University of Economics, Prague

Faculty of Informatics and Statistics

Forensic analysis of mobile applications

BACHELOR’S THESIS

Study program: Applied informatics

Field of study: Applied informatics

Author: Daria Constantinov

Supervisor of the bachelor’s thesis: doc. Ing. Vilém Sklenák, CSc.

Prague, December 2018

Prohlášení

Prohlašuji, že jsem bakalářskou práci Forensic analysis of mobile applications vypracovala samostatně za použití v práci uvedených pramenů a literatury.

V Praze dne 10. prosince 2018 ....

Daria Constantinov

Poděkování

Ráda bych tímto poděkovala svému vedoucímu doc. Ing. Vilému Sklenákovi, CSc za užitečné rady, čas věnovaný při konzultacích a trpělivost při psaní bakalářské práce. Chtěla bych také poděkovat Jakubovi Weberschinkovi, senior manažerovi ve forenzním oddělení za poskytnutí licence pro použitý software a odborné rady při tvorbě této práce. Za podporu též děkuji svoji mamince, přátelům a kolegům z práce.

Abstrakt

Zvýšené používání různých typů aplikací na mobilních telefonech vytváří v těchto zařízeních bohatý zdroj osobních informací pro forenzní vyšetřovatele. Mobilní zařízení mohou uchovávat potenciální důkazy, které lze vytěžit pomocí forenzních nástrojů a analýzy. Tato bakalářská práce se zabývá prováděním forenzní analýzy dvanácti mobilních aplikací, a to: Messenger, WhatsApp, Viber, iMessage, Google Chrome, Safari, Firefox, Opera Mini, Google Maps, Apple Maps, Mapy.cz a Waze. Aplikace jsou rozděleny do tří typů: komunikace, mapy a navigace, prohlížení. Výzkum byl proveden na zařízení iPhone 6, na kterém byly nainstalovány zmíněné aplikace. V každé aplikaci byly prováděny stanovené uživatelské aktivity. Poté byly na mobilním telefonu provedeny tři typy extrakcí. Konkrétně logická, pokročilá logická a extrakce souborového systému. Následně byla provedena manuální forenzní analýza získaných dat. Forenzní analýza měla za cíl zjistit, zda byly na zařízení uloženy a zachovány konkrétní činnosti prováděné ve vybraných aplikacích. Výzkum vedl k závěru, že se z aplikací pro navigaci nepodařilo získat téměř žádné stopy, s výjimkou Waze. Aplikace pro komunikaci a prohlížení poskytly příležitost získat značné množství cenných osobních údajů, které mohou soudní vyšetřovatelé například použít v řešení trestních případů.

Klíčová slova

Cellebrite UFED, extrakce dat, forenzní analýza, forenzní nástroj, iPhone, mobilní telefon.

Abstract

The increased use of different types of applications on mobile phones makes these devices a goldmine of personal information for forensic investigators. Mobile devices can store potential evidence, which can be acquired with the forensic tools and analysis. This bachelor's thesis focuses on performing forensic analysis of twelve mobile applications, such as Messenger, WhatsApp, Viber, iMessage, Google Chrome, Safari, Firefox, Opera Mini, Google Maps, Apple Maps, Mapy.cz, and Waze. The applications are categorized into three types of mobile applications, namely communicating, maps and navigation, and browsing. The study was conducted on iPhone 6, on which were installed mentioned applications. In each application were performed specific user activities. Then three types of extractions were conducted, specifically logical, file system, and advanced logical. After that manual forensic analysis was performed on the acquired data. The forensic analysis aimed to determine whether specific activities conducted through chosen applications were saved and stored on the device. The study led to the conclusion that almost no traces could be recovered from applications for navigation, except Waze. Applications for socializing and browsing gave the opportunity to extract a substantial amount of valuable personal data that can be used by forensic investigators for solving criminal cases.

Keywords

Cellebrite UFED, data extraction, forensic analysis, forensic tool, iPhone, mobile phone.

Contents

Seznam obrázků

Introduction

In today's world of technology, nearly everyone has a mobile phone. Initially, the main functionality that was expected from a mobile was the capability of communication. In the course of time, it has become an excellent tool not only for communication but also for taking photos, listening to music, browsing, using navigation, etc. Installing various applications gave user an opportunity to extend functions of their mobile phones. As a result, people are used to taking their phones everywhere they go and constantly using different types of applications. In this way, the applications store a substantial amount of personal data that can be disclosed by malicious users or contain traces of illicit activities. Disclosure of personal information, for example, can lead to crimes such as identity theft, stalking, blackmailing, etc. Therefore, mobile devices can hide important evidence, which can be used by authorized bodies for solving criminal cases. In this connection, nowadays it is essential to study different types of applications from a forensic point of view. This results in the topic of this bachelor's thesis.

The crimes related to disclosure of personal information from the mobile phones become more frequent these days, and as a consequence, people start thinking about possible ways to protect their private data. In order to achieve that, the users give preference to applications, which promise them to secure their information. This is another indicator of the importance and relevance of the topic.

There are several reasons behind choosing this particular topic for the bachelor's thesis. The first reason is the fact that the author's occupation is related to a particular phase of the forensic process, namely data acquisition. Another reason is the author's interest in the matter and willingness to know further details not only about the data acquisition but also about the next phase of the forensic process, namely forensic analysis. At present this area is on the upswing, which increases the author's curiosity and desire to work with innovations and know-how.

This thesis intends to reveal differences in data stored in various types of applications. The purpose of the bachelor's thesis is to analyze data from applications, which are obtained during the forensic collection of the mobile phone. The mobile applications were chosen from the three most used categories, specifically communication, maps and navigation, and browsing. In each category were analyzed data from 4 applications, which means that a total of 12 mobile applications were installed on the phone, if there were not already integrated with it. Subsequently, the author was using mentioned applications in his everyday life and was performing specific activities in them. After a particular period of time, the created data were extracted from the phone using two software forensic tools and the forensic analysis was performed.

1 Forensic Process

The term “forensic” is derived from the Latin "forensis", which means "before a forum, public", and was used when presenting a case in court. The term “forensics” is an abbreviated form of “forensic science”. Forensic science studies collection, preservation, and analysis of the scientific evidence during the investigation. Forensic science consists of various categories, or branches, such as toxicology, ballistics, anthropology, DNA profiling, fingerprint analysis, and more.

Digital Forensic is one of the branches of Forensics Science, which is comprised of the recovery and examination of data that are found in examined devices and electronic media. (Carrier et al., 2002) Originally, digital forensic was mainly known as the forensic section that studies evidence from computers. In the course of time, the meaning of the term has expanded to include examination of new devices that appeared on the market and were able to store digital data. Therefore, the forensic section that studies evidence from mobile phones is called mobile phone forensics.

As stated by National Institute of Standards and Technology in the U.S., mobile phone forensics can be defined as the science of retrieving digital evidence from a mobile phone under forensically sound conditions by applying accepted methods. Due to the fact, that every investigation is conducted differently, it is difficult to determine a unified procedural approach to the forensic process. Even though there is no standardized guideline, the process can be widely separated into four key areas: preservation, acquisition, examination and analysis, and reporting. (Ayers et al., 2014) The first phase is very important, as a whole investigation is based on the correct way of preserving the integrity and chain of custody of the digital evidence. Failing this phase might jeopardize the entire investigation. The second phase consists of acquisition of the evidentiary data, after which follows the next phase of their examination. In the final phase, the findings of the analysis are brought in a format that can be presented for example in front of the jury. (Majeed et al., 2015) In this bachelor’s thesis, only two stages are relevant to us: acquisition and analysis, which are described below in more detail.

1.1 Acquisition

The acquisition is presented by the process of imaging or, in other words, extraction of information, that is stored on the mobile device and its peripheral equipment and media. (Ayers et al., 2014) Peripheral equipment and media are understood to be associated with the phone secure digital memory cards (from now onwards SD cards) and subscriber identity module cards (from now onwards SIM cards).

As mentioned above, there are different approaches and steps that can be followed during the forensic process. The main requirement for all the procedures is that extraction of data and its further documentation must be carried out in such a way, that acquired information is reliable for usage in criminal proceedings.

The first step in the forensic examination is considered to be the identification of the device. Set of characteristics of mobile phone determine the route, which should be taken in creating an image of the evidence. Mobile characteristics are understood to be manufacturer, model, serial number, international mobile equipment identity (from now onwards IMEI), capacity, etc. With a knowledge of the exact type of the phone, we are able to define an appropriate forensic tool for mobile extraction. There are several software forensic tools for mobile phones on the market. They differ in price, methods of extraction, supported types of mobile devices, user experience and type of output. Unfortunately, in some cases, data that are extracted using different tools are not identical. One forensic tool, for example, can uncover more data, than the other. In such cases, it is better to use several tools, in order to have verified data.

Discovered information also depends on the type of extraction that is used during acquisition. In general, software forensic tools allow to perform 3 types of acquisition, which include logical, file system and physical extractions. These types of acquisition are further explained in chapter 4.

Before connecting the mobile device to the forensic tool, it is necessary to properly prepare it for the examination. In some procedures the first step is turning off the mobile phone if it is not already turned off. Next step would be removing SIM cards and SD cards that are examined separately, in order to provide a comprehensive analysis based on the type of trace. In such cases, special adapters are required for imaging SD and SIM cards.

Another approach that can be applied during the acquisition process is keeping the mobile phone turned on. This results in the necessity of turning on the airplane mode in order to disable cellular communications and to avoid modification or destruction of data on the evidence. This can also be achieved with the help of Faraday bag, but it is important to keep in mind, that it does not completely eliminate the potential for cellular and wireless networks, especially when it is not properly sealed. (Sachowski, 2018)

Conducting acquisition with removed SIM and SD cards is not a strict rule either. If SD card is left inside the mobile phone while the phone is being imaged, then SD card does not need to be removed and imaged once again, as all the data from the card were collected along with the data from internal memory of the phone. SIM card, on the other hand, must be always imaged apart from the mobile device.

1.2 Data analysis

After the acquisition is performed on the mobile device, there comes a time when data need to be analyzed. The analysis consists of an examination of the evidence, determining the significance of findings, and drawing conclusions based on them. (Ayers et al., 2014)

There is a rich variety of different information that is stored on mobile devices. Some data are characteristic for all types of mobile devices and some data are created by user's installed applications. The second type of data can reveal a great amount of information about the user. Extracted data generally include contact lists, SMS messages, call logs, pictures, videos, audio files, e-mails, notes, calendars, visited locations, etc.

This phase is aimed to examine and reveal digital evidence from the extracted data. The process of analyzing data is generally supported by special forensic tools, which are able to open files that are generated after the acquisition process. The chosen tool gives forensic examiner an opportunity to examine and correlate findings with the crime scene in order to reach strong conclusions. During this phase, investigator traces connections between people and events using information about time, images, calls, online activities, movements and other incidents, which may occur after the acquisition.

2 Forensic tools

At the present time, there are several commercial tools for forensic analysis of mobile devices on the market. These forensic tools can be divided into two main categories. The first category includes software tools that are installed on a workstation. In order to obtain data from a mobile device, it is later connected to the workstation via USB cable. The second category is represented by hardware tools. That means that data from mobile devices are extracted using a particular apparatus, which is developed specially for acquiring the data. In this case, mobile device is not connected to the workstation, but to the hardware forensic tool. However consequent data analysis is conducted by means of software tools installed on the workstation. Generally, companies that develop forensic tools offer both types of tools: hardware and software. In this chapter are described some of them, specifically MSAB XRY, Oxygen Forensic, MOBILedit Forensic Express, and Cellebrite UFED.

2.1 MSAB XRY

XRY is a software forensic tool from a Swedish company MSAB. XRY offers physical as well as, logical extractions. More than 25 000 mobile device profiles are supported by this tool, including drones. XRY is able to extract device information, contacts, call logs, appointments, notes, tasks, SMS, MMS, iMessages, e-mails with attachments that can be viewed immediately. The tool supports over 1 600 application versions and gives the opportunity to obtain media files, such as photos, videos, audio files and voice recordings that can be instantly listened to. It can also extract locations, WiFi connection history, passwords for device owner’s accounts

Another function includes technology of image recognition that classifies images into categories, such as drugs, weapons, and humans. XRY is able to recover data from a cloud storage without re-entering user’s login details. Next feature is an ability to extract data from another type of mobile phones, such as cheap imitation phones from Asia. The tool supports the latest smartphones, including the latest iOS version 11, and a variety of new Android devices. (MSAB, 2018)

2.2 Oxygen Forensic

Oxygen Forensic is a forensic software that extracts data from mobile devices, their backups, SIM cards, memory cards, drones, and cloud storage. With this tool forensic examiner is able to extract and analyze device information, call logs, contacts, media files, calendars, notes, iMessages, SMS, MMS, e-mails, GPS coordinates, Wi-Fi connection history, etc. Among other features is finding passwords to encrypted images and backups, bypassing screen lock on well-known Android OS devices, extracting metadata and GPS location from drones, recovering deleted files, for example, contacts, messages, call logs, photos, etc.

Oxygen Forensic supports more than 430 application updates for mobile phones, more than 16 900 smartphones with various operating systems. The tool allows user to import multiple types of backups, as well as images of iOS and Android devices that were created by other forensic tools. It has the ability to extract data using a USB data cable or Bluetooth connection. The price for different packages varies from $2,499 to $89,999 depending on the number of concurrent connections. (Oxygen Forensics, 2018)

2.3 MOBILedit Forensic Express

MOBILedit Forensic Express is able to extract data from mobile devices and cloud storage, analyze them and immediately generate a report. All these functions nowadays are a standard among forensic tools. This tool is an extractor with a wide range of supported mobile devices. One of the newest features is Photo Recognizer, which automatically searches and recognizes suspicious content in photos, such as weapons, drugs, nudity, currency, and documents. Photo Recognizer uses artificial intelligence and machine learning that allows the forensic examiner to quickly analyze an unlimited number of pictures, instead of wasting a lot of time on exhaustive manual search of key evidence in large photo databases. The forensic tool also gives an opportunity to generate reports in multiple languages. MOBILedit Forensic Express does not have the exact number of supported mobile devices on their website.

Applications are examined in detail, including data of deleted applications, if available. MOBILedit Forensic Express provides a comprehensive report on contacts, phone calls, messages, audio and video files, and deleted files, if available. The tool also extracts and break passwords from applications and accounts. It can obtain information about Wi-Fi connection, for example, name of the Wi-Fi network, security mode, and time of the last connection. The investigator can also acquire GPS location and web browser history. However, the amount and types of extracted data depend on the particular model of the mobile device, its operating system and its condition. The price for different packages varies from $99 to $1,500 depending on the number of mobile phones and available features. (MOBILedit, 2018)

2.4 Cellebrite UFED

Cellebrite UFED is a family brand name for a group of mobile forensics products of Israeli company Cellebrite. UFED includes both hardware and software tools. Various products from this package are able to perform different types of extraction, such as logical, advanced logical, file system, physical, etc. They also have the ability to restore deleted files from the mobile devices and decode information, which is encrypted or protected with a password. UFED can extract data not only from mobile devices, such as tablet computers, smartphones, personal digital assistants (from now onwards PDAs), but also from SD and SIM cards. For this reason, UFED products come complete with adapters, cables and other peripherals, which then become a part of the forensic accessory kit. It is also important to mention, that Cellebrite UFED products are not the cheapest ones. (Mahalik, 2016) The price ranges from approximately $149 to $16,000. (Digital shield, 2018; SC Media UK, 2015)

Two software forensic tools from Cellebrite UFED are chosen for performing data acquisition and data analysis in the practical part of this bachelor's thesis. The main reason for using these tools is the author's experience with software and hardware tools from this company, and his access to them and their license that he has available at work. The chosen tools also have a user-friendly interface that is an advantage for some inexperienced users, who might become interested in them after reading the performed study. The UFED Cellebrite supports a vast number of device profiles as well. Therefore, next chapter includes a more profound description of the two software tools from Cellebrite UFED, which are used later in a practical part of the thesis.

3 Forensic tool Cellebrite UFED

Cellebrite UFED provides investigations with field-ready tools, such as Ruggedized Laptop and Touch2, that are able to withstand different types of damage during various situations. Other software and hardware products, that are offered by UFED are 4PC, Touch, UFED Cloud Analyzer, UFED Logical Analyzer, UFED Physical Analyzer, UFED InField, Phone Detective, etc.

The latest version 7.11 of the Cellebrite UFED products was released in November 2018 and now supports 26 179 device profiles and 7 043 app versions. (Cellebrite, 2018) It is necessary to take into account, that each software forensic tool has its own specifications, and is not obliged to work with all types of mobile devices. For instance, UFED Physical Analyzer is able to extract data only from iOS, GPS and mass storage devices, nevertheless it can open any type of extraction from other devices. UFED 4PC, on the other hand, can extract data from a greater range of mobile devices, including newly released models, such as iPhone X that was released in November 2017. On that account for the practical part of this bachelor's thesis is chosen iPhone 6, as data extraction from devices that run iOS provides a more in-depth view of the device. This chapter introduces the reader to the following software forensic tools: UFED 4PC and UFED Physical Analyzer, that are used in the practical part of the thesis later on.

3.1 UFED Physical Analyzer

The UFED Physical Analyzer application uses advanced deciphering, analysis, and reports in order to provide a comprehensive view of the device's memory. As has been mentioned above, this software tool can decode all types of extractions created by UFED and carry out powerful extraction for GPS and iOS devices. Physical Analyzer is able to reconstruct file system of the device and decipher various analyzed data types such as Contact lists, call logs, text messages (SMS), device and application information, and more. Among its key features is also the ability to provide access to both current and deleted data on the device. Physical Analyzer offers an opportunity for powerful analysis and search. It allows the user to conduct an advanced search based on multiple parameters, regular expressions (RegEx) and a predefined list of keywords. The application supports a single chronological view, that represents a timeline of all the events performed via the mobile device. It enables to add, remove and write your own plug-ins as well. It is also important to mention, that it has intuitive and user-friendly user interface (from now onwards UI) for browsing the extracted information.

