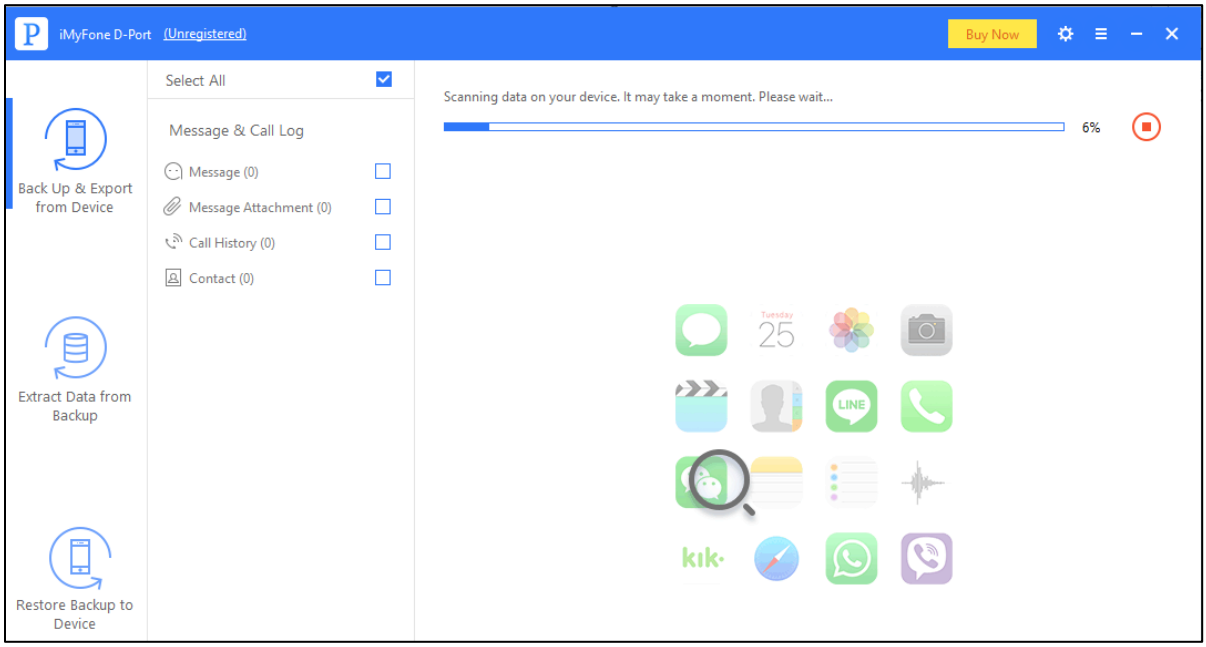


Figure 23.3: iMyFone backup extractor (data extraction method).

I have unselected all the unnecessary applications which does not give me valuable information and only picked up applications which are required for my forensic examination.

Extracting evidential message data through iMyFone D-port. As I have been discussing in the previous chapters that messages are one of the most valuable information that we require for forensic evidences. If you see the below image we can see that in just one click all the messages have been extracted.

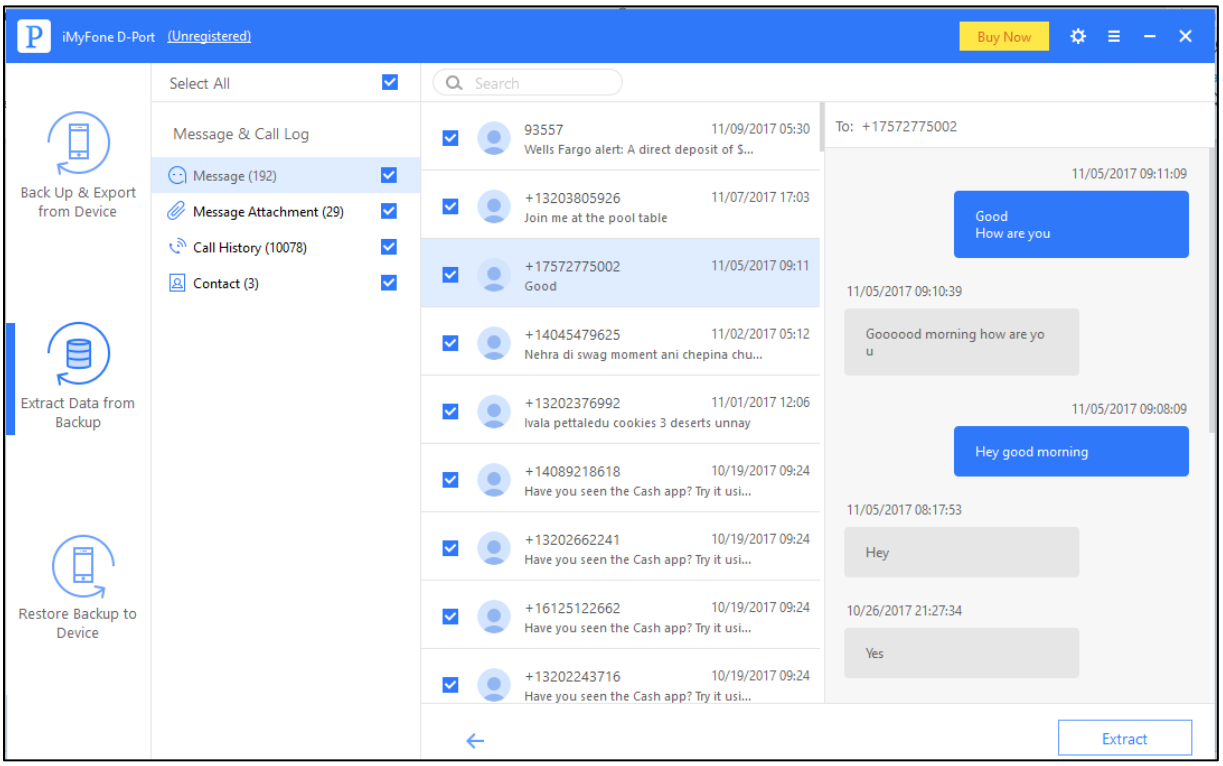


Figure 24: iMyFone backup extractor (data extraction method).

In the above image we can see the messages and images that has been exchanged through messages as well. When I have tried to export these messages in to the computer it is not allowing as I am using the free trail version. But we can very clearly read the messages in the application itself. This makes the life of the forensic investigators easy as they do not have to go through all the unnecessary information (imyfone-Backup Application, 2018).