Before installing Physical Analyzer, it is important to take into consideration system requirements that are presented in the Table 3.1-1. (Cellebrite PA Manual, 2018)

UFED Physical Analyzer can be activated in one of the following ways: using a software license, a hardware license key (from now onwards dongle) and a network dongle license. In this bachelor's thesis the second method is used, namely, the dongle license. It is necessary to note that user must have administrative rights over the computer, in order to activate the application.

Table 3.1-1 System requirements for UFED Physical Analyzer

PC	Windows compatible PC with a Pentium IV or compatible processor running at 1.6 GHz or higher
Operating System	Microsoft Windows 10, 64-bit; Microsoft Windows 8.x, 64-bit; Microsoft Windows 7, 64-bit
Memory (RAM)	16 GB
Space requirements	1 GB of free disk space for installation
Additional Requirements	Microsoft .Net version 4.6 or older versions 4.5.2, 4.5.1, 4.5, 4.0

3.2 UFED 4PC

UFED 4PC enables to perform different types of data extraction, such as logical, file system, physical, SIM and password extractions. Later on, acquired information can be saved to an SD memory card, USB flash drive, or directly to the PC that is used for acquisition.

4PC has the ability to extract data from the wide range of operating systems, among which are: Apple iOS, Android, Blackberry, Microsoft Mobile, Symbian, and Palm OS. Extracted data are represented by phonebook entries, SMS messages, call logs, pictures, videos, audio files, device information, etc. The software tool is able to clone the SIM ID, which allows the user to extract phone data while preventing the mobile device from connecting to the network. It can also help if the SIM card is missing. The user interface is instinctive, complete and easy to use. Before installing UFED 4PC, it is important to take into consideration system requirements from the Table 3.2-1. (Cellebrite 4PC Manual, 2018)

Table 3.2-1 System requirements for UFED 4PC

PC	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher
Operating system	Microsoft Windows 10, 64-bit; Microsoft Windows 8.x, 64-bit; Microsoft Windows 7, 64-bit; Microsoft Windows 7 Boot Camp on MAC
Memory (RAM)	16 GB (recommended), 4 GB (minimum)
Space requirements	1.5 GB of free disk space for installation
Additional requirements	Microsoft .Net version 4.5 or later

UFED 4PC can be activated using four different methods. Three of them repeat methods for UFED Physical Analyzer, and the fourth includes an online license. The UFED 4PC works in conjunction with Cellebrite’s Physical Analyzer software and allows the user to view, search and analyze the extracted data. (RCFL, 2014)

4 Types of data extraction in Cellebrite UFED

As discussed in the previous chapter, UFED 4PC and UFED Physical Analyzer allow conducting different types of data extraction. One of the differences is, that UFED 4PC works with a great variety of mobile devices, whereas the UFED Physical Analyzer is able to extract data primarily from devices, that run iOS. This chapter discusses 4 main types of data acquisition available for iOS devices. The UFED 4PC has the ability to perform logical, file system, and physical extractions. The UFED Physical Analyzer gives the opportunity to conduct physical and advanced logical extractions.

4.1 Logical extraction

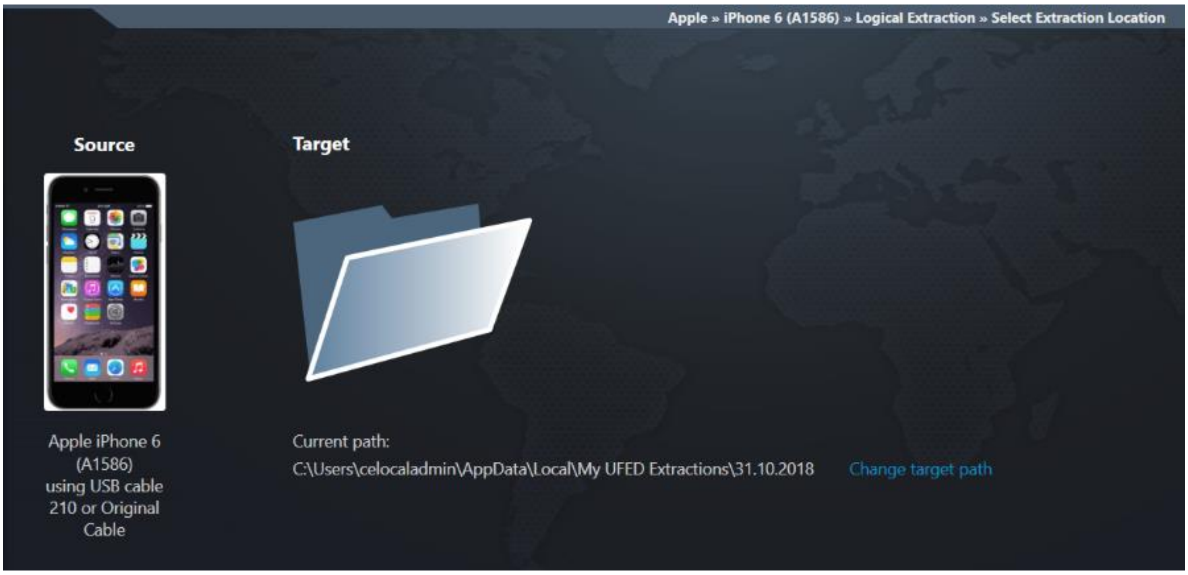
Logical extraction is the lowest level of extraction, that is available for the most mobile devices. For interaction with the mobile device, this type of acquisition uses Application Programming Interface (from now onwards API), that specifies the way firmware and applications collaborate. The UFED 4PC offers this function for the majority of iOS, Android, BlackBerry and Windows Phone apps. The available types of extracted data may vary depending on the source device manufacturer and model and the version of the program. This type of extraction does not support the extraction of deleted files. (Cellebrite 4PC Manual, 2018)

The folder that is created after the extraction contains:

- Folder with multimedia files named Images, Video, Audio, and Ringtones folders, containing each of the corresponding type of media files.
- UFED Manager files of the extracted phonebook (*.pbb), SMS messages (*.sms), MMS (*.MMS), IM (*.IM), calls log (*.clog), calendar (*.cal), and Email (*.Email) data.
- Report files in HTML and XML formats.
- UFD file. (Cellebrite 4PC Manual, 2018)

The steps described below are intended to guide the user through the process of logical data extraction from iPhone in UFED 4PC.

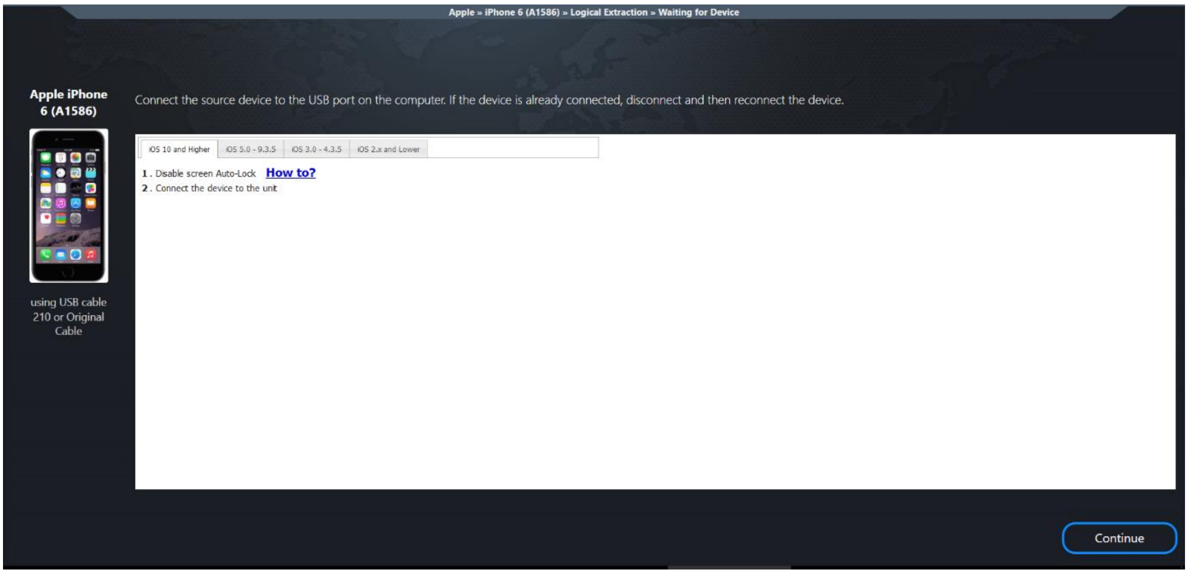
1) The first step is selecting extraction location, specifically targeted folder, which afterwards serves to store the extracted files. (Figure 4.1.1)


Apple » iPhone 6 (A1586) » Logical Extraction » Select Extraction Location
Source
Target
Apple iPhone 6 (A1586) using USB cable 210 or Original Cable
Change target path

Current path:
C:\Users\celocaladmin\AppData\Local\My UFED Extractions\31.10.2018

Figure 4.1.1 Logical extraction - Select location (source: author)

2) During the second step, the user needs to connect the source device to the USB port on the computer. If the device is already connected, the user can proceed with the extraction by pressing a button "Continue" in the right bottom corner. However, in some cases, the button is not enabled immediately, then arises necessity to disconnect the device and reconnect it again. This action allows the user to proceed to the next step. (Figure 4.1.2)


Apple » iPhone 6 (A1586) » Logical Extraction » Waiting for Device
Apple iPhone 6 (A1586)
using USB cable 210 or Original Cable
iOS 10 and Higher
iOS 5.0 - 9.3.5
iOS 3.0 - 4.3.5
iOS 2.x and Lower
Continue

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

1 . Disable screen Auto-Lock How to?
2 . Connect the device to the unit

Figure 4.1.2 Logical extraction - Waiting for device (source: author)

3) The user specifies types of data that he needs to extract from the mobile device. In the UFED 4PC there are available following information types: Contacts, SMS, MMS, Email, IM (instant message), Calendar, Apps Data, Pictures, Audio/Music, Videos, Ringtones, Call Logs, and Browsing Data. User Dictionary is available only for devices with the Android operating system. (Figure 4.1.3)

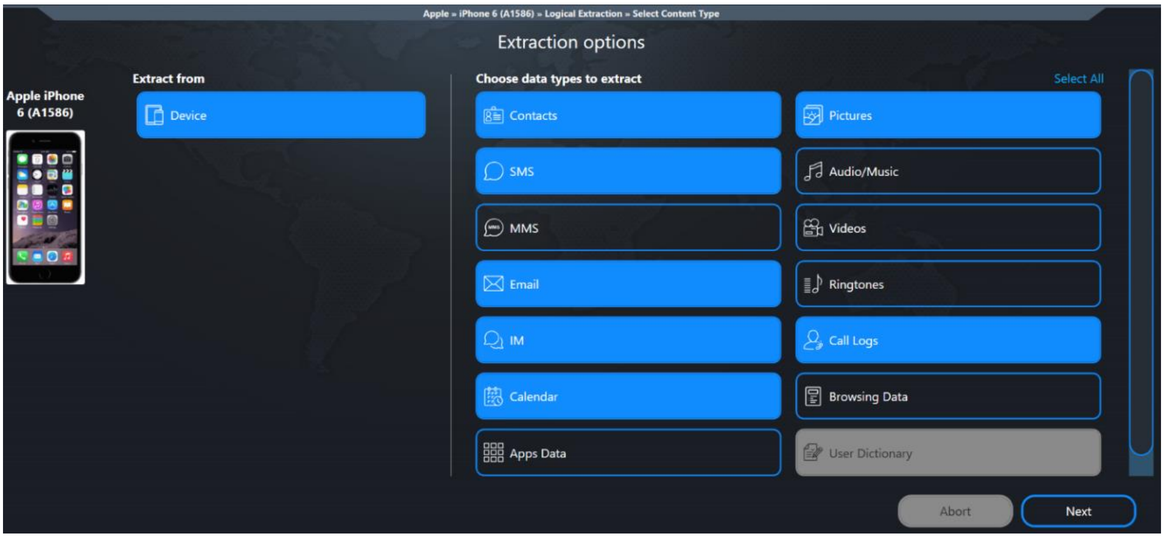
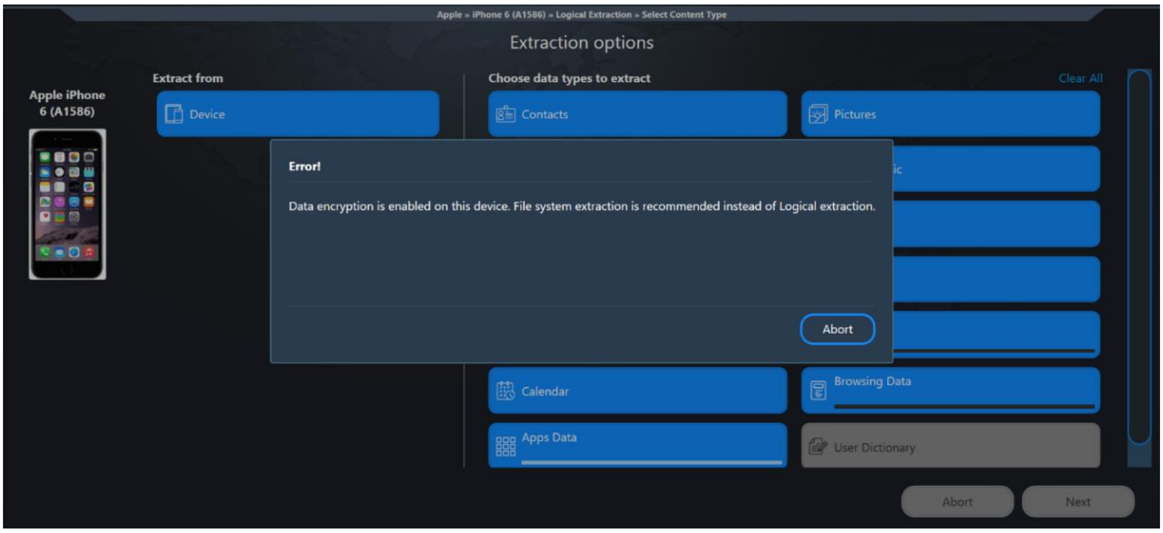


Figure 4.1.3 Logical extraction - Select Content Type (source: author)

4) Before proceeding to the next step the user needs to unlock the device and choose "Trust" when the trust message displays. If the investigated device is running iOS 11 or higher, then it may also require the device password.

5) When performing data extraction from encrypted iOS devices, the following "Error!" window appears. As can be seen from the alert, file system extraction is recommended instead of logical extraction of information from the encrypted device. Close the window by clicking on the Abort button. (Figure 4.1.4)

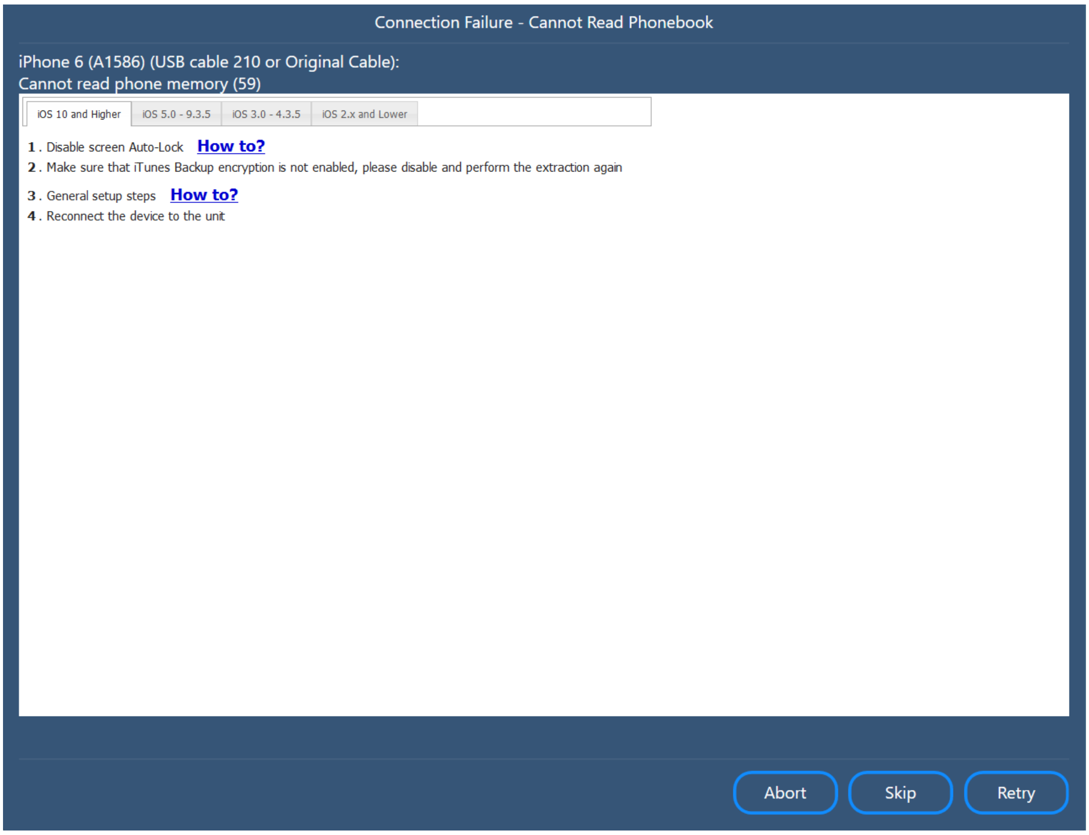


Error!

Data encryption is enabled on this device. File system extraction is recommended instead of Logical extraction.

Figure 4.1.4 Logical extraction - Error window (source: author)

6) There may appear a few windows in a row. Each of them informs the user about the type of information that cannot be read from the device. The user may choose to Abort the extraction, Skip this type of information and proceed with the extraction, or Retry the action after following recommended steps. The unreadable data types can include, for example, Phonebook, Calendar, and more. (Figure 4.1.5)



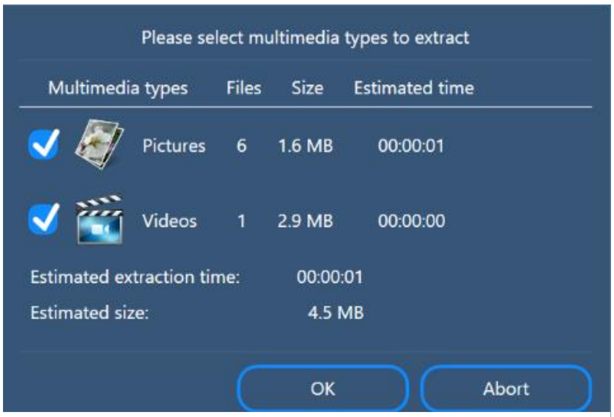
Connection Failure - Cannot Read Phonebook

iPhone 6 (A1586) (USB cable 210 or Original Cable):
Cannot read phone memory (59)

1 . Disable screen Auto-Lock How to?
2 . Make sure that iTunes Backup encryption is not enabled, please disable and perform the extraction again
3 . General setup steps How to?
4 . Reconnect the device to the unit

Figure 4.1.5 Logical extraction - Cannot read data (source: author)

7) After determining readable information on the device UFED 4PC offers to select the multimedia types to extract. The user must choose the required types and click Ok. (Figure 4.1.6)



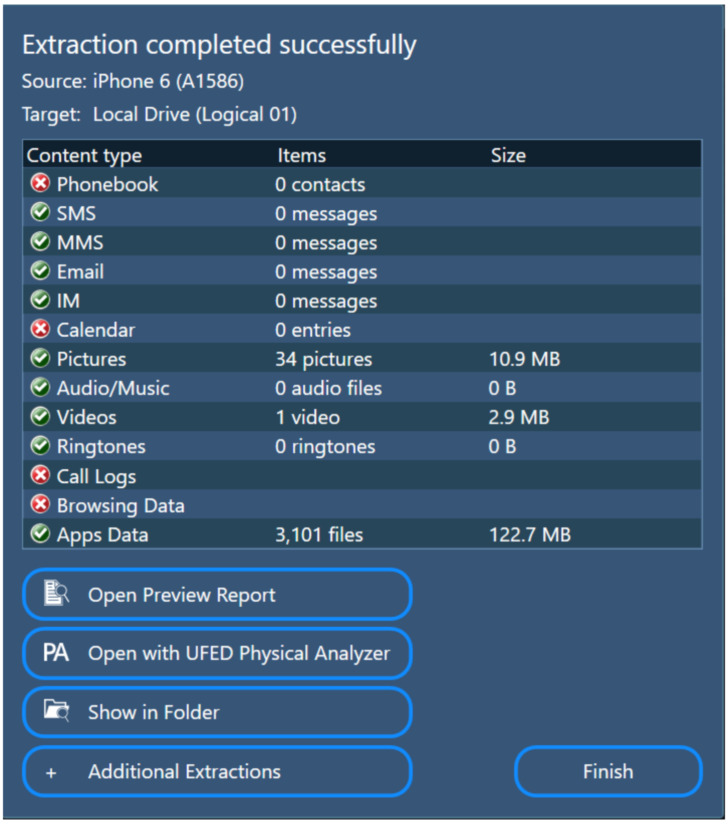
Please select multimedia types to extract

Multimedia types	Files	Size	Estimated time
☑ Pictures	6	1.6 MB	00:00:01
☑ Videos	1	2.9 MB	00:00:00

Estimated extraction time: 00:00:01
Estimated size: 4.5 MB

Figure 4.1.6 Logical extraction - Multimedia types (source: author)

8) When the extraction is complete, the following window appears. The UFED 4PC offers the user different options. He is able to view an HTML preview report that includes information about the device and the extraction. Another option is opening the extraction with the UFED Physical Analyzer. The user can also open the folder with the UFD extraction file and add additional extraction types for the same device. To end the process and return to the home screen the user must press the Finish button. (Figure 4.1.7)



Extraction completed successfully

Source: iPhone 6 (A1586)

Target: Local Drive (Logical 01)

Content type	Items	Size
✗ Phonebook	0 contacts	
✓ SMS	0 messages	
✓ MMS	0 messages	
✓ Email	0 messages	
✓ IM	0 messages	
✗ Calendar	0 entries	
✓ Pictures	34 pictures	10.9 MB
✓ Audio/Music	0 audio files	0 B
✓ Videos	1 video	2.9 MB
✓ Ringtones	0 ringtones	0 B
✗ Call Logs		
✗ Browsing Data		
✓ Apps Data	3,101 files	122.7 MB

Figure 4.1.7 Logical extraction - Extraction completed (source: author)

4.2 File system

This type of acquisition extracts the complete file system of the mobile device. File system extraction is also able to obtain deleted files in contrast to logical extractions. File system extraction is conducted by the UFED 4PC and can be afterwards viewed using the UFED Physical Analyzer.

There are four modes available for this type of acquisition, that are presented below:

- Data files mode runs the Apple file system extraction and provides media files and applications data.
- Backup mode runs the iTunes backup and provides a wider range of data including call logs, application data, SMSs, MMSs, and locations.
- Full mode is recommended for extracting data included in both of the above modes.

The extraction time depends on the mode selected by user and on the amount of data on the iOS device. For example, an extraction in a Backup mode from an actively used device can take several hours to complete.

The UFED 4PC includes an option to encrypt the iOS file that results in extracting more sensitive information not found on a standard iCloud or iTunes backup file. This additional layer of security gives the ability to obtain login details for apps, email accounts, user credentials (keychain), and more. As soon as the extraction is completed, the encryption is automatically reset.

Folder that is generated after the extraction is completed contains the following:

- A zipped archive of the device file system, which contains folders and files in the respective structure they were extracted.
- UFD file of the system extraction information. (Cellebrite 4PC Manual, 2018)

The steps described below are intended to guide the user through the process of file system extraction from iPhone in the UFED 4PC:

1) The user must select one of the displayed modes. Availability of the certain modes depends on the particular device. iOS full File System is available from Cellebrite Advanced Investigative Services (from now onwards CAS). CAS experts work only with law enforcement agencies with legal authority to unlock phones. They provide these agencies with forensically sound access to sensitive mobile digital intelligence. (Cellebrite, 2018) (Figure 4.2.1)

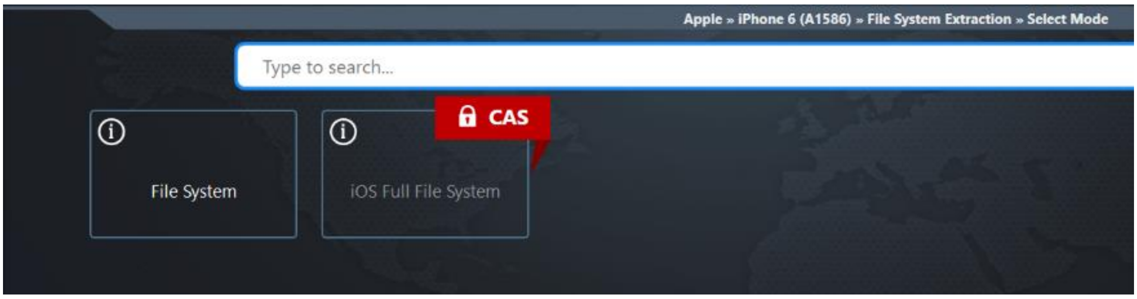
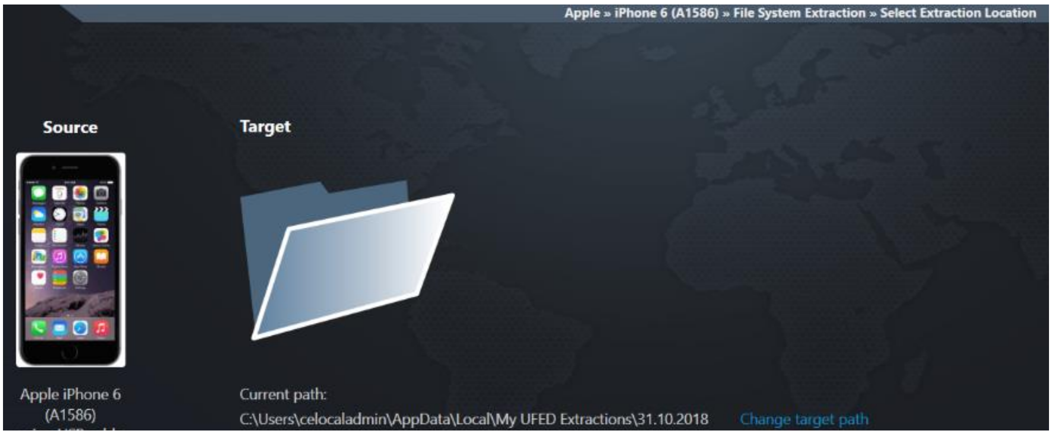

Apple » iPhone 6 (A1586) » File System Extraction » Select Mode
Type to search...
CAS
File System
iOS Full File System

Figure 4.2.1 File system extraction - Select Mode (source: author)

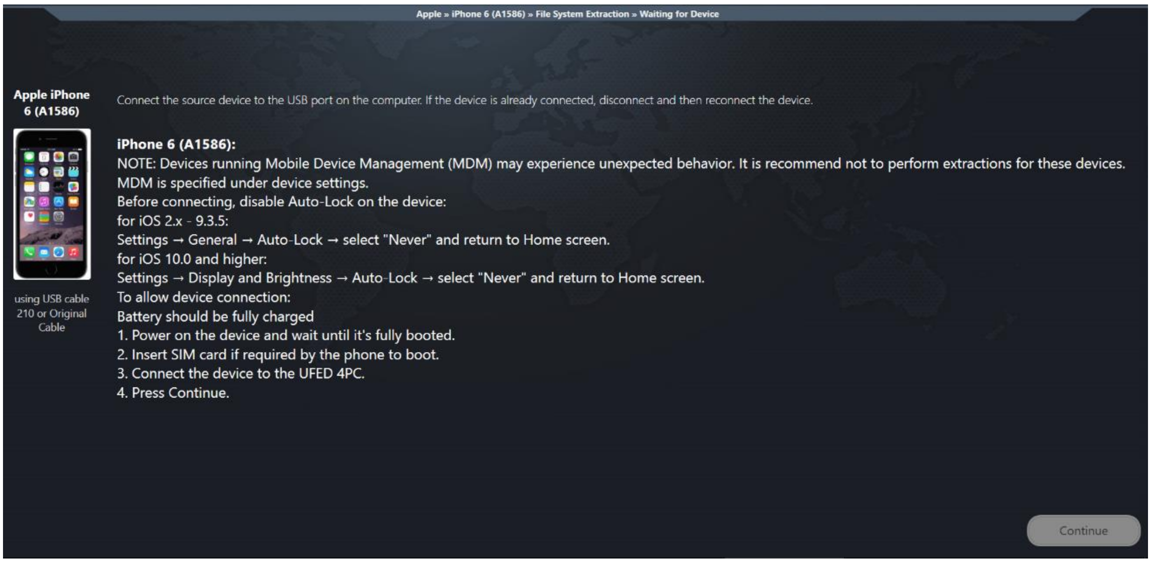
2) Select the destination folder, to which extracted data are saved after the acquisition. (Figure 4.2.2)


Apple » iPhone 6 (A1586) » File System Extraction » Select Extraction Location
Source
Target
Apple iPhone 6
(A1586)
Change target path

Current path:
C:\Users\celocaladmin\AppData\Local\My UFED Extractions\31.10.2018

Figure 4.2.2 File system extraction - Select location (source: author)

3) This step repeats step 2 from Logical extraction and additionally gives more detailed instructions on how to disable Auto-Lock on the device and to connect it to the UFED 4PC. (Figure 4.2.3)



Apple » iPhone 6 (A1586) » File System Extraction » Waiting for Device

Apple iPhone 6 (A1586)

using USB cable 210 or Original Cable

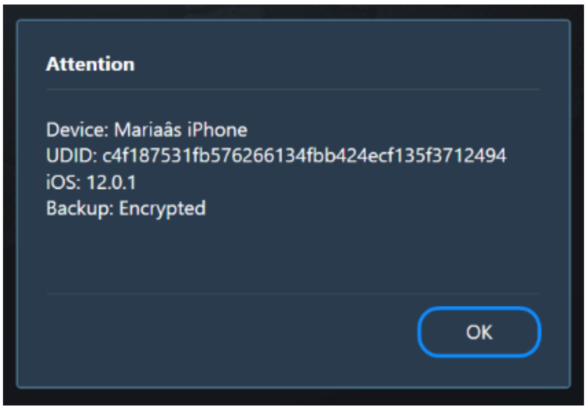
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

iPhone 6 (A1586):
NOTE: Devices running Mobile Device Management (MDM) may experience unexpected behavior. It is recommend not to perform extractions for these devices.
MDM is specified under device settings.
Before connecting, disable Auto-Lock on the device:
for iOS 2.x - 9.3.5:
Settings → General → Auto-Lock → select "Never" and return to Home screen.
for iOS 10.0 and higher:
Settings → Display and Brightness → Auto-Lock → select "Never" and return to Home screen.
To allow device connection:
Battery should be fully charged
1. Power on the device and wait until it's fully booted.
2. Insert SIM card if required by the phone to boot.
3. Connect the device to the UFED 4PC.
4. Press Continue.

Figure 4.2.3 File system extraction - Waiting for device (source: author)

4) Before proceeding to the next step the user needs to unlock the device and choose “Trust” when the trust message displays. If the investigated device is running iOS 11 or higher, then it may also require the device password.

5) The “Attention” message with information about the device appears. The window displays the device name, Unique Device ID (UDID), iOS version, and whether the backup is encrypted. Click OK. (Figure 4.2.4)



Attention

Device: Mariaâs iPhone
UDID: c4f187531fb576266134fbb424ecf135f3712494
iOS: 12.0.1
Backup: Encrypted

Figure 4.2.4 File system extraction - Attention message (source: author)

6) The user must choose one of the available modes as explained previously. The modes displayed differ depending on the particular device. (Figure 4.2.5)

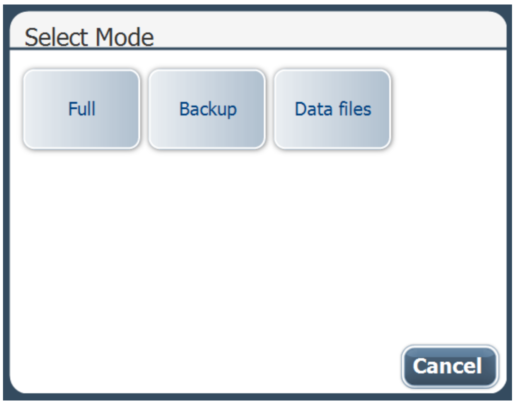
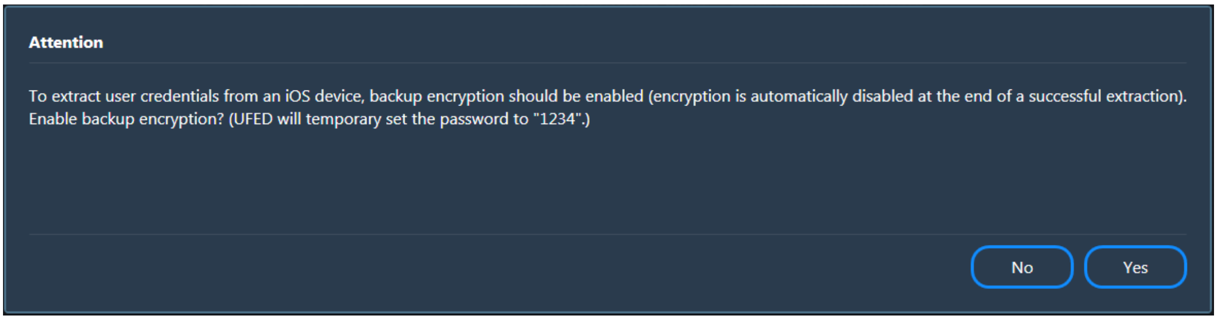


Figure 4.2.5 File system extraction - Select mode (source: author)

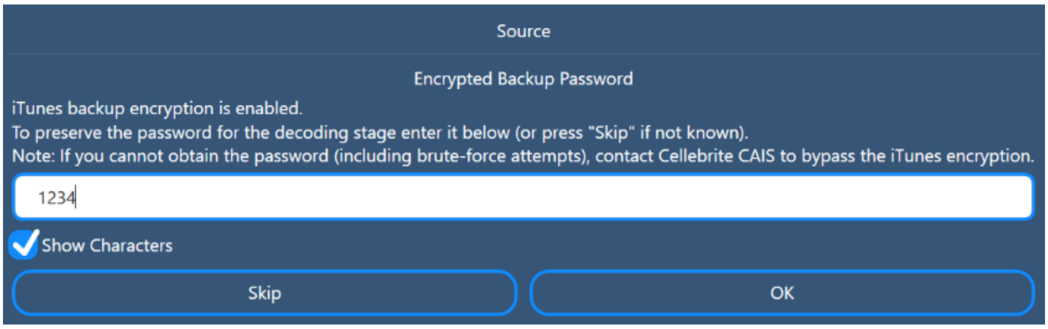
7) Next step depends on whether the iTunes backup is encrypted or not.
    a. If the iTunes backup is not encrypted, the following message about data encryption appears (not applicable to the Data files mode). The message informs the user about the requirement for a backup encryption to be enabled in order to extract user credentials from an iOS device. If the user chooses to temporarily encrypt the backup, the UFED 4PC will set the password to “1234”. (Figure 4.2.6)


Attention

To extract user credentials from an iOS device, backup encryption should be enabled (encryption is automatically disabled at the end of a successful extraction). Enable backup encryption? (UFED will temporary set the password to "1234".)