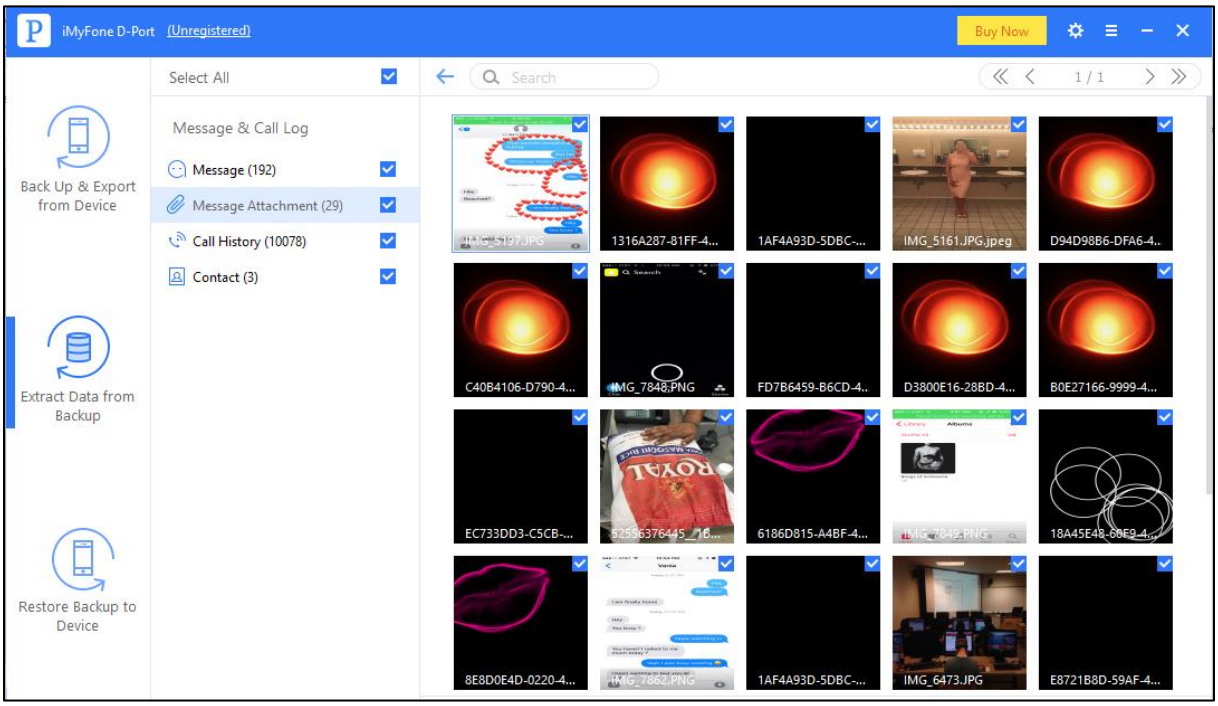


Figure 24.1: Images transferred through messages.

In the next step I have looked in to the images that have been exchanged through messages. This is a very sensitive information that would be very helpful to forensic investigators for their examination.

Extracting evidential call history through iMyFone D-port. As discussed in our previous chapter, we know that importance of Call History data. In Call History data the information we would be finding is incoming call, Outgoing call and missed calls. Look at this information forensic investigator will check who was the suspect regularly in contact with. Let us start with the process of extracting call history data.

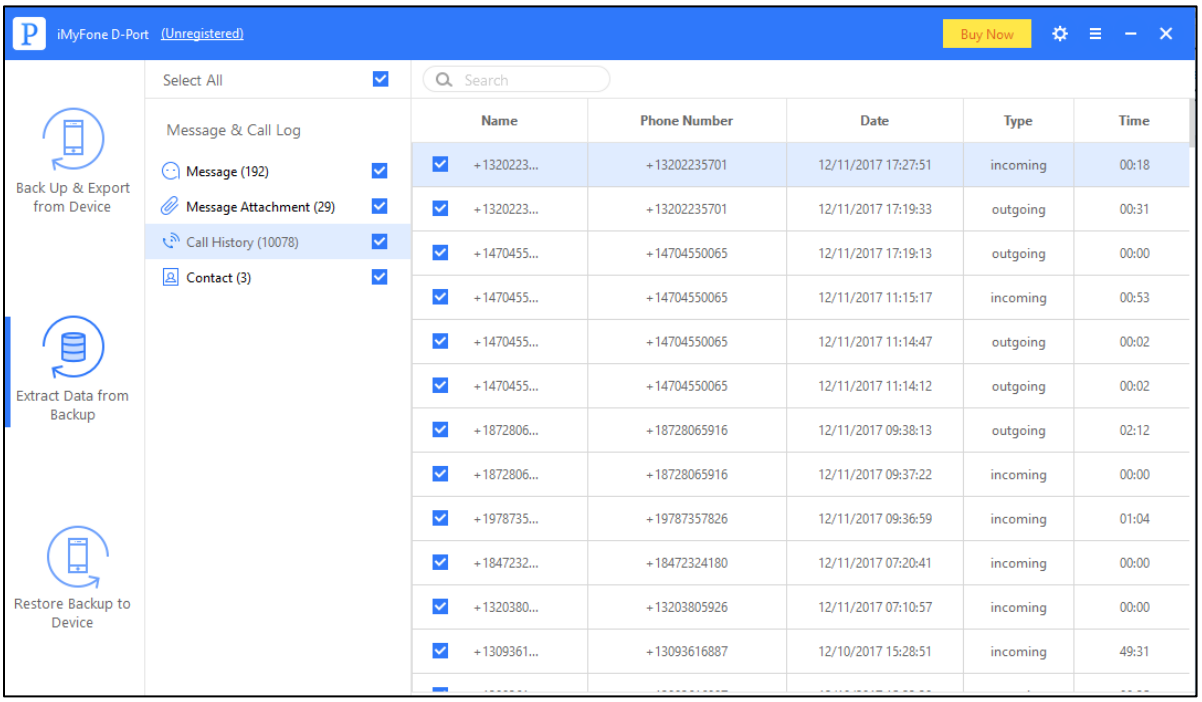


Figure 25: Call history data.

If you observe in the above image call history data is been properly been arranged the most recent once. As we can see that there are five columns and every column is providing sensitive information. Let us start discussing the columns one by one. First is the name column there is proving us with the name of the person called. Second is the phone number column which help us to tract the suspect nest us the time and data and then is the history column which tells us if the call was incoming or outgoing. Last but not the least is the duration column, this column explains us how long the call was been.

Extracting evidential contact through iMyFone D-port. As discussed in our previous chapter, we know that importance of Contacts. In Contact data the information we would be finding is saved contacts in the phone. Looking at this information forensic investigator can get the people with whom the suspect is in contact with. Let us go ahead and start extracting contact information (imyfone-Backup Application, 2018).