Figure 4.2.6 File system extraction - Backup encryption (source: author)

    b. If the iTunes backup encryption is already enabled, then the following window appears. If the user knows the iTunes backup password, he can enter it in this step so that it will be automatically used during the decoding stage in the UFED Physical Analyzer. If the user does not know the password, he can skip this step. (Figure 4.2.7)


Source

Encrypted Backup Password

iTunes backup encryption is enabled.
To preserve the password for the decoding stage enter it below (or press "Skip" if not known).
Note: If you cannot obtain the password (including brute-force attempts), contact Cellebrite CAIS to bypass the iTunes encryption.

1234

☑ Show Characters

Figure 4.2.7 File system extraction - Encrypted backup password (source: author)

8) The extraction to a local drive or removable storage device starts. (Figure 4.2.8)

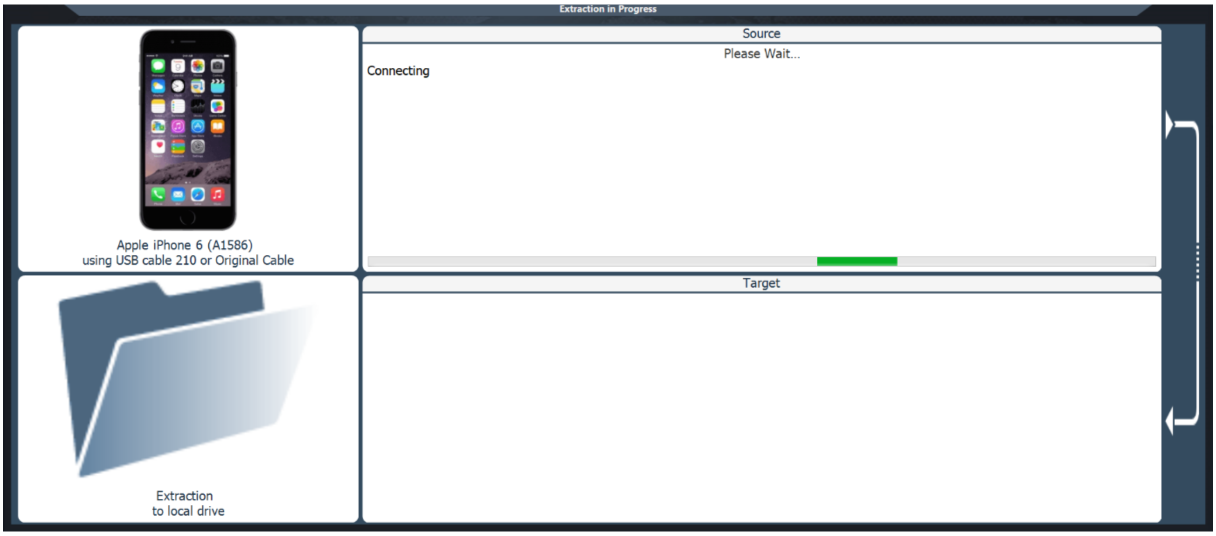
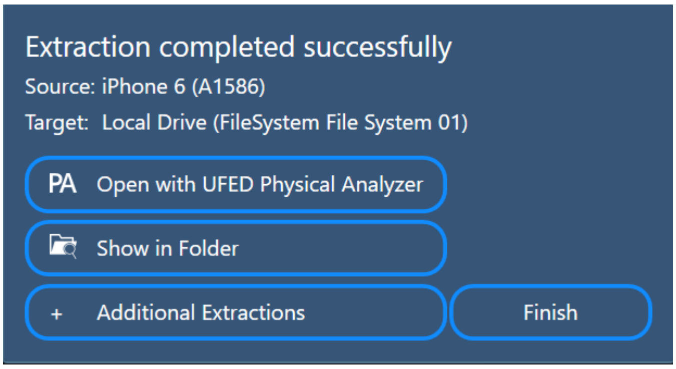


Figure 4.2.8 File system extraction - Extraction in progress (source: author)

9) When the extraction completes, the user may choose what actions he wants to perform. The available options were explained in step 8 of Logical extraction. (Cellebrite 4PC Manual, 2018) (Figure 4.2.9)



Extraction completed successfully

Source: iPhone 6 (A1586)

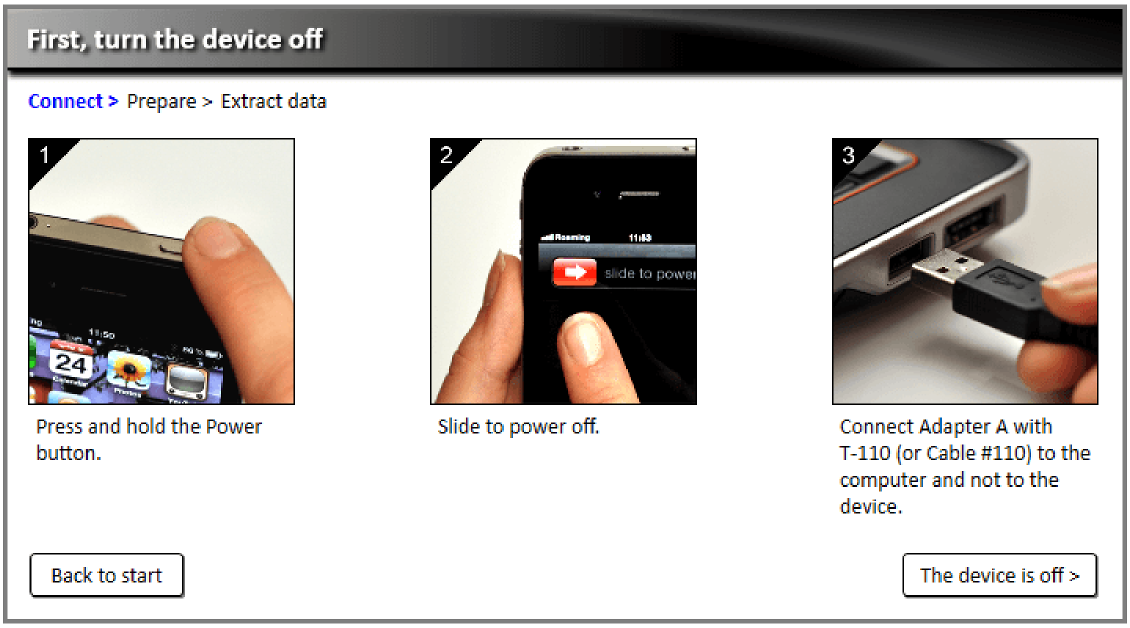
Target: Local Drive (FileSystem File System 01)

Figure 4.2.9 File system extraction - Extraction completed (source: author)

4.3 Physical extraction

Physical extraction is also available in the UFED 4PC, but this method supports primarily devices with Android operating systems. UFED Physical Analyzer provides physical mode as well, but only for iOS mobile devices with full root access, in other words, jailbroken iOS devices. The user can process the physical extraction using the steps described below.

1) After choosing the Physical mode, the user must turn the device off and click button The device is off. (Figure 4.3.1)



First, turn the device off

Connect > Prepare > Extract data

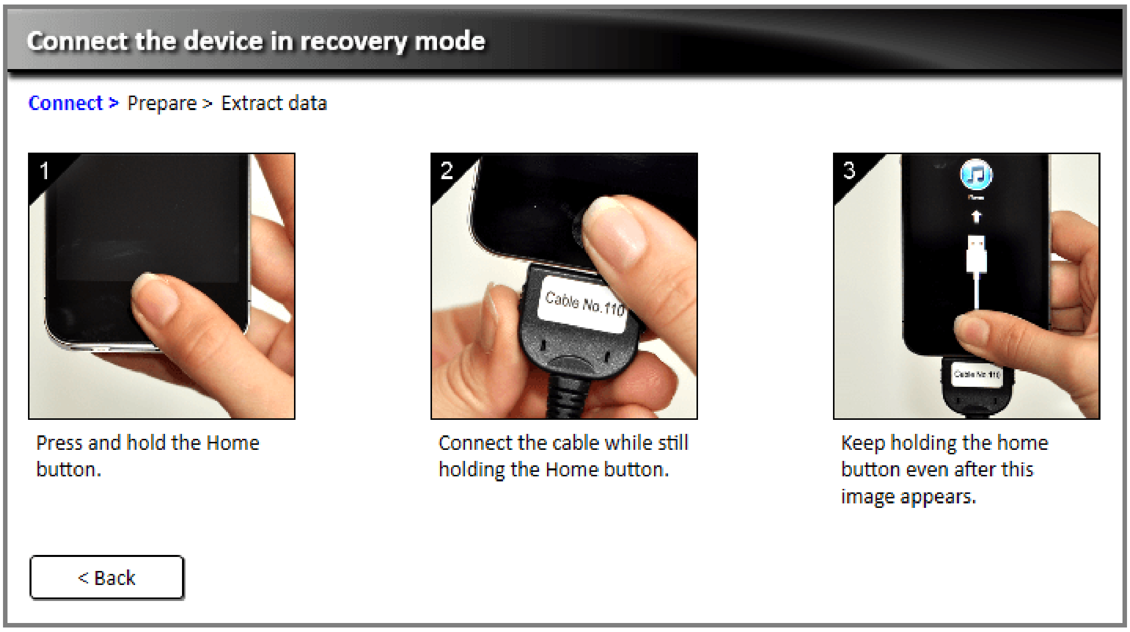
1 Press and hold the Power button.

2 Slide to power off.

3 Connect Adapter A with T-110 (or Cable #110) to the computer and not to the device.

Figure 4.3.1 Physical extraction - Turn the device off (source: author)

2) The user must follow the displayed instructions in order to activate the iOS mobile phone in Recovery Mode. (Figure 4.3.2)



Connect the device in recovery mode

Connect > Prepare > Extract data

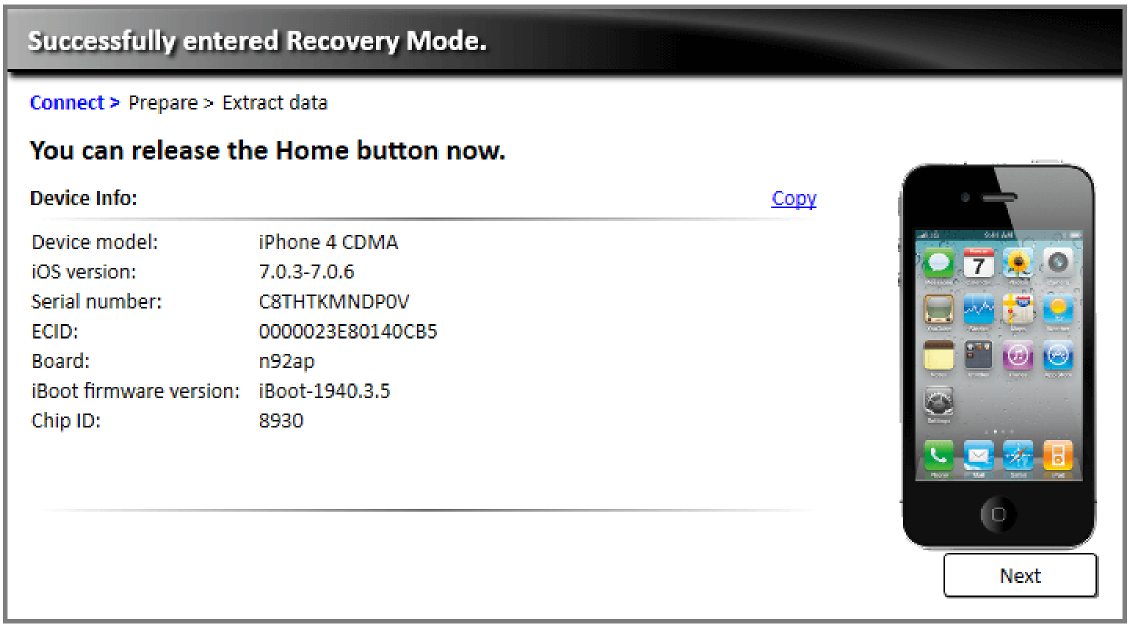
1 Press and hold the Home button.

2 Connect the cable while still holding the Home button.

3 Keep holding the home button even after this image appears.

Figure 4.3.2 Physical extraction - Connect in recovery mode (source: author)

3) After the device in Recovery Mode is detected, the device information is presented, such as iOS version, serial number, and more. Click Next. (Figure 4.3.3)



Successfully entered Recovery Mode.

Connect > Prepare > Extract data

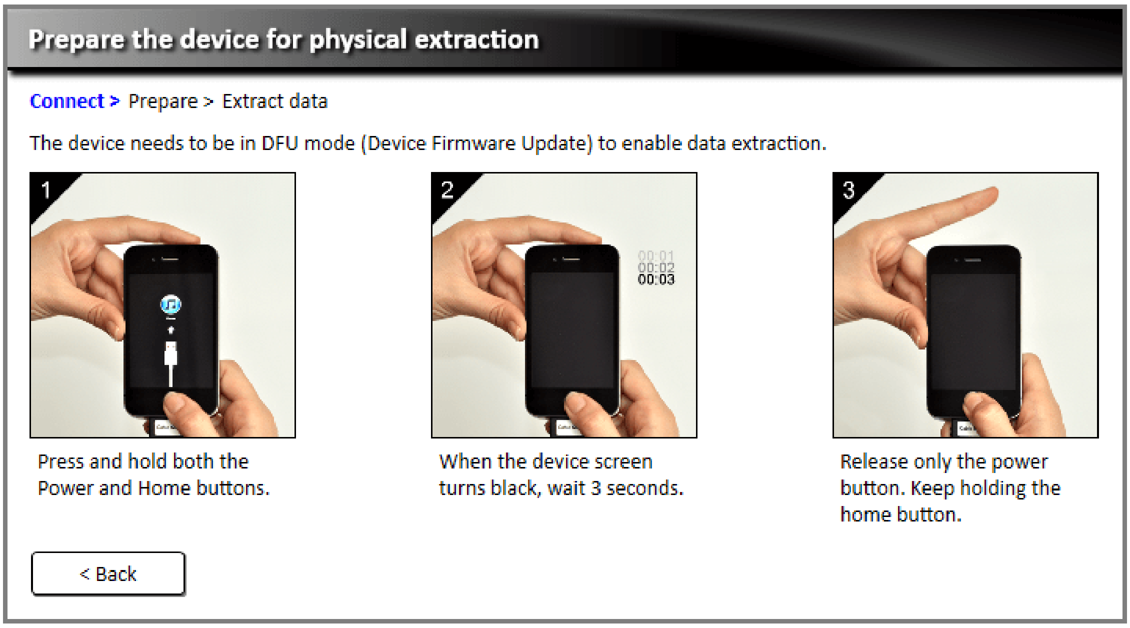
You can release the Home button now.

Device Info: Copy

Device model:	iPhone 4 CDMA
iOS version:	7.0.3-7.0.6
Serial number:	C8THTKMNDP0V
ECID:	0000023E80140CB5
Board:	n92ap
iBoot firmware version:	iBoot-1940.3.5
Chip ID:	8930

Figure 4.3.3 Physical extraction - Entered Recovery mode (source: (Cellebrite PA Manual, 2018))

4) The device needs to be entered into the Device Firmware Update mode (from now onwards DFU). For that the user must follow the steps on the screen of the forensic tool. (Figure 4.3.4)



Prepare the device for physical extraction

Connect > Prepare > Extract data

The device needs to be in DFU mode (Device Firmware Update) to enable data extraction.

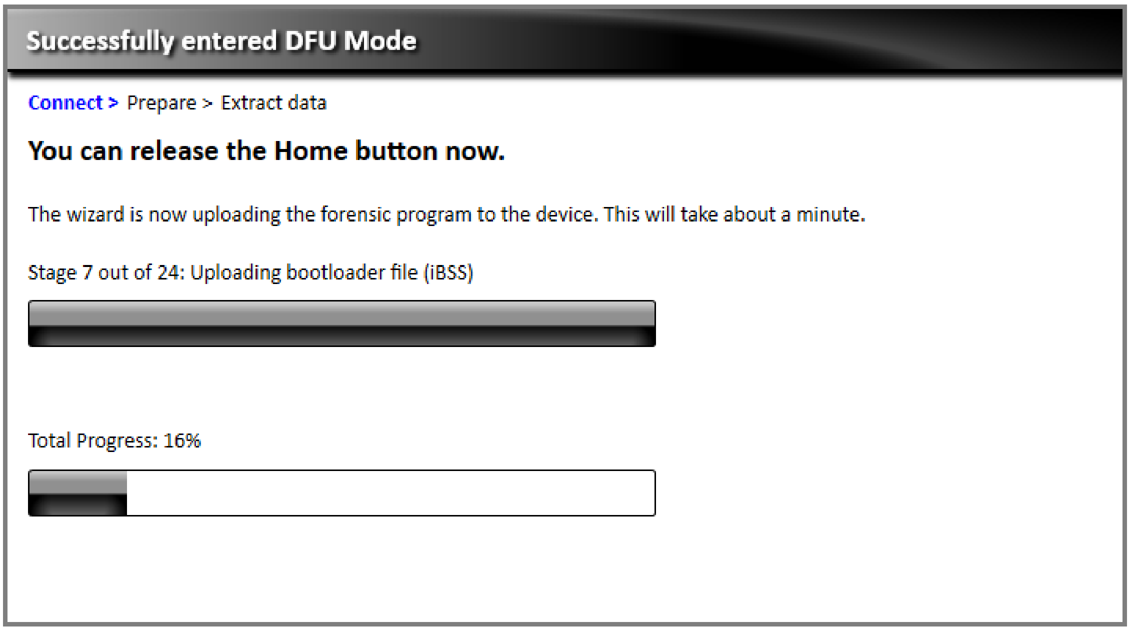
1 Press and hold both the Power and Home buttons.

2 When the device screen turns black, wait 3 seconds.

3 Release only the power button. Keep holding the home button.

Figure 4.3.4 Physical extraction - Prepare device (source: (Cellebrite PA Manual, 2018))

5) When the device is in DFU mode, the forensic program starts automatically uploading to the device. Then the device is ready for physical extraction. (Figure 4.3.5)



Successfully entered DFU Mode

Connect > Prepare > Extract data

You can release the Home button now.

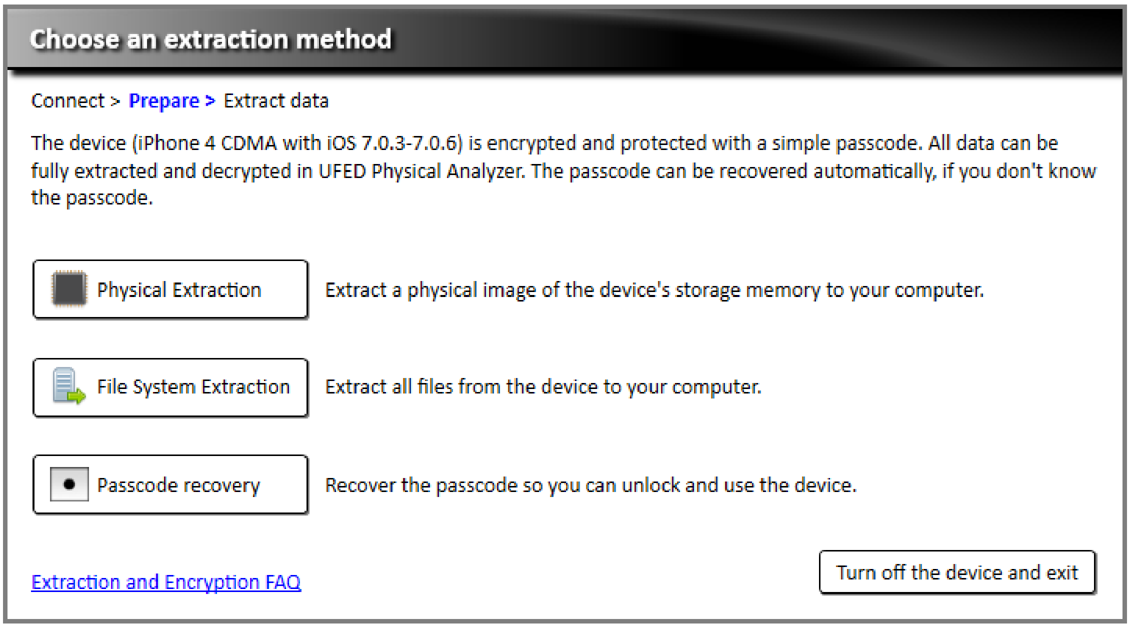
The wizard is now uploading the forensic program to the device. This will take about a minute.

Stage 7 out of 24: Uploading bootloader file (iBSS)

Total Progress: 16%

Figure 4.3.5 Physical extraction - Entered DFU mode (source: (Cellebrite PA Manual, 2018))

6) In the next step the Physical extraction mode must be chosen by the user. (Figure 4.3.6)



Choose an extraction method

Connect > Prepare > Extract data

The device (iPhone 4 CDMA with iOS 7.0.3-7.0.6) is encrypted and protected with a simple passcode. All data can be fully extracted and decrypted in UFED Physical Analyzer. The passcode can be recovered automatically, if you don't know the passcode.

Physical Extraction — Extract a physical image of the device's storage memory to your computer.

File System Extraction — Extract all files from the device to your computer.

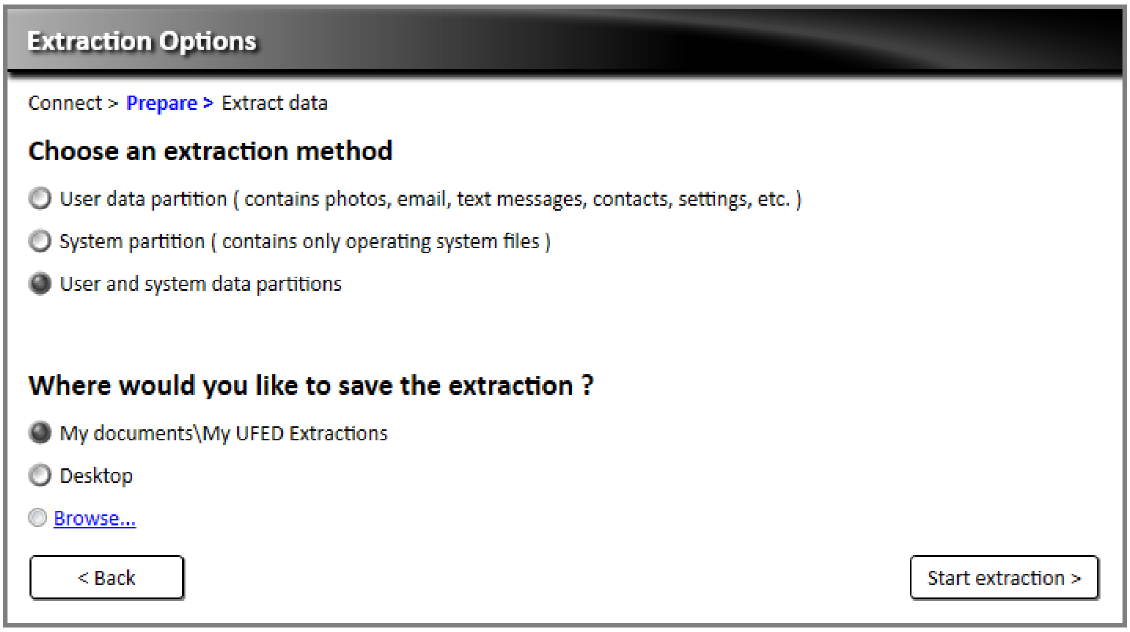
Passcode recovery — Recover the passcode so you can unlock and use the device.

Extraction and Encryption FAQ

Turn off the device and exit

Figure 4.3.6 Physical extraction - Extraction method (source: (Cellebrite PA Manual, 2018))

7) For Physical Extraction are available three methods: User data partition (contains photos, email, text messages, contacts, settings, etc.), System partition (contains only operating system files), or both. The user must choose the location to which he wants to save the extracted files. Click Start extraction. (Figure 4.3.7)



Extraction Options

Connect > Prepare > Extract data

Choose an extraction method

○ User data partition (contains photos, email, text messages, contacts, settings, etc.)

○ System partition (contains only operating system files)

● User and system data partitions

Where would you like to save the extraction ?

● My documents\My UFED Extractions

○ Desktop

○ Browse...

< Back

Start extraction >

Figure 4.3.7 Physical extraction - Extraction options (source: (Cellebrite PA Manual, 2018))

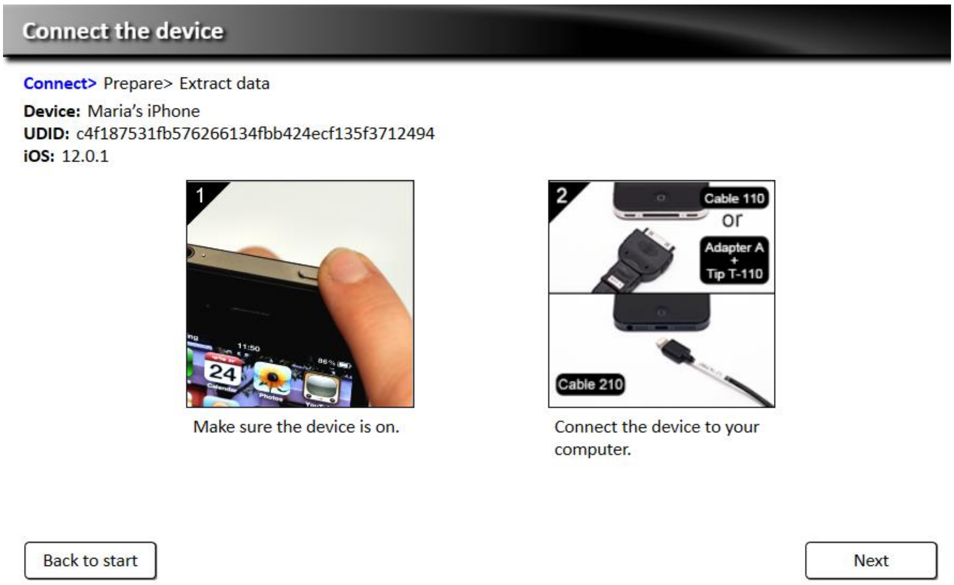
8) After extraction is completed the following options become available:

- Open in UFED Physical Analyzer, which loads the extraction file in the mentioned tool.
- Open file location.
- Turn off the device and exit.
- Back to extraction options, which returns the user to the extraction methods screen. (Cellebrite PA Manual, 2018)

4.4 Advanced Logical extraction

Advanced Logical extraction is available in the UFED Physical Analyzer. While conducting this type of extraction the device must be turned on in order to acquire its phonebook, call log, iMessages, SMSs, MMSs, calendar, pictures, video, audio, ringtones, application data, and more. The duration varies depending on the extraction method, the device model, the amount of data on the device, the extracting computer, and other parameters. The advanced logical extraction is saved to the selected location as a *.UFD file and a *.TAR file and can be opened in UFED Physical Analyzer to access all extracted information, including any deleted information. (Cellebrite PA Manual, 2018) The user can process the advanced logical extraction using the steps described below.

1) After choosing the Advanced Logical extraction, the user must turn the iOS device on and connect it to the computer either with a specified cable from a forensic accessory kit or a cable supplied with the device. (Figure 4.4.1)



Connect the device

Connect> Prepare> Extract data

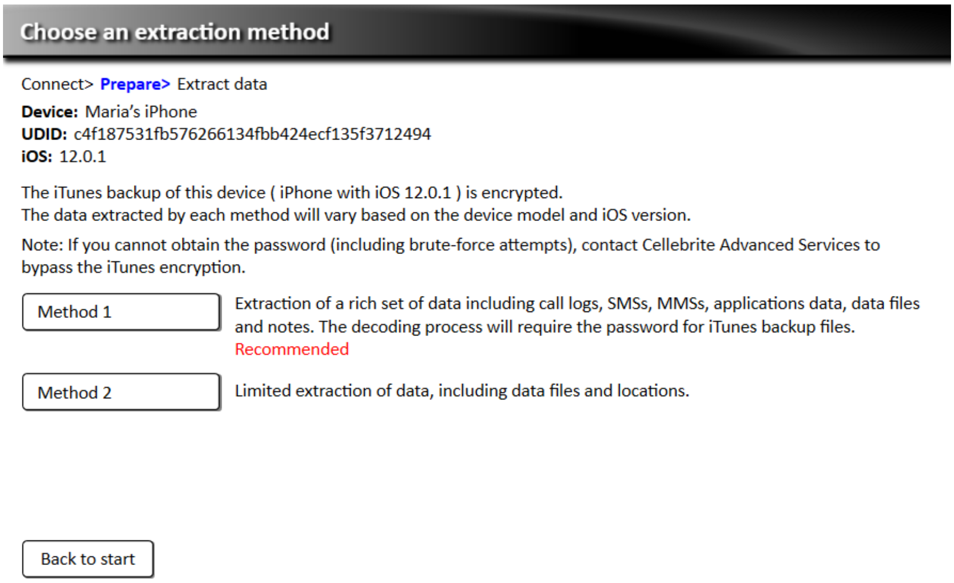
Device: Maria's iPhone
UDID: c4f187531fb576266134fbb424ecf135f3712494
iOS: 12.0.1

1 Make sure the device is on.

2 Connect the device to your computer.

Figure 4.4.1 Advanced logical extraction - Connect the device (source: author)

2) The user must select one of the displayed methods of Advanced Logical extraction. There are available three different methods depending on whether the device is encrypted and/or jailbroken (Figure 4.4.2):
   a. Method 1 extracts a wide range of data, such as SMSs, MMSs, application data and locations. This method does not obtain call logs, email body and attachments.
   b. Method 2 extracts a set of data that includes call logs, SMSs, MMSs, application data and locations. This method might require from the user entering the iTunes backup password.
   c. Method 3 extracts the widest range of data, which includes call logs, SMSs, MMSs, application data, data files and notes. On the picture below it is shown as Method 1.



Choose an extraction method

Connect> Prepare> Extract data

Device: Maria's iPhone
UDID: c4f187531fb576266134fbb424ecf135f3712494
iOS: 12.0.1

The iTunes backup of this device (iPhone with iOS 12.0.1) is encrypted.
The data extracted by each method will vary based on the device model and iOS version.

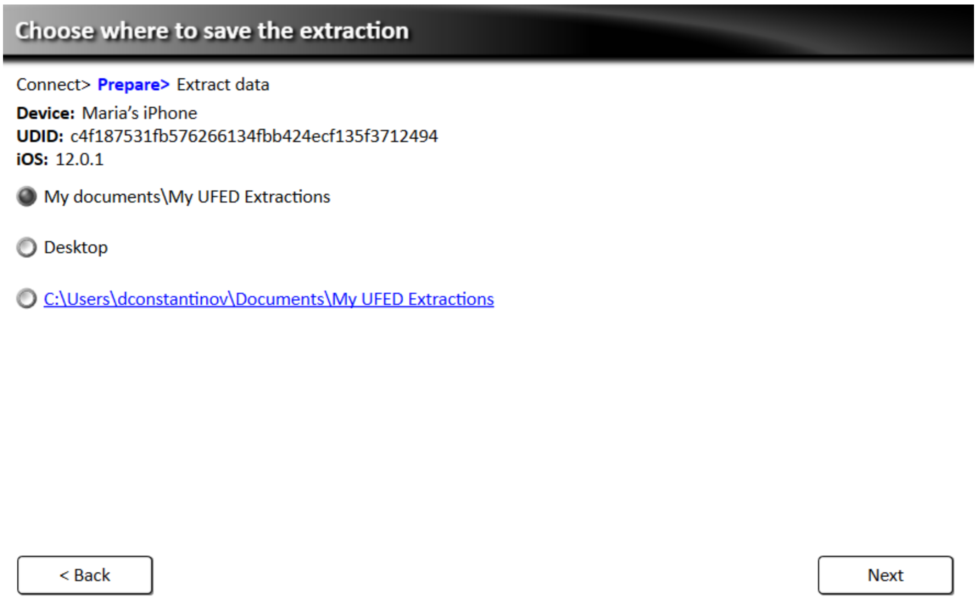
Note: If you cannot obtain the password (including brute-force attempts), contact Cellebrite Advanced Services to bypass the iTunes encryption.

Method 1 — Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. The decoding process will require the password for iTunes backup files. Recommended

Method 2 — Limited extraction of data, including data files and locations.