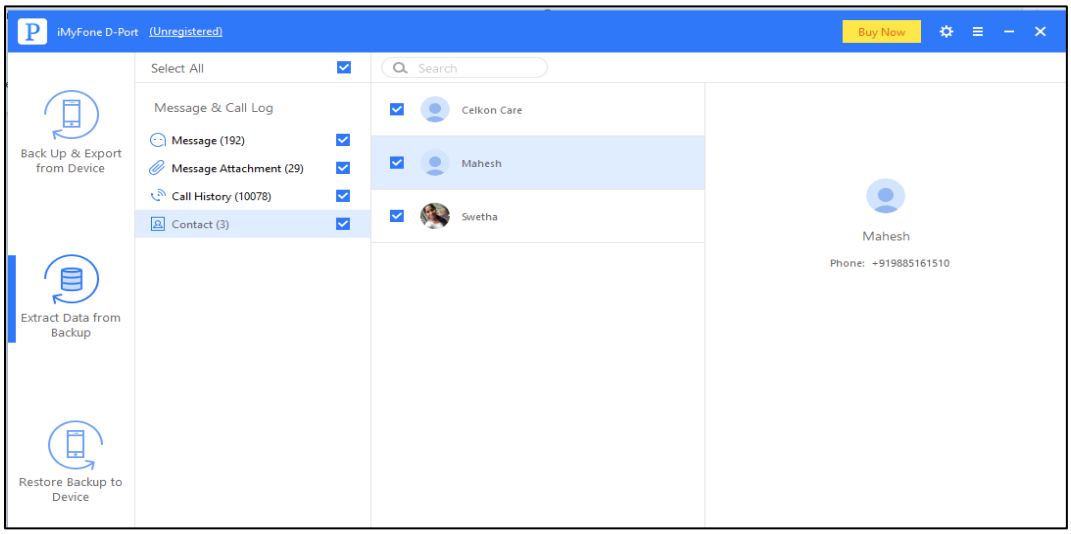


Figure 26: Contact information.

In the above Figure 25 we can see that there are three contacts in the phone that are stored, these three contacts have been extracted. This was a very easy and effective procedure of extracting contact information through iMyFone D-Port (imyfone-Backup Application, 2018).

Extracting whatsapp data through iMyFone D-port. WhatsApp data is very valuable information. Let us go ahead and extract WhatsApp data through iMyFone D-Port.

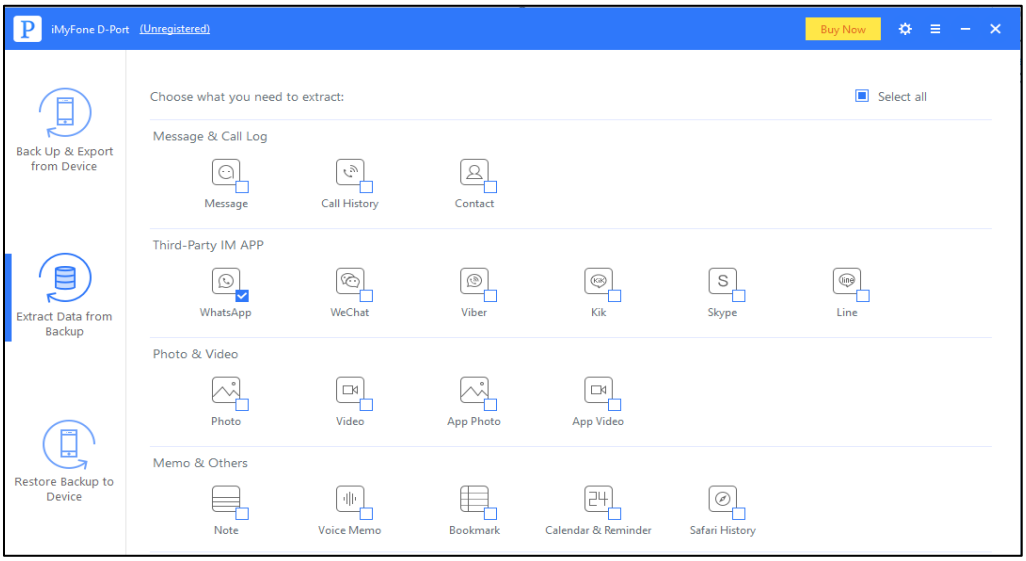


Figure 27: WhatsApp data (third-party application).

In the above image I have unchecked rest of the applications and only selected WhatsApp Data because that is the only data that contains sensitive data which would be helpful to forensic investigators (imyfone-Backup Application, 2018).

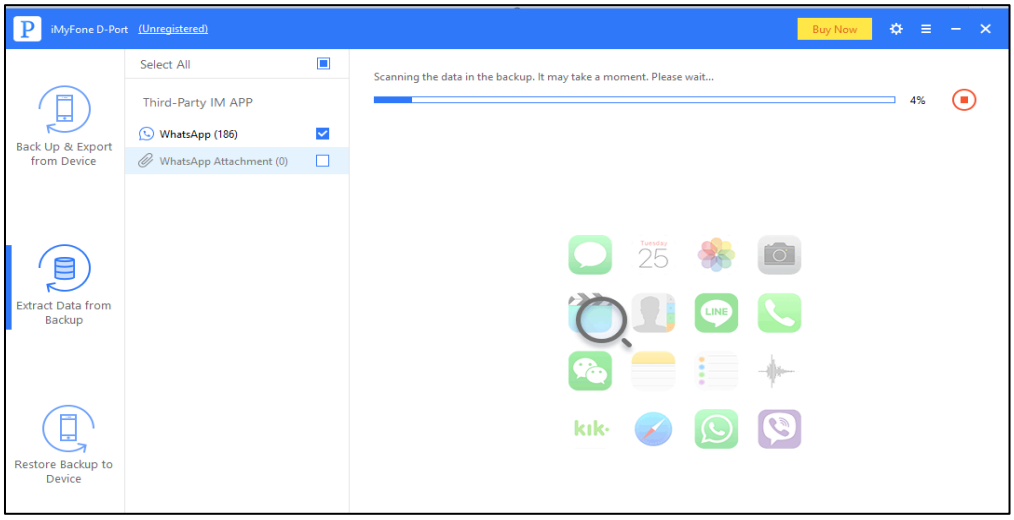


Figure 27.1: WhatsApp data extraction process.

In the above Figure 27.1 we can see that scanning process has been started and it is quite time taking but very essential data it is providing (imyfone-Backup Application, 2018).