Figure 4.4.2 Advanced logical extraction - Methods for a non-jailbroken encrypted iOS device (source: author)

3) The user must choose the location for saving the extracted data. The location can be on the computer, removable storage device or a network. (Figure 4.4.3)



Choose where to save the extraction

Connect> **Prepare>** Extract data

Device: Maria's iPhone
UDID: c4f187531fb576266134fbb424ecf135f3712494
iOS: 12.0.1

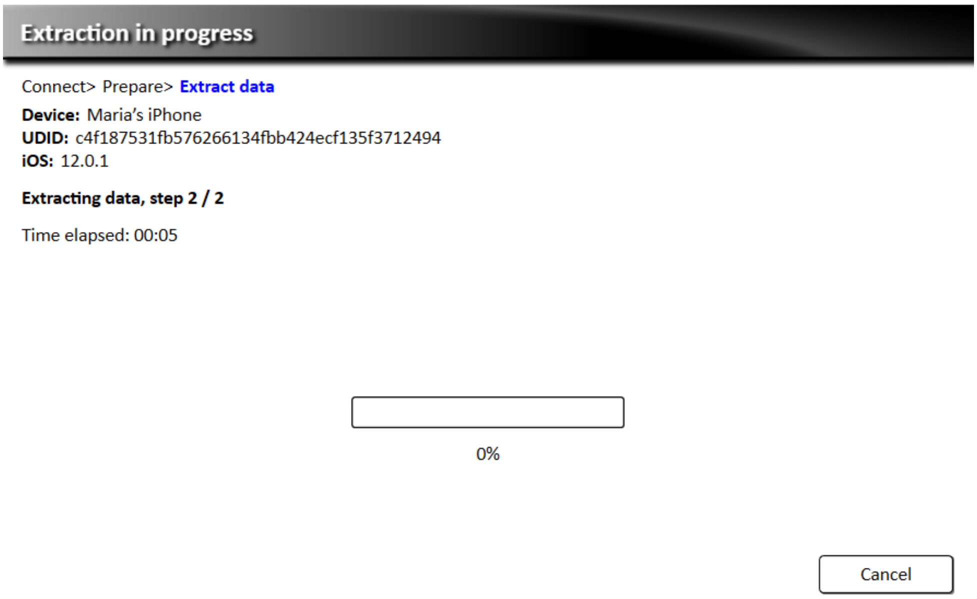
● My documents\My UFED Extractions

○ Desktop

○ C:\Users\dconstantinov\Documents\My UFED Extractions

Figure 4.4.3 Advanced logical extraction - Select location (source: author)

4) Appears next window that shows a progress of the extraction process. (Figure 4.4.4)



Extraction in progress

Connect> Prepare> **Extract data**

Device: Maria's iPhone
UDID: c4f187531fb576266134fbb424ecf135f3712494
iOS: 12.0.1

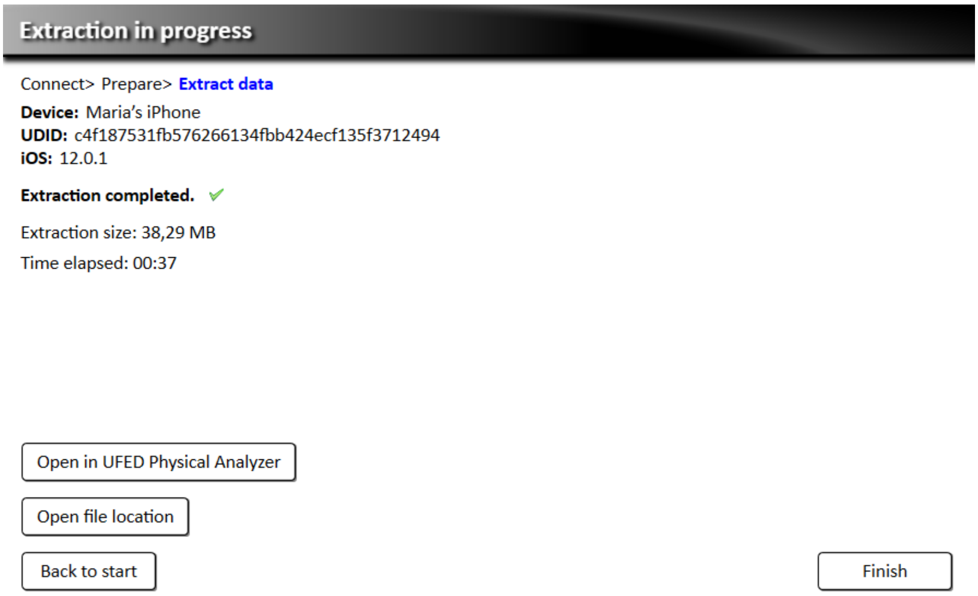
Extracting data, step 2 / 2

Time elapsed: 00:05

0%

Figure 4.4.4 Advanced logical extraction - Extraction in progress (source: author)

5) The extraction is completed and the user can choose from the available options. (Figure 4.4.5)



Extraction in progress

Connect> Prepare> **Extract data**

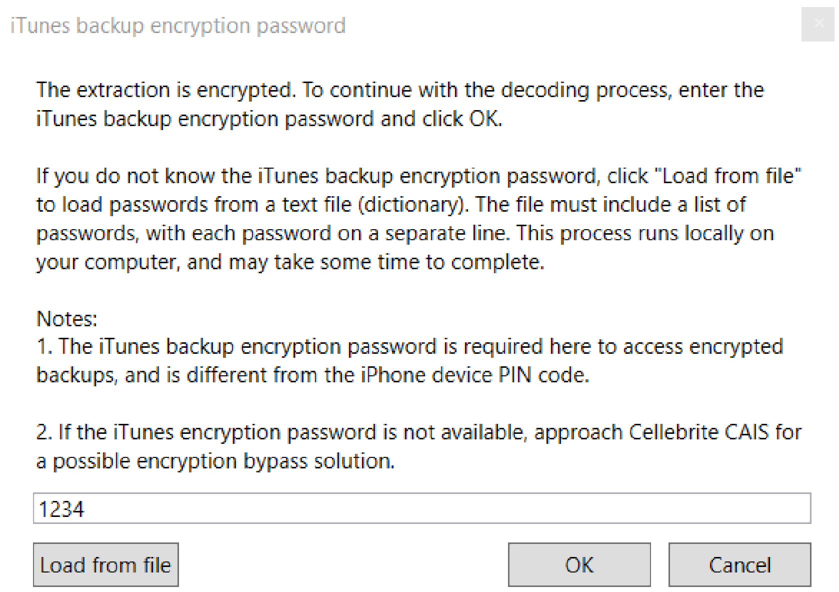
Device: Maria's iPhone
UDID: c4f187531fb576266134fbb424ecf135f3712494
iOS: 12.0.1

Extraction completed. ✓

Extraction size: 38,29 MB
Time elapsed: 00:37

Figure 4.4.5 Advanced logical extraction - Extraction completed (source: author)

6) To open the encrypted extraction in the UFED Physical Analyzer, the iTunes backup encryption password is required to continue the decoding process. (Figure 4.4.6)



iTunes backup encryption password

The extraction is encrypted. To continue with the decoding process, enter the iTunes backup encryption password and click OK.

If you do not know the iTunes backup encryption password, click "Load from file" to load passwords from a text file (dictionary). The file must include a list of passwords, with each password on a separate line. This process runs locally on your computer, and may take some time to complete.

Notes:
1. The iTunes backup encryption password is required here to access encrypted backups, and is different from the iPhone device PIN code.

2. If the iTunes encryption password is not available, approach Cellebrite CAIS for a possible encryption bypass solution.

1234

Figure 4.4.6 Advanced logical extraction - iTunes backup encryption password (source: author)

5 Analysed applications

Nowadays people cannot imagine their lives without their mobile phones. The reason for that is the constant need of keeping in touch with their friends and family, reading news and books, watching movies and videos for self-development, exploring new restaurants and cities, etc. Most of these activities the user is able to conduct in three types of mobile applications, such as communication, browsing, and maps & navigation. This chapter is devoted to all three of them and introduces the reader to four applications from each category, which are later used in the practical part of this bachelor's thesis.

5.1 Communication

For the purpose of this paper were chosen three applications for communication that make the list of the most popular social networking applications throughout the world and one application, which is available only for Apple devices. Thereby the forensic analysis is conducted on the following apps: Messenger, WhatsApp, Viber and iMessage.

5.1.1 Messenger

Facebook messenger (more commonly known as Messenger) is a messaging app developed by Facebook, Inc. According to the App Store Messenger is available in 28 languages, requires iOS 9.0 or later version and is compatible with iPhone, iPad, and iPod touch. The size of the application is 246.1 MB. As of 20 November 2018, the latest version of the app is 193.0, which was released on 20 November 2018. (Apple, 2018)

Messenger offers the ability to communicate with friends from Facebook as well as with other contacts in the user's phone book, who might not have a Facebook account, but they have the Messenger app installed on their phones. The app gives the opportunity to create group chats, name them, set group photos and make a group phone or video call. The users are able to send photos and videos from their camera roll, take pictures, record videos and voice clips right from the app. They can send different types of documents to their friends as well. Messenger offers some further features, such as sending and sharing user's location for 60 minutes, creating plans and polls in group chats. Users can express their emotions with the help of emoji, stickers and images in the Graphics Interchange Format (from now onwards GIFs).

5.1.2 WhatsApp

WhatsApp is one of the applications that is included in a top list of the most used social networking apps. It was developed by WhatsApp Inc. and later owned by Facebook, Inc. The app is available in more than 35 languages and requires iOS 8.0 or later version of operating system. WhatsApp is compatible with iPhone and its size is 134.8 MB. This free messaging application gives user the opportunity to message and call friends and family by using his phone's internet connection.

WhatsApp works with the user’s phone number and integrates seamlessly with the phone's existing address book. Among the main features of the WhatsApp the user can find:

- sending and receiving photos, videos, documents, stickers, GIFs, and Voice Messages;
- available group chats with the user’s contacts;
- being always logged in so the user doesn't miss messages;
- even if the user misses his notifications or turns off his mobile phone, WhatsApp saves his recent messages until the next time he uses the app;
- marking messages as “Starred Messages”, which can be later found in the separate folder;
- sharing location, exchanging contacts, setting custom wallpapers and notification sounds, email chat history, broadcast messages to multiple recipients at once, and more. (Apple, 2018)

5.1.3 Viber

Viber is a messaging application that is developed by Rakuten, Inc. and is translated into more than 35 languages. It is compatible with iPhone, iPad, and iPod touch and requires iOS 9.3 or later version. The application takes 245.1 MB of the phone’s memory space. The user must be at least 17 years old to download this app. After downloading Viber user can expect to find the following features:

- creating group chats with up to 250 participants and opportunity to “like” messages when the user doesn’t have time to reply;
- no need to set up a username or provide login information;
- sending voice or video messages;
- secured communications and trusted contacts - all messages and calls are protected by end-to-end encryption;
- expressing emotions with stickers;
- deleting messages for everyone, not only for the sender;
- hiding chats that user doesn’t want to be visible in his chat list and accessing them later with a PIN;
- instant video messages that are recorded when the user taps and holds the instant video icon to capture the moment with 30-second videos and releases to send;
- chatting with favourite brands, businesses and personalities that have Public Accounts, and following them for news and updates;
- games, sharing contacts and location, being able to see message information including who has seen and liked it, and more. (Apple, 2018)

5.1.4 iMessage

iMessage is a messaging application developed by Apple Inc. that serves for sending messages over a cellular network, mobile phone internet access, and Wi-Fi. It is compatible with iPhone, iPad, and iPod touch. Users are able to express themselves in richer ways by sending stickers, emoji, and voice clips. iMessage allows users to send photos and videos from their camera roll, taking pictures and recording a video right in the app. The user has the opportunity to share his location as well. The app is integrated into iOS thus it cannot be deleted from the device. (Apple, 2018)

5.2 Browsing

In today's society browsers are constantly used throughout the day by millions of people. Users look for the new information, which they intend to use for their education, entertainment, work, personal development, etc. Every day dozens of questions arise in people's minds, and thus browsing application becomes one of the fastest ways to find the answer. The following subsection describes four browsing applications that a person seeking the answer can find in the App Store.

5.2.1 Google Chrome

One of the most popular browsing applications nowadays is Google Chrome, which is compatible with iPhone, iPad, and iPod touch. It requires iOS 10.0 or later version of the operating system and is translated into more than 35 languages. The app is developed by Google LLC and its size is 107.6 MB. The lower age limit for downloading Google Chrome is 17.

Google Chrome offers to a user the following main features:

- creating bookmarks;
- translating an entire site in a single click with Google Translate built-in;
- ability to autofill not only passwords but also user's address and payment details;
- using voice search to find answers on-the-go without typing;
- synchronizing open tabs, bookmarks, history and passwords across different devices after signing into Chrome;
- easy access to recently closed tabs;
- browsing in incognito mode, which prevents the app from remembering history or cookies, but at the same time allows the user to save new bookmarks;
- adding web pages to a reading list, and more. (Apple, 2018)

5.2.2 Firefox

Firefox Web Browser (more commonly known as Firefox) is developed by Mozilla Corporation and is available in more than 70 languages. The app is compatible with iPhone, iPad, and iPod Touch and requires iOS 10.3 or later version. Firefox takes only 98.8 MB from the iPhone memory space and has an age limit, thereby the user must be at least 17 years old to download this application.

Main features of the Firefox browser are:

- creating bookmarks;
- enabling reading mode;
- ability to autofill passwords;
- synchronizing open tabs, bookmarks, history and passwords across different devices that have installed Mozilla Firefox browser;
- easily access shortcuts to search providers including Wikipedia, Twitter and Amazon;
- enabling night mode that applies not only to the application interface but also to all web pages;

- browsing in private mode, which prevents the app from remembering history or cookies, but at the same time allows the user to save new bookmarks;
- adding web pages to a reading list;
- hiding images on web pages;
- enabling tracking protection, and more. (Apple, 2018)

5.2.3 Safari

Safari is a default web browser on iOS mobile devices and is developed by Apple Inc. The browser does not have its own page in the App Store and cannot be uninstalled from the mobile devices running iOS, only deactivated.

The application provides users with the following features:

- synchronizing passwords, bookmarks, history, tabs, names, credit card numbers, and Reading List across Apple devices using iCloud;
- creating bookmarks;
- saving web pages to the Reading List in order to read them later, even without the internet connection;
- enabling Reading mode, where the user can change font style, font size, and colour of background;
- using private browsing prevents Safari from remembering pages the user visited, his search history, and autofill information;
- adding web pages to Favourites or Home screen;
- creating PDF from the web pages, and more. (Apple, 2018)

5.2.4 Opera Mini

Opera Mini web browser (commonly known as Opera Mini) is developed by Opera Software and is translated into more than 30 languages. It is compatible with iPhone, iPad and iPod touch and requires iOS 9.0 or later version of operating system. The size of the web browser is 77.1 MB. Opera mini is primarily focused on saving data while browsing. After downloading the application, the user has access to various features among which he can find the following:

- getting the latest news on the start page that serves user the top stories and freshest content from across the web;
- choosing from search results that appear as the user types;
- quick access to previously visited pages;
- blocking advertisements and saving screen space for the content the user wants to see;
- reducing mobile data usage by up to 90%;
- opening an unlimited number of tabs;
- using private tabs to browse incognito without leaving a trace on user’s device;
- smart night mode that lets the user read more comfortably in the dark;
- video boost that saves lots of data on videos, and more. (Apple, 2018)

5.3 Maps & Navigation

As time went by, people started to put aside their paper maps and began to use map applications on their mobile phones, where they could easily zoom in or out on the map, turn on the navigation to the point of their destination and more. Nowadays maps are constantly changing, new roads come into service, new traffic regulations are applied on different road sections. From this point of view, it becomes easier to only once install a map application on your phone, instead of spending money and wasting paper on the new paper maps. This type of applications allows the user to get to his home or office in the shortest possible time by calculating the fastest route based on up-to-the-minute information about traffic. Users give their preference to technological advancements that offer more features and easier understanding. This subsection introduces the reader to the four navigation applications that can be downloaded from the App Store.

5.3.1 Google Maps

Google Maps - Transit & Food (more commonly known as Google Maps) was developed by Google LLC. The app is available in more than 30 languages and is compatible with iPhone, iPad, and iPod touch. In order for Google Maps to work properly, the Apple device must be running iOS 10.0 or later version of operating system. The size of the application is 192.6 MB. Over 220 countries and territories are mapped, and hundreds of millions of businesses and places are marked on the map. The user is able to get real-time GPS navigation, traffic, and transit info, and explore local neighbourhoods by knowing where to eat, drink and go - no matter what part of the world he is in.

The user of Google Maps has access to the following features:

- automatic rerouting based on live traffic, incidents, and road closures;
- real-time transit info that helps to catch a bus, train, etc.;
- deciding more confidently with “Your match” that displays a number on how likely the user is to like a place;
- group planning that requires sharing a shortlist of options and involves voting in real-time;
- creating lists of favourite, “Want to go”, and “Starred” places and sharing them with others;
- offline maps to search and navigate without an internet connection;
- Street View and indoor imagery for restaurants, shops, museums and more. (Apple, 2018)

5.3.2 Maps

Application Maps is developed by Apple Inc. and its size is 1.4 MB. The app is compatible with iPhone, iPad and iPod touch, and requires iOS 10.0 or later version. Maps is translated into more than 30 languages and among its main features the user can find the following:

- suggesting the best route that avoids traffic;
- using voice-guided turn-by-turn navigation when driving or walking;
- guidance on which lane the user should be in, and the current speed limit;
- along the way, the app can factor in real-time traffic conditions, incidents, and road closures, so the user knows exactly how long until he arrives;
- searching and browsing by category, including food, drink, shopping;
- looking up information about places, including hours, photos, ratings, and reviews;

- making restaurant reservations, dialling phone numbers, and opening websites directly from within Maps;
- getting transit schedules and directions via subways, buses, trains, and ferries;
- viewing major cities around the world with photo-realistic, interactive 3D views using Flyover.
- automatic night mode;
- finding a parked car and getting directions to it, and more. (Apple, 2018)

5.3.3 Mapy.cz

Mapy.cz is a Czech mapping application developed by Seznam.cz. The size of the app is 133.1 MB and it is compatible with iPhone, iPad, and iPod touch. Mapy.cz is available in English and Czech languages and requires iOS 10.3 or later version of operating system. The application has numerous features, most of which are available without internet access. Among multiple features of the Mapy.cz the user can find the following:

- looking through and sorting out saved and recorded trips in “My Maps”;
- synchronizing “My Maps” across multiple devices after logging in;
- planning routes and navigating to points of destination even with no cellular service;
- offline tourist maps with marked tourist trails and bikeways;
- offline voice navigation for drivers, bikers and hikers in 7 languages (Czech, English, Polish, German, French, Spanish, and Russian);
- trip tips in the surrounding area;
- tracker for recording user’s routes and sharing them;
- offline route planning with an unlimited number of passing-through points;
- elevation profiles for a car, a bike or a hike;
- offline winter maps with cross-country skiing tracks and ski resorts;
- satellite maps and 3D view;
- first aid guide and sharing location in case of emergency;
- up-to-date fuel prices at petrol stations in Europe, and more. (Apple, 2018)

5.3.4 Waze

Waze is a GPS navigation application developed by Waze Mobile, which later was acquired by Google LLC. The app is available in more than 40 languages and requires iOS 9.0 or later version. Waze is great for navigation, especially during long road trips and daily commutes, and its size is 167 MB. To its users Waze offers the following features:

- receiving notifications about traffic, police, hazards and more while driving;
- instant routing changes to avoid traffic and save driver’s time;
- playing favourite applications for music, podcasts and more right from Waze;
- arrival time is based on live traffic data;
- searching for the cheapest gas along the route;
- choosing from a variety of voices to guide the user while he is driving, and more. (Apple, 2018)

6 Description of methodology

In this chapter is described the procedure of preparing necessary devices (laptop and mobile phone), generating dataset and conducting supplementary actions for the purpose of the study.