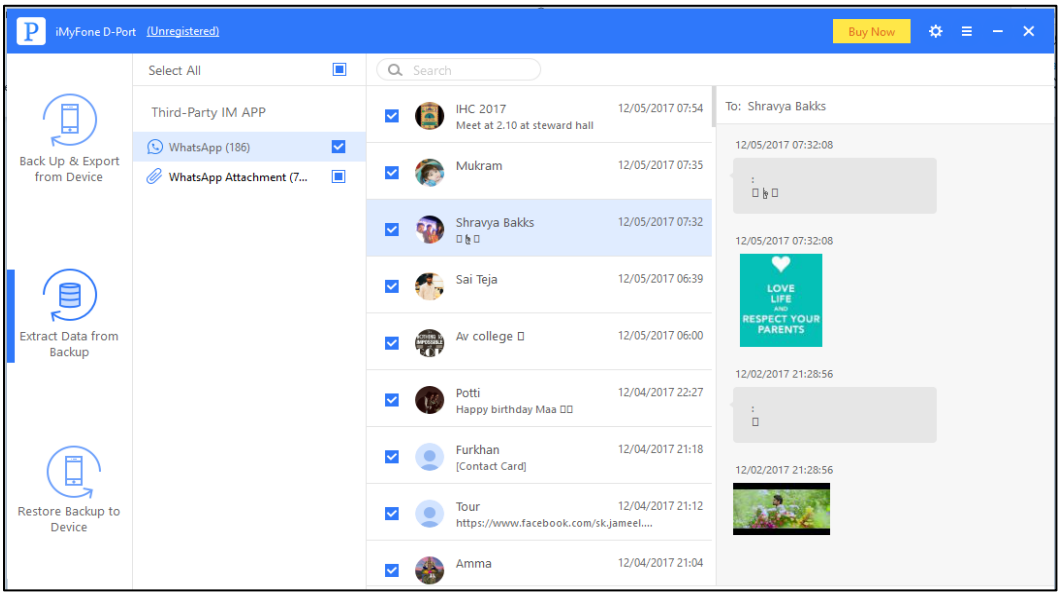


Figure 27.2: WhatsApp data extraction process.

We were successfully been able to extract WhatsApp data though iMyFone D-Port software application. If we look closely under the WhatsApp at the top on the image, we can also see the images that have been exchanged through WhatsApp. The only disadvantage we have is that we are unable to import that data in to our computer as we are using the free trial version.

Extracting photos data through iMyFone D-port. Photos and videos contain sensitive information, and these can be extracted by iMyFone D-Port software application. Lets us go ahead and extract the data.

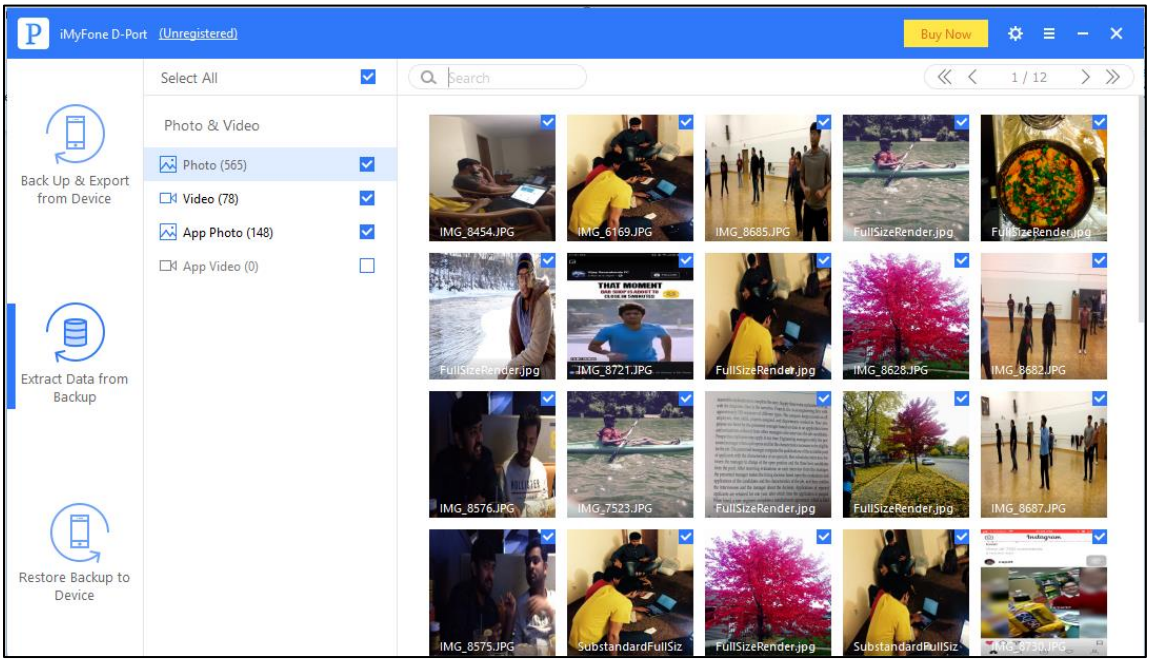


Figure 28: iMyFone D-port–photos and videos.

As we can see in the above image 28 photos and videos can be viewed and they cannot be extracted to local computer (imyfone-Backup Application, 2018).

Extracting photos data through iMyFone D-port. Videos provide more sensitive information then photos as photos can be morphed. Videos provide us with the exact suspect. Let's us go ahead and extract the data.

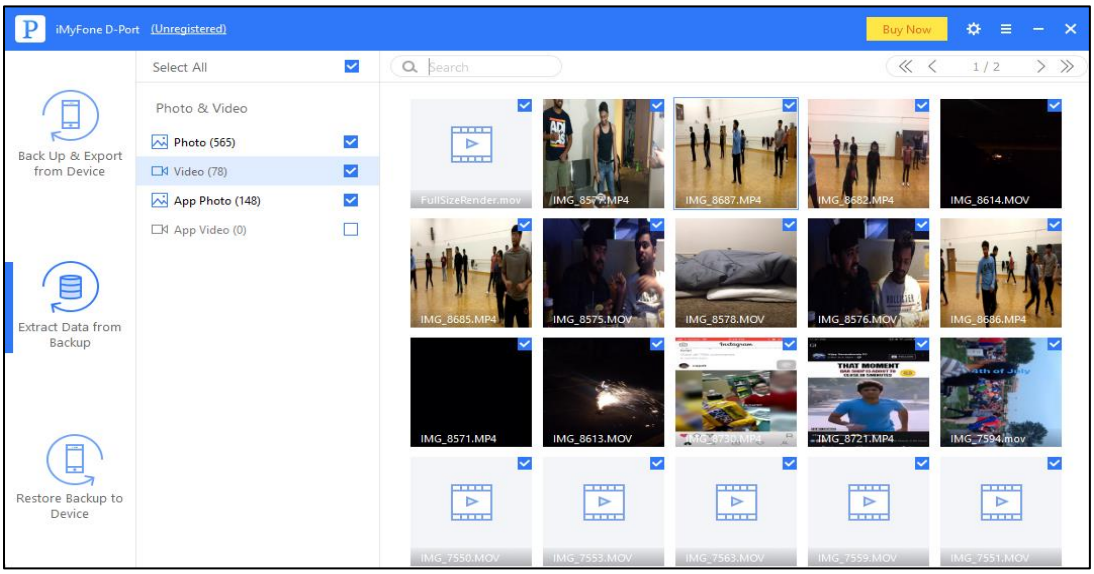


Figure 29: iMyFone D-port–videos.

In the above Figure 29 we can see that videos have been viewed and the only disadvantage of this application is that data cannot be extracted on your computer. They can only be viewed.

Extracting app data through iMyFone D-port. Once we connect experimental iPhone to iMyFone D-Port data is been backup in to the software and it is stored in the application. These third-party applications also stored some informative data like photos, videos, notes and messages. Let us extract App data of experimental iPhone (imyfone-Backup Application, 2018).

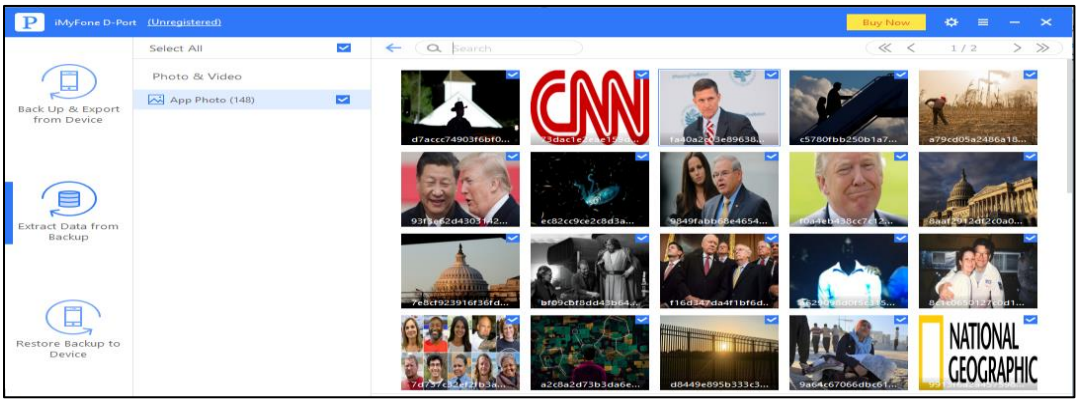


Figure 30: iMyFone D-port–app data.

As we can see from the above picture that App Data has been extracted on to the application. Looking at this data forensic investigators can catch the suspect.

Extracting notes through iMyFone D-port. Notes is the location in the iPhone where most of user id's and passwords have been stored as it is keep a track of data (imyfone-Backup Application, 2018).

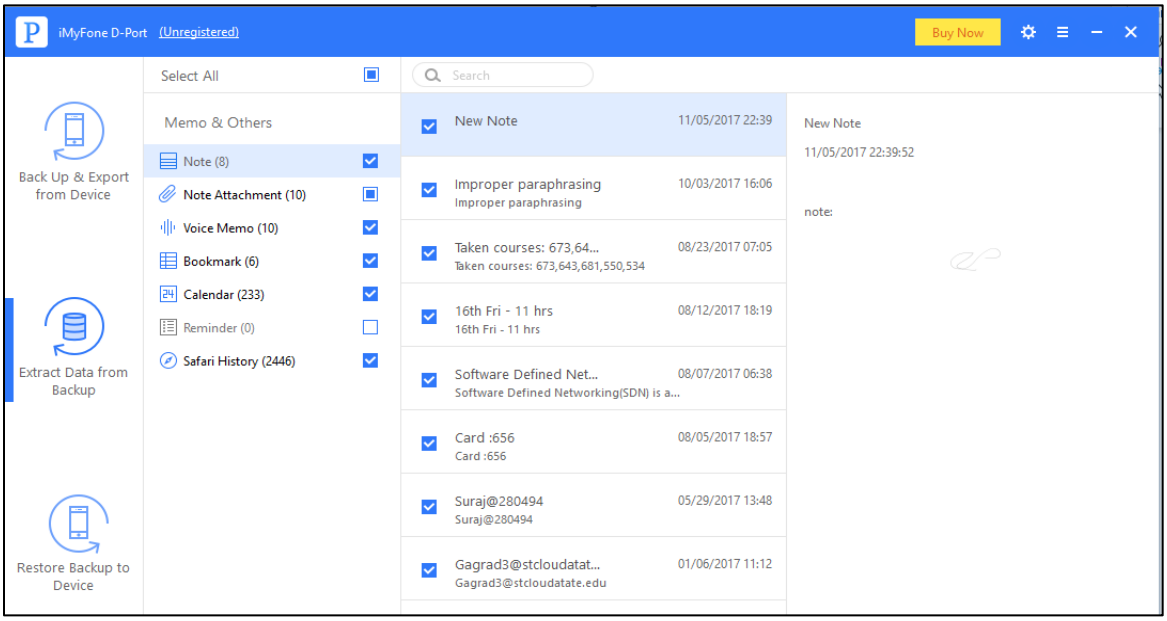


Figure 31: iMyFone D-port–notes.

We can extract notes data to in the application backup storage data. This is useful to forensic investigators (imyfone-Backup Application, 2018).

Extracting notes attachments through iMyFone D-port. Notes attachment is the location in the iPhone where most of Photos and screen shorts have been stored as it is keeping a track of data.