Tools and software used for the achievement of the goal in this bachelor's thesis are presented in the table below. (Table 6.3-1)

Table 5.3-1 Tools and Software used in the practical part

Device / Software	**Purpose**	**Model / Version**
Mobile phone	A device that had analyzed applications installed on it	iPhone 6, model A1586
OS of the mobile phone	Platform for carrying out the experiment	iOS 12.1
Laptop	A device that had two software forensic tools installed on it for the purpose of the experiment	Lenovo ThinkPad T480s
OS of the laptop	Platform for performing acquisition of the mobile device	Microsoft Windows 10 Enterprise, version 10.0.16299 Build 16299
UFED 4PC	Software used for conducting two types of extractions	7.10.1.1080
UFED Physical Analyzer	Software used for conducting a type of extraction	7.11.1.1
Cellebrite UFED dongle	The hardware license key that is essential for the work of the two forensic tools	The license is valid until 7 February 2019

For the experiment was chosen encrypted mobile phone manufactured by Apple, specifically iPhone 6, on account of the fact that for iOS devices is available greater number of extractions in the Cellebrite UFED in comparison with Android devices. In the first step of the preparation was created an Apple ID, specifically mkonty@icloud.com, and fictitious user's name was set to Maria Konty. As soon as the initial setting has been completed, three types of selected applications were installed on the iPhone from the App Store. Applications for socializing included Messenger, Viber, and WhatsApp. Among browsing applications were Google Chrome, Firefox, and Opera Mini. Google Maps, Mapy.cz, and Waze can be found in the list of navigation applications. Additional 3 apps, specifically iMessage, Safari and Maps, were preinstalled on the mobile device, thus did not require any additional manual installation. The author did not change any settings of the installed applications. A total of twelve applications were prepared for further examination on the iPhone. Following this, a set of data was generated. Performed activities are specified in the following subchapters for each type of applications.

At the same time, the author was preparing the laptop that was used for the future extractions. Two software forensic tools, namely Cellebrite UFED 4PC and UFED Physical Analyzer, were downloaded and installed on the laptop from the developer website. In order to access links for downloading mentioned software, the author was given user credentials with the help of which he logged on to the registered account on the Cellebrite's website. On the website among others can be found software updates, license information, latest release notes, documentation, etc.

For a forensic examiner it is crucial to ensure the integrity of the examined evidence. Therefore, the extractions were performed in a forensically sound environment. It was essential to disable cellular and wireless networks by switching on the airplane mode on the iPhone, before attaching it to the forensic workstation. The mobile device, which was identified for the collection, was connected to the mentioned laptop via USB 2.0 cable. The process of acquiring the phone image was performed multiple times, due to the necessity of making certain amendments. On the mobile phone were performed a total of three types of extractions, specifically logical, file system, and advanced logical. The physical extraction could not be conducted, as the mobile phone was not supported by the UFED Physical Analyzer. The processes of performing each extraction were described in the chapter 4. For opening specific types of files, for example, audio files, GIFs, the author used a web browser, specifically Google Chrome.

6.1 Activities performed in the applications

In this subchapter are described activities that were performed in three types of applications in order to generate a set of data for future examination.

6.1.1 Communication

For the purpose of this bachelor's thesis dummy accounts on Facebook, WhatsApp, and Viber were created. iMessage does not require any registration, as it is automatically tailored to the Apple ID and the phone number. The actions that were performed for the purpose of the study are outlined in the following list:

1) Creating Group chats in applications that consist of three members.
2) Making calls in personal and group chats.
3) Interacting in personal and group chats and deleting some messages, which were both received and sent. In Viber and WhatsApp, a message was also deleted for everyone.
4) Sending and receiving photos, videos, audio clips, GIFs, stickers, emoji in the conversations.
5) Creating Secret Conversation and interacting with another user in Messenger and Viber.
6) Setting timer in the secret conversation that is intended to delete a message after a specified time, where countdown starts the moment the recipient has read the message.
7) Sharing location in personal and group chats.
8) Conducting a poll in group chats, voting and adding options to the poll in Messenger.
9) Creating plans in personal and group chats in Messenger.
10) Deleting one of the conversations.
11) Creating in WhatsApp Broadcast list and sending a broadcast message to two recipients at once without creating a group chat that includes selected participants.
12) Adding a reaction to some messages in Messenger and iMessage.

6.1.2 Browsing

The data, which were used in this study, were generated by the user, who followed the same steps in each application. Performed activities in applications for browsing are presented in the list below:

1) Some tabs were left open in the normal as well as in the private (or incognito) mode.
2) In both modes were visited some websites, and then the tabs were closed.
3) From browser history were deleted visited pages from a website www.CSFD.cz.
4) Website www.notino.cz was saved as a bookmark.
5) In browsers Google Chrome, Mozilla Firefox and Safari were saved login credentials for the website www.notino.cz. Browser Opera Mini did not offer such an opportunity.
6) Page from the website www.kinopoisk.ru was added to the "Reading list" in Chrome, Mozilla Firefox, Safari. Opera Mini does not support the mentioned function.
7) In private mode was opened website www.servis24.cz and the tab was not closed.
8) In private mode was opened website www.ted.com and the tab was closed afterwards.

6.1.3 Maps & Navigation

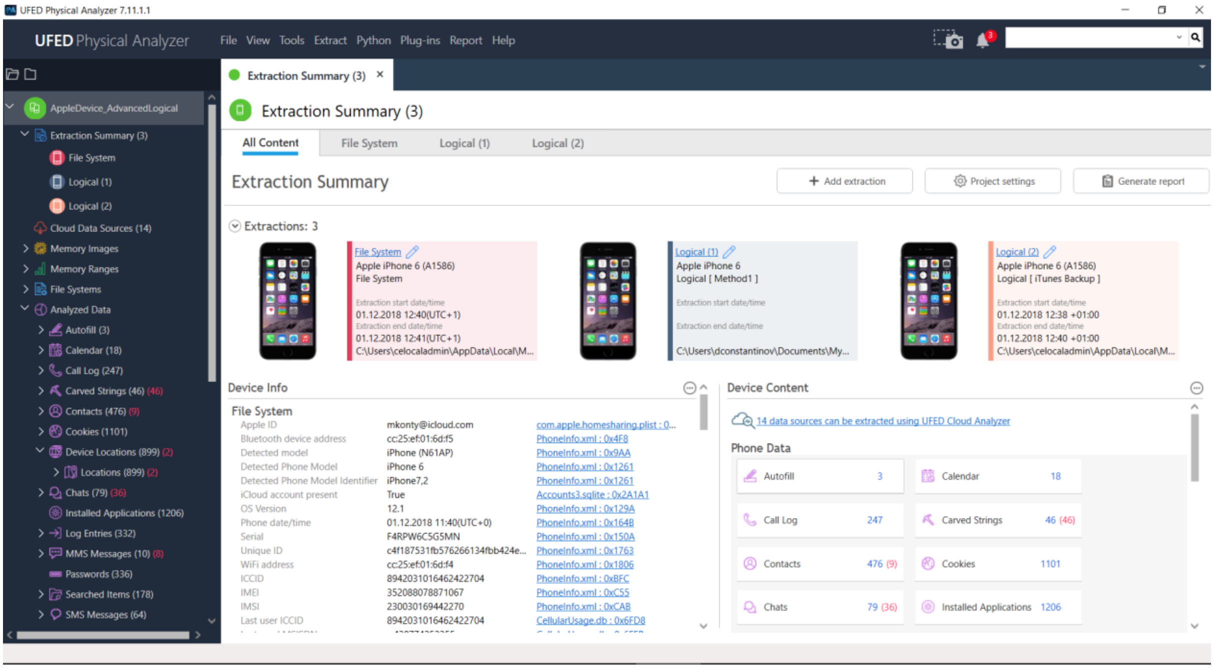
For the purpose of the study, the author used a similar procedure while generating the data in four applications for navigation. The actions that were performed by the user are outlined in the following list:

1) Logging on to the Google Chrome and Mapy.cz.
2) Using all four applications during the movements around the city.
3) Setting destination points and turning the navigation on.
4) Setting addresses for home and work, and saving favourite places.
5) Turning on the tracker in Mapy.cz that is used for recording the user's activity.
6) Turning on the timeline function in Google Maps. The mentioned function rediscovers locations the user has been to and records his routes.

While using the applications the user was constantly switching between all of them. In this way, he could guarantee that none of the running applications would stop working during the navigation.

7 Forensic analysis

The forensic analysis of the acquired data was performed using the UFED Physical Analyzer. This forensic tool gives the user an opportunity to open multiple extractions in the same project, that enables automatic aggregation and deduplication of data. The forensic tool also offers to generate a report with the specified types of acquired data. The author generated a report with all necessary types, which is now a part of this bachelor's thesis as an attachment that was not printed out. The image below demonstrates three types of extractions, namely File System, Logical (1) (stands for Advanced Logical), and Logical (2) (stands for Logical), that are opened in one project. (Figure 7.1) For the examination were used various functions, which are available in the UFED Physical Analyzer. Among used functions can be found the following: search in the whole project and in separate tabs, display only deleted items, open a conversation view, retrieve a physical address for locations, filter by the presence of deduplications and by the majority of available information that is separated into columns, and more. Findings for each application are presented in the following subchapters.



File System
Apple iPhone 6 (A1586)
File System
Extraction start date/time
01.12.2018 12:40(UTC+1)
Extraction end date/time
01.12.2018 12:41(UTC+1)
C:\Users\celocaladmin\AppData\Local\M...

Logical (1)
Apple iPhone 6
Logical [Method1]
Extraction start date/time
Extraction end date/time
C:\Users\dconstantinov\Documents\My...

Logical (2)
Apple iPhone 6 (A1586)
Logical [iTunes Backup]
Extraction start date/time
01.12.2018 12:38 +01:00
Extraction end date/time
01.12.2018 12:40 +01:00
C:\Users\celocaladmin\AppData\Local\M...

Device Info

File System

Apple ID	mkonty@icloud.com	com.apple.homesharing.plist : 0...
Bluetooth device address	cc:25:ef:01:6d:f5	PhoneInfo.xml : 0x4F8
Detected model	iPhone (N61AP)	PhoneInfo.xml : 0x9AA
Detected Phone Model	iPhone 6	PhoneInfo.xml : 0x1261
Detected Phone Model Identifier	iPhone7,2	PhoneInfo.xml : 0x1261
iCloud account present	True	Accounts3.sqlite : 0x2A1A1
OS Version	12.1	PhoneInfo.xml : 0x129A
Phone date/time	01.12.2018 11:40(UTC+0)	PhoneInfo.xml : 0x164B
Serial	F4RPW6C5G5MN	PhoneInfo.xml : 0x150A
Unique ID	c4f187531fb576266134fbb424e...	PhoneInfo.xml : 0x1763
WiFi address	cc:25:ef:01:6d:f4	PhoneInfo.xml : 0x1806
ICCID	8942031016462422704	PhoneInfo.xml : 0xBFC
IMEI	352088078871067	PhoneInfo.xml : 0xC55
IMSI	230030169442270	PhoneInfo.xml : 0xCAB
Last user ICCID	8942031016462422704	CellularUsage.db : 0x6FD8

Device Content

14 data sources can be extracted using UFED Cloud Analyzer

Phone Data

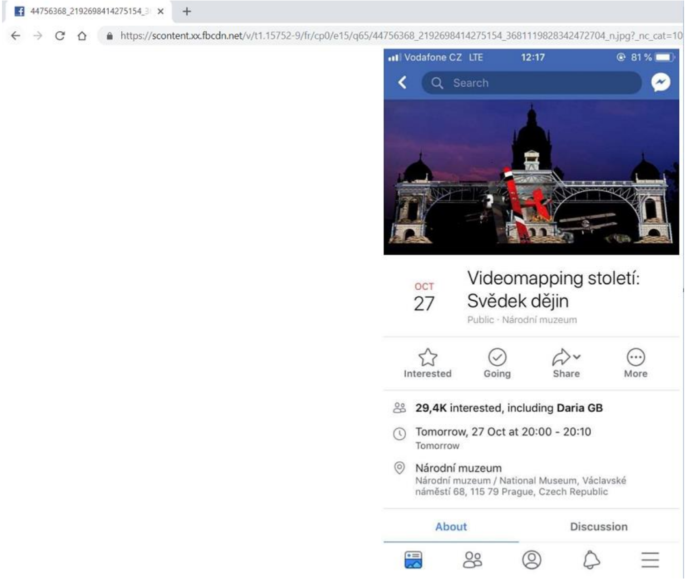
Autofill	3	Calendar	18
Call Log	247	Carved Strings	46 (46)
Contacts	476 (9)	Cookies	1101
Chats	79 (36)	Installed Applications	1206

Figure 6.1 Three types of extractions in one project (source: author)

7.1 Findings in Messenger

The examination showed, that all current messages from open conversations were extracted from the Messenger. However, the UFED Physical Analyzer was not able to extract certain messages, that were previously deleted from opened conversations. No evidence of secret conversation was found as well. Messages, which had videos attached to them, contained only a path, that appeared as 'video/video-1540487208.mp4' and could not be opened. At the same time, messages, which had images attached to them, additionally consisted of a path that could be opened in any web browser and viewed as an image. As an example, the author opened a link from one message in Google Chrome web browser that displayed a screenshot, which was attached to the chosen message. (Figure 7.1.1)

Among others the extracted data included information about contacts, call logs, and shared locations. Plans and polls, created by the user in conversations were also revealed by forensic tools. However, the extractions did not contain any information about reactions that were added to the messages by interlocutors. Audio clips could not be opened, and stickers and GIFs could not be viewed as well.



https://scontent.xx.fbcdn.net/v/t1.15752-9/fr/cp0/e15/q65/44756368_2192698414275154_3681119828342472704_n.jpg?_nc_cat=10

OCT 27 Videomapping století: Svědek dějin

Public · Národní muzeum

29,4K interested, including Daria GB

Tomorrow, 27 Oct at 20:00 - 20:10
Tomorrow

Národní muzeum
Národní muzeum / National Museum, Václavské náměstí 68, 115 79 Prague, Czech Republic

Figure 7.1.1 Image opened in Google Chrome from a link (source: author)

Deleted conversations deserve special mention. One of the multiple extractions was conducted an hour after one of the conversations in Messenger was deleted. In this case, the forensic tools were able to obtain messages from the deleted conversation. Another extraction was performed two days later, and this time the acquired data did not contain previously deleted conversation. This finding indicates that recently deleted conversations are still kept in the phone's memory cache.

7.2 Findings in WhatsApp

The analysis of the extractions revealed that forensic tools were able to acquire contacts, call logs, GIFs, and shared locations in WhatsApp. Deleted messages in conversations weren't obtained during the acquisition process, but all other presented messages were displayed in the UFED Physical Analyzer. WhatsApp also offers a function that gives the user an opportunity to delete a particular message for everyone. After this action is performed, the deleted message is replaced with the text "You deleted this message". Two forensic tools were able to detect this text as well. Another interesting finding is the extracted message, that says "Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info". Thus the UFED forensic tools were able to extract decrypted messages, even though they were end-to-end encrypted, which means that only a recipient and a sender are allowed to read them. The message that was sent in a Broadcast list appeared in a separate group conversation and at the same time in two personal conversations with its recipients.

In the author's opinion, the most remarkable finding relative to WhatsApp was the ability to listen to audio clips that were sent and received in the application. The author was able to download the file from the UFED Physical Analyzer in the audio format and after that open and listen to it in the web browser, namely Google Chrome. In a similar way, the author opened stickers after downloading their file from the forensic tool and opening it in the Google Chrome. The photos and videos, on the other hand, were available for viewing directly in the UFED Physical Analyzer.

Regarding deleted conversation, it was found that its detecting by forensic tools depended on the time of performed extractions as was the case with the Messenger. Thus one set of three types of extractions revealed the deleted conversation, whereas another set of extractions that was performed later, did not include the mentioned conversation.

7.3 Findings in Viber

The performed extractions revealed all the messages from the open and secret conversations. Contacts, call logs, received video files, and shared locations were acquired as well. Deleted messages, deleted conversations, and stickers, on the other hand, could not be obtained from the mobile device. One of the functions offered by Viber gives the user the ability to delete a selected message for everyone. In this case, the message is then replaced with the text "You deleted a message", which existed on the examined device. Two forensic tools were able to reveal the text, that appeared as "Maria Konty deleted a message". Sent and received audio clips were saved as an audio file to the computer, but the length of the recording was zero seconds, which made listening to the audio impossible.

Sent images could not be opened in the program, whereas the received pictures were available for viewing. Some GIFs could be opened within the UFED Physical Analyzer, others required copying their link and opening it in the Google Chrome.

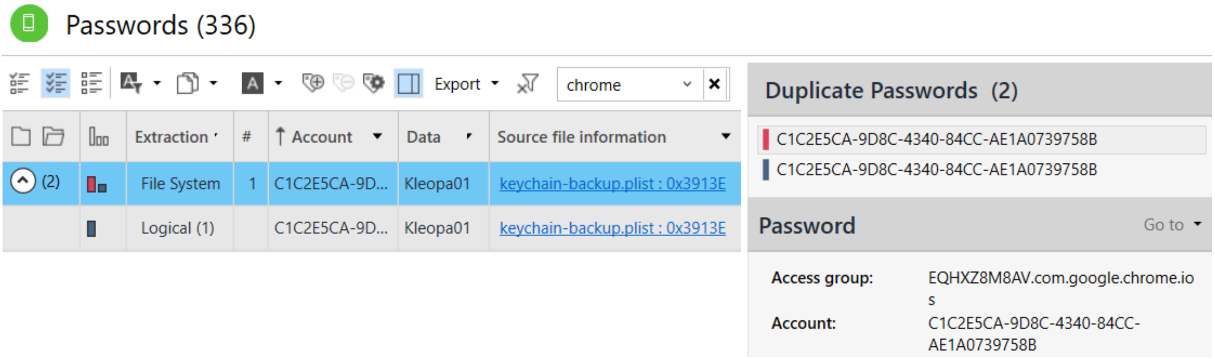
During the analysis phase, it was also discovered that the user was automatically included into two group chats, which he did not give his consent to be a part of. These group chats were located in the tab "Public" in Viber. As a result, the extractions included images of avatars of all the participants in the mentioned chats, which made the examination a little bit harder, as the author needed to sort files every time when investigating the Images tab.