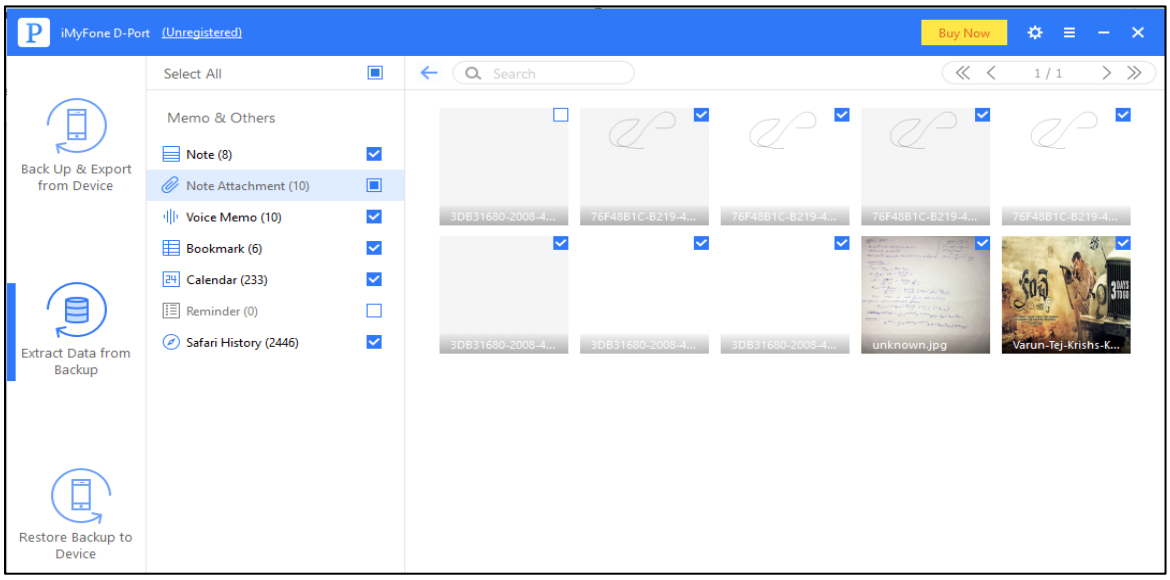


Figure 32: iMyFone D-port–notes attachments.

We can extract notes attachment data to in the application backup storage data. This is useful to forensic investigators.

Extracting voice recording through iMyFone D-port. Recoding provide sensitive information. Let's extract voice recording using iMyFone D-Port and see what results we get.

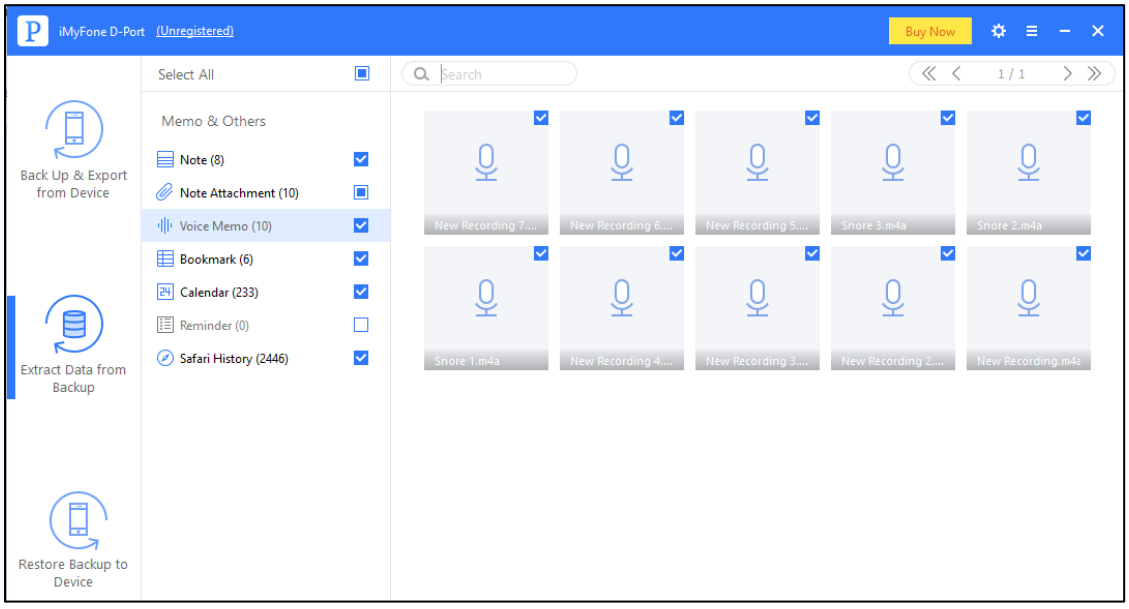


Figure 33: iMyFone D-port–voice recordings.

Extracting book mark through iMyFone D-port. Book Marks are the websites that a person would be asking on to his web-browser as it is easy for him or her to assess it every time. This also contains sensitive data. Forensic investigators would also look to this data to see what web sites are saved in Book Mark data. Let's go ahead and extract Book Mark Data using iMyFone D-Port.

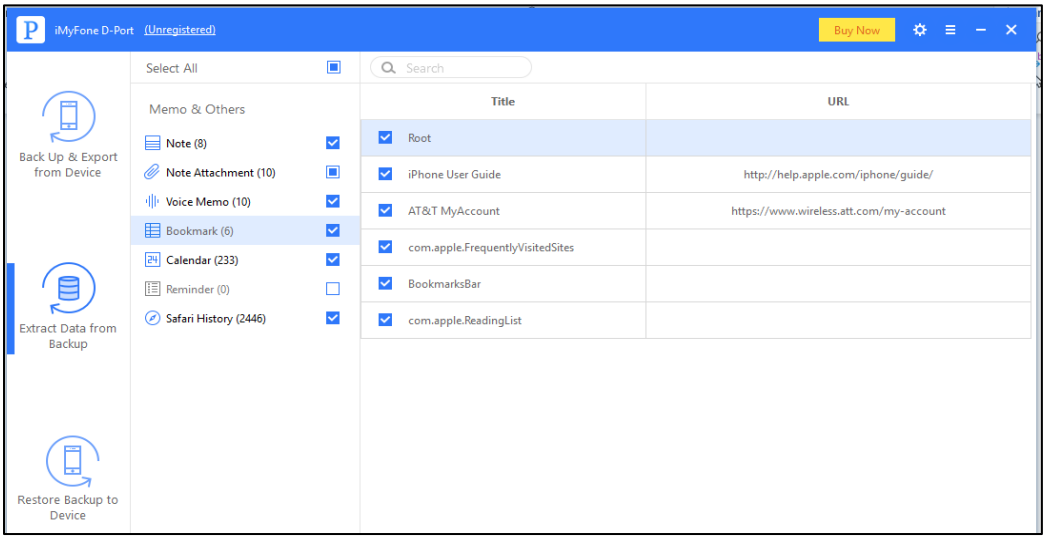


Figure 34: iMyFone D-port–book mark.

If we look at the left side of the above screen short we can observe that Book Marked web site information can be captured and look at this forensic investigators can catch the suspect.

Extracting calendar data through iMyFone D-port. Calendar Data is that data that can be stored and notes on that particular data, if a suspect was to commit any crime, he or she might save the date and a short note in the calendar data. Let's go ahead and extract Calendar data using iMyFone D-Port.

After backing up the iPhone data in to the iMyFone D-Port application. All the data is stored into the software, we just need to select that data whatever we required and results are popped out (imyfone-Backup Application, 2018).

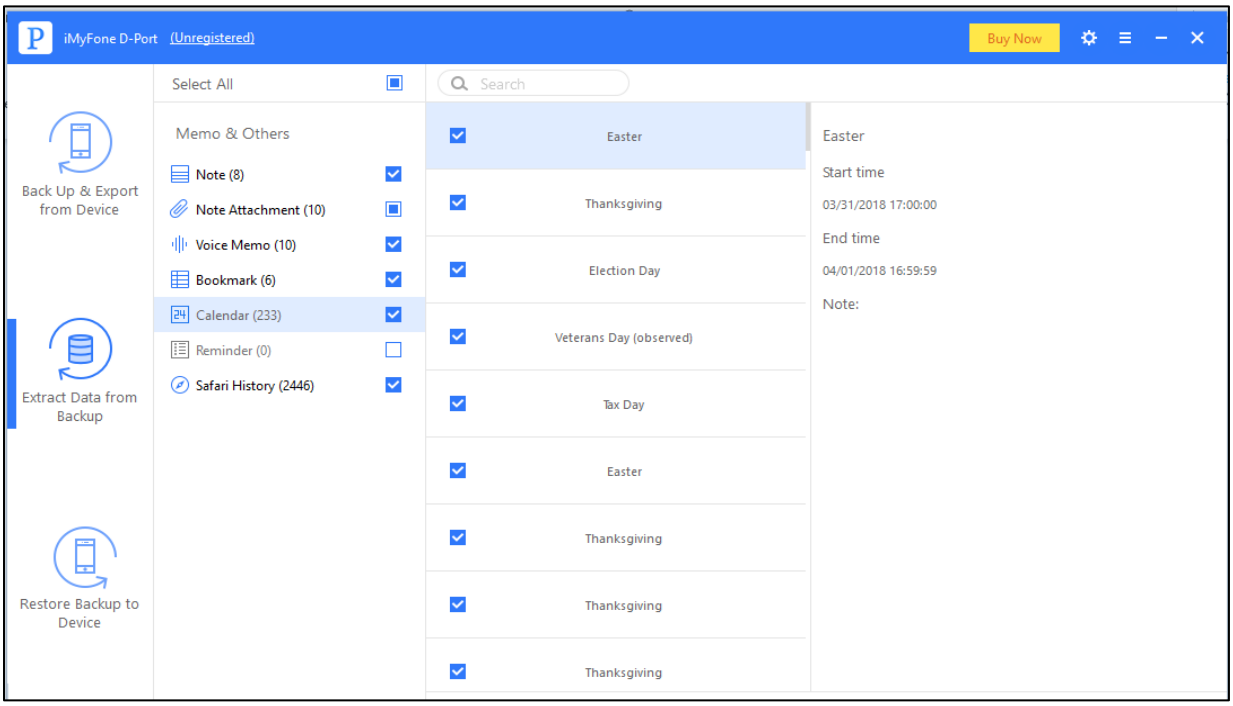


Figure 34.1: iMyFone D-port–calendar.

As you could see in the above image I have selected the calendar data and it has provided me the dates and also a short notes about that particular date.

Extracting Safari History through iMyFone D-port. Safari History is a very valuable data that needs to investigate the examination phone has it contacts much of the suspicious data. This is a search engine that provides results for your questions or doubts. This information is very important.

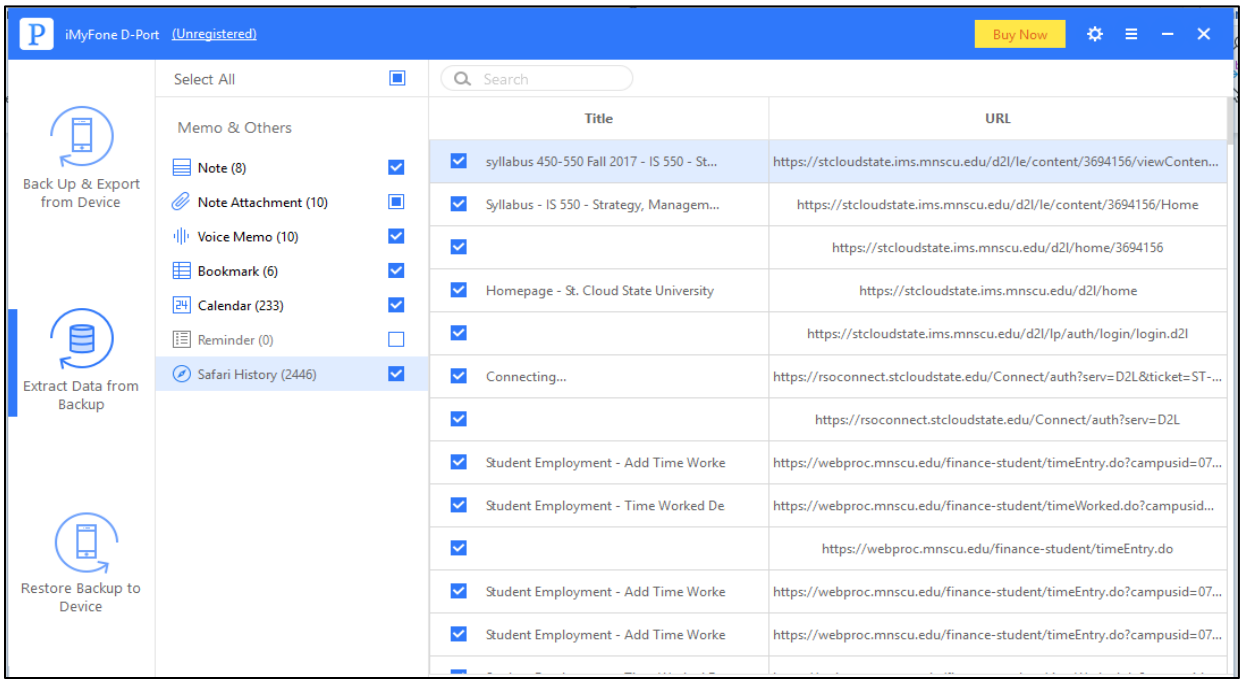


Figure 35: iMyFone D-port–Safari History.

As we can see in the above picture safari history can be extracted using iMyFone D-Port software application. This is a very crucial information that helps forensic investigators to catch the suspect (imyfone - Backup Application , 2018).

Summary

In this chapter we have learnt the different methods of data extracting and how data needs to be extracted using iTunes, iPhone Backup Exporter and the final one iMyFone D-Port software applications. This was a very interesting lesson to learn and experience.

Chapter 5: Results, Conclusion and Recommendations

Introduction

This is last chapter of the paper. In this section of the chapter we would be comparing the extracted results from Apple iPhone. For the purposes of extraction, I have used iTunes, iPhone Backup Extractor and iMyFone D-Port software application. Comparison of these extracted data is necessary as some of the software give very informative data and some pull just basic information which is not much helpful.

Results

Extraction of evidential data for iPhone forensics is very necessary and useful in this current generation as every second person has an Apple iPhone. For this experimental paper I have used two Apple iPhone. The iPhone I have used are Apple iPhone 5 with an IOS software version on 11.2.1 and Apple iPhone 7 with an IOS software version of 12.1.4.

In the process of extracting evidential data I have used three software which are iTunes, iPhone Backup Extractor and iMyFone D-Port. These three software applications are very effective and extract useful data.

Let us start our discuss with first application which is iTunes. iTunes is the software application that is been developed and maintained by Apple.com. This is an internal software application, as per my experiment of extracting sensitive data from iPhone through iTunes I could find out some interesting data like Phone number, IMEI number, Serial number, Photos, Videos, voice recordings, Phone recordings. iTunes is very effective software which has provided evidential data.

In the second place I have used iPhone Backup Extractor software application for extracting evidential data. This is a third-party software that is been developed and maintained

by itself. iPhone Backup Extractor is free access application and it has extracted some valuable information for my examination like Photos, Videos, voice recordings, Phone recordings, Notes, Messages, WhatsApp and Location data. When compared to iTunes according to my understand iPhone Backup Extractor has extracted more sensitive information.

The only constrain regarding this application is that to extract full or semi-partial data we need to buy that software. For this paper I have used the basic plan of the software which is Lite version. It has extracted minimal amount of data, but it is very informative.

The last and final software that I have used for my experiment is iMyFone D-Port. This is also a third-party application which is very effective in extracting data.

- How to apply forensics on Apple iPhone?

  There are multiple methods and ways to apply forensics on Apple iPhone, as we have seen in our above chapters different software applications have given different results.

- What are the Tools and Technology need to perform Forensics on iPhone?

  Tools I have used in my study of forensic on iPhone are hardware (iPhone, Cable, Laptop) and Software Technology (iTunes, iPhone Backup Extractor and iMyFone D-port)

- What are the challenges faced by forensics investigators while examining iPhone?

  Challenges that I have faced while performing iPhone forensics in that phone keeps getting switched off and the IOS software keeps on updating and according to phone software I need to update the software's.

- What are the problems faced while retrieving data from iPhone.

  iPhone is very secured device and it is very difficult for the forensic investigators to extract evidential data. To analyze the problems faced while retrieving the data from

iPhone many does not provide key information that we are looking for. Only way to get the key information is just keep looking for the evidential data.

- What data needs to needs to be extracted?

  In Apple iPhone there lots junk data. The data we are only interested, and we are looking for is Photos, Videos, Messages, Voice recordings, Call History, WhatsApp data, Notes, Safari History.

Conclusion

Apple iPhone is smart device with lot of fire walls protecting its data. It was quite difficult to extract data from iPhone. As I have been successful is extracting and viewing forensic data using different methodologies. Most of the software applications has directed me to the same forensic data However, some of the application could not extract limited data and some out extract complete data.

In my first data extraction procedure I have used iTunes software which is developed, maintained and licensed by Apple.com. This software application has extracted some valuable information like Phone number, IMEI number, Service number. This information could not be extracted by other two applications.

In the second place I have used iPhone Backup Extracted for extracting data from iPhone. This is wonderful application that could extract Messages, Notes and Voice Recordings. The only drawback for this application was it could not yield us with limited data as we have used free version to extract data.

The last and final software application that I have used is iMyFone D-Port to extract data from iPhone. This is perfect application to extract evidential data from iPhone. This application has extracted all the information that other two applications have extracted and also part from

then it has also provided some extract data like Book Mark data, Safari History, WhatsApp Data, Notes attachments. The only drawback for this application is that we could not extract data from its backup as we have used the trail version of this application.

As a forensic investigator evidential information is very required to catch hold of the suspect. We need to keep on looking for evidential data till we find that data. Some applications provide valuable information. I would conclude this paper by saying keep looking for evidences till you find.

Further Work

Apple is the number one company in smart phone inductor and keep up its position it keeps on add new feathers and software upgrades to its products. Through iPhone 5S Apple has introduced finger print unlocking technology, iPhone can also be unlocked through thumb impression and recently through iPhone 10 Apple has brought a new amazing feature called Face ID detector. This is an amazing feature, just by looking at the phone the device would get unlocked. In my further study I would like to crack the method of unlocking an iPhone without finger print or face id and extract data from it.

References

Apple-iPhones. (2018, January 18). *Apple*. Retrieved from iPhones: https://www.apple.com/

biography-Steve Paul Jobs. (2018, March 15). Steve Paul Jobs. Retrieved from biography: https://www.biography.com/people/steve-jobs-9354805

Cell Phone and Tablet Forensics. (2018, February 17). *Capitol-digital.com.* Retrieved from phone-forensics: https://capitol-digital.com/califorensics/cell-phone-forensics/

Digital Forensics. (2018, January 13). *Digitalforensics.com*. Retrieved from digital-forensics: https://www.digitalforensics.com/digital-forensics/cell-phone-forensics?utm_source=google&utm_term=cell%20phone%20forensics&utm_campaign=MN-DF&gclid=EAIaIQobChMIj8mqgY7T2gIVEdvACh3SNADqEAMYASA AEgLdEfD_BwE

Extractor, B. E. (2018). *iPhone backup*. Retrieved from https://www.iphonebackupextractor.com/?utm_source=bing&utm_medium=ad&utm_campaign=itunes-icloud-trusted-by-experts&msclkid=3d9cef59765e1250a568b3d2890a0463

imore-files in iPhone and iTunes. (2018, April 1). *imore.com*. Retrieved from files in iPhone and iTines: https://www.imore.com/how-find-and-remove-other-files-iphone-and-ipad

imyfone-Backup Application . (2018, March 26). *imyfone*. Retrieved from Backup Application: https://www.imyfone.com/iphone-data-recovery/?gclid=EAIaIQobChMI_qPxlLOu2gIVWrbACh1HWQtoEAAYASAAEgKNAPD_BwE

iTunes. (n.d.). Retrieved from https://www.apple.com/itunes/download.

Kandidatuppsats. (2013). *Forensic investigations of Apple's*. In Kandidatuppsats, Forensic investigations of Apple's (p. 23). Rapport: IDE.

Phone.html. (2018). Retrieved from https://www.computerworld.com/article/2604020/apple-ios/the-evolution-of-apples-iphone.html

Ttechtarget-NAND flash memory . (2018, March 25). *Techtarget*. Retrieved from NAND flash memory: http://searchstorage.techtarget.com/definition/NAND-flash-memory

What Do iPhone Forensic Investigations Reveal? (2018, February 22). *Burgessforensics.com*. Retrieved from iphone-forensic-investigations: https:// burgessforensics.com/iphone-forensic-investigations/