7.4 Findings in iMessage

The examination of the performed extractions showed that all the messages, contacts, call logs, and shared locations in iMessage were obtained from the iPhone. Photos attached to the messages were also available for viewing. The forensic tools managed to detect reactions added by the participants to certain messages, in comparison with Messenger. Messages from the deleted conversation appeared in the extractions, which were performed an hour later after the deletion, as separate chats that included each message independently. Further extractions that were conducted a couple of days later, did not discover the previously deleted conversation. It was also found, that audio recordings were available for download in audio format, which could be opened only after its conversion into another audio format, specifically MP3. After the mentioned actions were performed, the author was able to listen to the audio clip.

7.5 Findings in Google Chrome

The conducted extractions were able to obtain from the mobile device the web history, bookmarks, search history, and saved passwords in Google Chrome. The screenshot below demonstrates the file that was acquired using file system and advanced logical extractions. The mentioned file contains the password for the website www.notino.cz, but it is not obvious for which account or website it was saved. (Figure 7.5.1) The user's account was later discovered in the tab Autofill in the UFED Physical Analyzer, but it was still not specified for which website these credentials were saved. No evidence of visited web pages in the private mode was found. Web pages that were added to the Reading list by the user were not discovered as well. In the tab Cookies in the UFED Physical Analyzer were revealed files that contained a domain of the website www.csfd.cz, which can be viewed as the evidence of deleted web pages from the browser's history.



Passwords (336)

		Extraction	#	Account	Data	Source file information
(2)		File System	1	C1C2E5CA-9D...	Kleopa01	keychain-backup.plist : 0x3913E
		Logical (1)		C1C2E5CA-9D...	Kleopa01	keychain-backup.plist : 0x3913E

Duplicate Passwords (2)

C1C2E5CA-9D8C-4340-84CC-AE1A0739758B
C1C2E5CA-9D8C-4340-84CC-AE1A0739758B

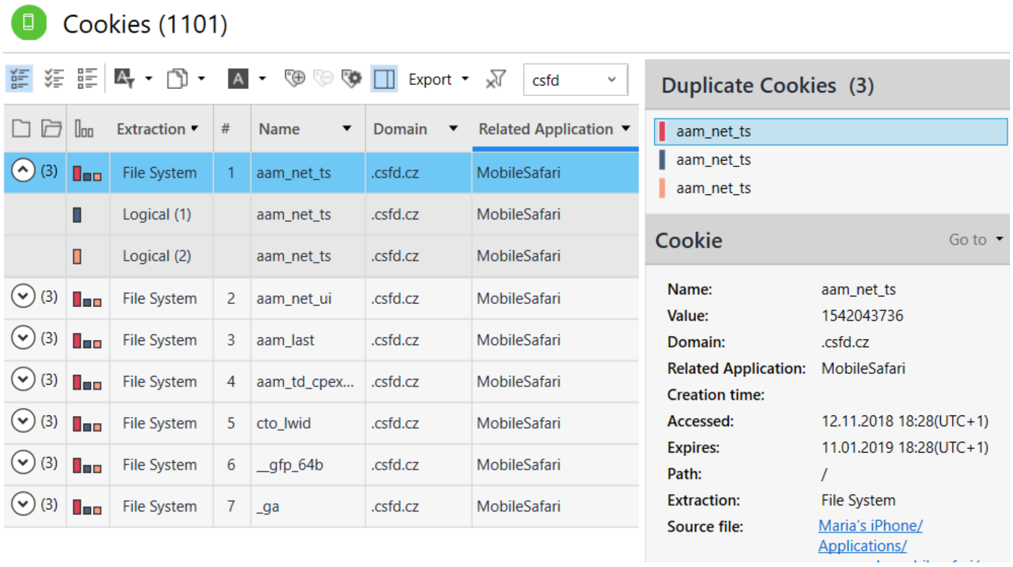
Password

Access group:	EQHXZ8M8AV.com.google.chrome.ios
Account:	C1C2E5CA-9D8C-4340-84CC-AE1A0739758B

Figure 7.5.1 Password for the website www.notino.cz (source: author)

7.6 Findings in Safari

During the examination of acquired data, it was found that the forensic tool was able to extract information about web history, searched items, web bookmarks, and reading list created in Safari. The reading list and web bookmarks can be found in two separate subfolders in the Extraction summary tree area. Login credentials that were saved in Safari for www.notino.cz were discovered by the forensic tool as well. This time, in comparison with Google Chrome, it was possible to read not only the password in the tab Passwords but also the e-mail used for logging on to the website.



Cookies (1101)

	Extraction	#	Name	Domain	Related Application
(3)	File System	1	aam_net_ts	.csfd.cz	MobileSafari
	Logical (1)		aam_net_ts	.csfd.cz	MobileSafari
	Logical (2)		aam_net_ts	.csfd.cz	MobileSafari
(3)	File System	2	aam_net_ui	.csfd.cz	MobileSafari
(3)	File System	3	aam_last	.csfd.cz	MobileSafari
(3)	File System	4	aam_td_cpex...	.csfd.cz	MobileSafari
(3)	File System	5	cto_lwid	.csfd.cz	MobileSafari
(3)	File System	6	__gfp_64b	.csfd.cz	MobileSafari
(3)	File System	7	_ga	.csfd.cz	MobileSafari

Duplicate Cookies (3)

- aam_net_ts
- aam_net_ts
- aam_net_ts

Cookie Go to

Name:	aam_net_ts
Value:	1542043736
Domain:	.csfd.cz
Related Application:	MobileSafari
Creation time:	
Accessed:	12.11.2018 18:28(UTC+1)
Expires:	11.01.2019 18:28(UTC+1)
Path:	/
Extraction:	File System
Source file:	Maria's iPhone/ Applications/

Figure 7.6.1 Deleted website from the web history (source: author)

0x1CBF (Size: 9610 bytes)

From the screenshot above it is obvious that in the tab Cookies were found files that correspond to the web pages from the www.csfd.cz that were previously deleted from the web history by the user. (Figure 7.6.1) The analysis did not reveal any information about web pages that were visited using the private mode.

7.7 Findings in Firefox

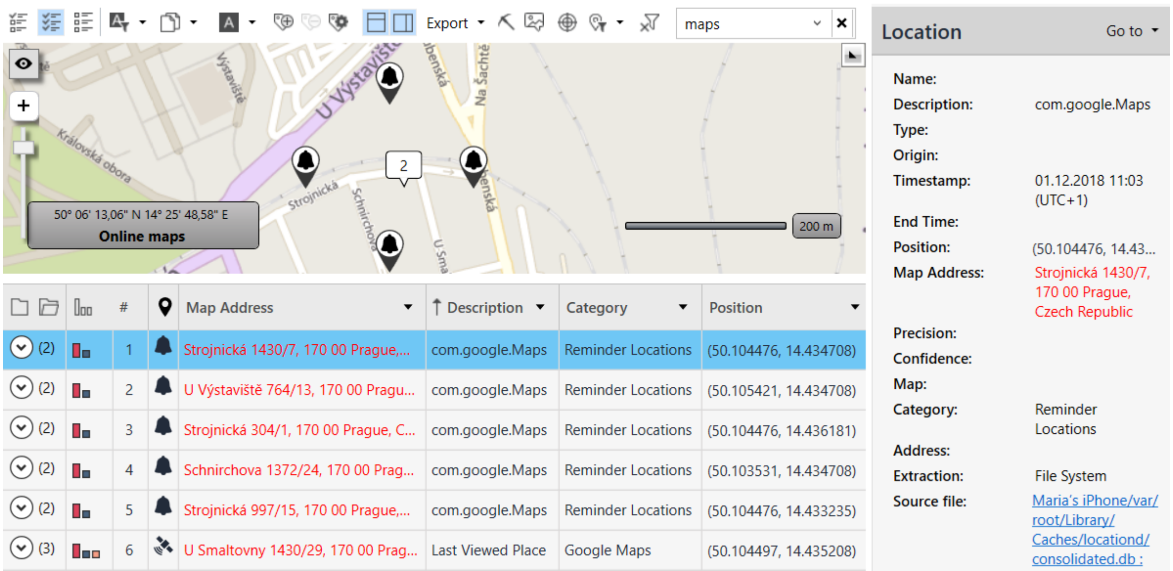
The performed extractions revealed all web pages visited in Firefox, except the ones that were deleted from the web history by the user. The UFED Physical Analyzer was able to extract the list of the searched items, bookmarks, and reading list as well. Compared to Safari, the websites from bookmark and reading lists in Firefox were situated in one subfolder in the project tree. No evidence of saved user credentials or web pages visited in the private mode was found in the three types of extractions.

7.8 Findings in Opera Mini

During the examination of three extractions, it was found that the forensic tool obtained from the iPhone information about web bookmarks, web history, and searched items in Opera Mini. Web pages that were deleted from the web history or visited in a private mode could not be discovered by the UFED Physical Analyzer. The application does not offer the opportunity to add web pages to the Reading list, thus the author did not include this function in his analysis.

7.9 Findings in Google Maps

During the acquisition process, the UFED Physical Analyzer was not able to discover almost any locations that were used by the author when navigating in Google Maps. On the screenshot below is shown the list of locations that were extracted from the application. (Figure 7.9.1) The last location in the list is described as Last Viewed Place and discloses almost the precise author's address, thus the most visited one. Other five locations, which are categorized as Reminder Locations, are all situated in the neighbourhood of the author's address and, unfortunately, their origin is not known to the author. From the mobile device could not be obtained the recordings of the routes that are available for viewing in the timeline in the application. The forensic tool was not able to extract any saved locations, such as home, work, favourite and starred places.



		#		Map Address	Description	Category	Position
(2)		1		Strojnická 1430/7, 170 00 Prague,...	com.google.Maps	Reminder Locations	(50.104476, 14.434708)
(2)		2		U Výstaviště 764/13, 170 00 Pragu...	com.google.Maps	Reminder Locations	(50.105421, 14.434708)
(2)		3		Strojnická 304/1, 170 00 Prague, C...	com.google.Maps	Reminder Locations	(50.104476, 14.436181)
(2)		4		Schnirchova 1372/24, 170 00 Prag...	com.google.Maps	Reminder Locations	(50.103531, 14.434708)
(2)		5		Strojnická 997/15, 170 00 Prague,...	com.google.Maps	Reminder Locations	(50.104476, 14.433235)
(3)		6		U Smaltovny 1430/29, 170 00 Prag...	Last Viewed Place	Google Maps	(50.104497, 14.435208)

Location Go to

Name:	
Description:	com.google.Maps
Type:	
Origin:	
Timestamp:	01.12.2018 11:03 (UTC+1)
End Time:	
Position:	(50.104476, 14.43...
Map Address:	Strojnická 1430/7, 170 00 Prague, Czech Republic
Precision:	
Confidence:	
Map:	
Category:	Reminder Locations
Address:	
Extraction:	File System
Source file:	Maria's iPhone/var/root/Library/Caches/locationd/consolidated.db :

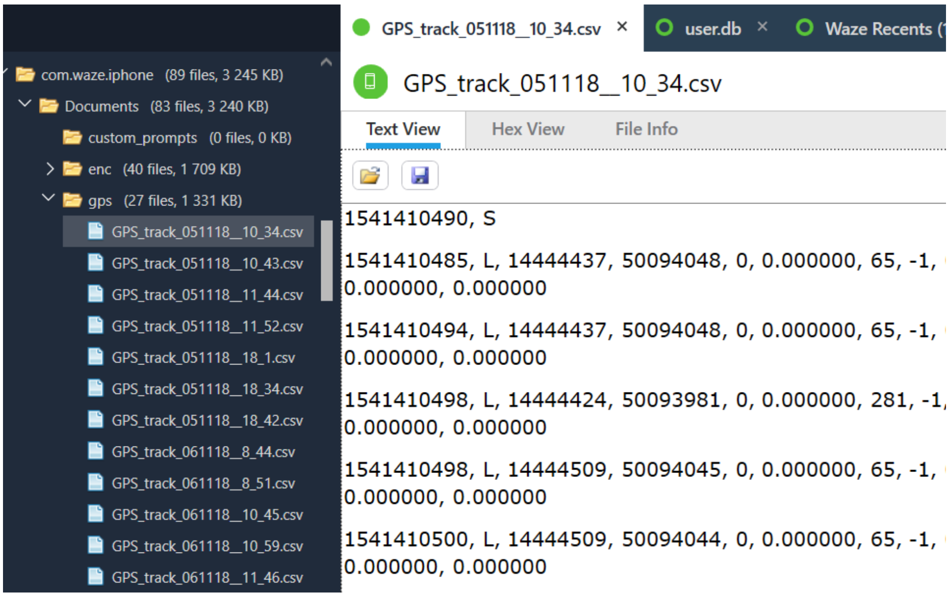
Figure 7.9.1 Extracted locations from Google Maps (source: author)

7.10 Findings in Mapy.cz

When the author was searching for information from the application Mapy.cz, he discovered that the forensic tools were not able to extract any visited or starred locations by the user. Addresses that were visited and saved in the application as a part of the route tracking tool were not extracted as well. The folder "Device Locations" in the project tree, where usually can be found all the locations categorized by their applications, did not even contain the subfolder for the Mapy.cz application.

7.11 Findings in Waze

In comparison to the previous application, Waze allowed forensic tools to extract almost all information that was consequently examined by the author. In the project tree were discovered three subfolders, such as Waze Favorites, Waze History, and Waze Recents, which contained the acquired data from the Waze application. Locations in the subfolder Waze History correspond to the addresses that were searched by the user and were used as destination points during navigation. The folder Waze Recents is represented by the list of recently visited places, which in the application is displayed directly under the search window. These locations only have names of the places, such as Albert Supermarket or Reinerova, and their precise addresses can be found in the application's database that was acquired as a part of the file system extraction. In the same database are stored addresses for favourite locations created by the user in the application. The file system extraction also obtained information of a route tracker, thus every navigation started by the user is contained in a separate file. The screenshot below represents data of one of the routes that took place on 5 November 2018. From the file it becomes possible to trace the user's movements.


com.waze.iphone (89 files, 3 245 KB)
Documents (83 files, 3 240 KB)
custom_prompts (0 files, 0 KB)
enc (40 files, 1 709 KB)
gps (27 files, 1 331 KB)
GPS_track_051118__10_34.csv
GPS_track_051118__10_43.csv
GPS_track_051118__11_44.csv
GPS_track_051118__11_52.csv
GPS_track_051118__18_1.csv
GPS_track_051118__18_34.csv
GPS_track_051118__18_42.csv
GPS_track_061118__8_44.csv
GPS_track_061118__8_51.csv
GPS_track_061118__10_45.csv
GPS_track_061118__10_59.csv
GPS_track_061118__11_46.csv
GPS_track_051118__10_34.csv ×
user.db ×
Waze Recents (
GPS_track_051118__10_34.csv
Text View
Hex View
File Info

```
1541410490, S

1541410485, L, 14444437, 50094048, 0, 0.000000, 65, -1,
0.000000, 0.000000

1541410494, L, 14444437, 50094048, 0, 0.000000, 65, -1,
0.000000, 0.000000

1541410498, L, 14444424, 50093981, 0, 0.000000, 281, -1,
0.000000, 0.000000

1541410498, L, 14444509, 50094045, 0, 0.000000, 65, -1,
0.000000, 0.000000

1541410500, L, 14444509, 50094044, 0, 0.000000, 65, -1,
0.000000, 0.000000
```

Figure 7.11.1 GPS tracker in Waze (source: author)

7.12 Findings in Maps

In the extraction summary tree, the subfolder, which is meant for storing acquired locations from the application Maps, did not contain almost any locations except only one. This one location had the same address as the Last Viewed Place in Google Maps, which is near the user's house. Hence no navigated routes or saved locations were extracted from the mobile device.

8 Experienced difficulties

In this chapter the author intends to describe some difficulties that he came across and resolved during his work on the practical part of this bachelor's thesis.

Initially, the experiment in the practical part was supposed to be conducted on a different mobile phone, specifically Samsung Galaxy A5 2016. During the period of one week the author was creating a dataset on the mentioned mobile device for the acquisition purpose. At the end of this period evidentiary data were acquired by running two types of available extractions in the UFED 4PC, namely logical, and file system. After the collection phase it emerged that none of the extractions acquired a sufficient amount of data for future analysis and examination. This discovery and the fact, that in the UFED 4PC for Android devices are available only two extractions, forced the author to make a decision on changing the examined device to an iPhone. Another fact, that also became one of the reasons for changing the mobile device was the availability of advanced logical extraction in the UFED Physical Analyzer for iOS devices.

Another complication was associated with the old version of the UFED 4PC and the UFED Physical Analyzer, which the author was using during the most part of the experiment. Using the old version resulted in an inability to extract the data from the Messenger. However, the author found a way around in order to obtain the conversations from the application. For this case he used an internal function in the application, which allowed him to save all the data from the app into an archive. For achieving that the author used the function, which was named "Download your information" and could be found in Account settings. This performed action saved the archive to the device, afterwards the archive was acquired with the rest of the data in the collection phase. Later the author gained an access to the latest versions of the forensic tools that were able to provide him with more sophisticated and profound extractions. Nevertheless, it is important to mention that in the case of manual interference in the evidential device it is crucial to properly document all the performed actions and alterations for preserving integrity and reliability of the evidence, which may be later presented in court.

An interesting fact was that for conducting one of the extractions the author used a cable, which was not manufactured by Apple or by Cellebrite (it wasn't a part of a forensic accessory kit). This became the reason that the forensic tool could not identify the connected mobile device and as a result the extraction could not be conducted.

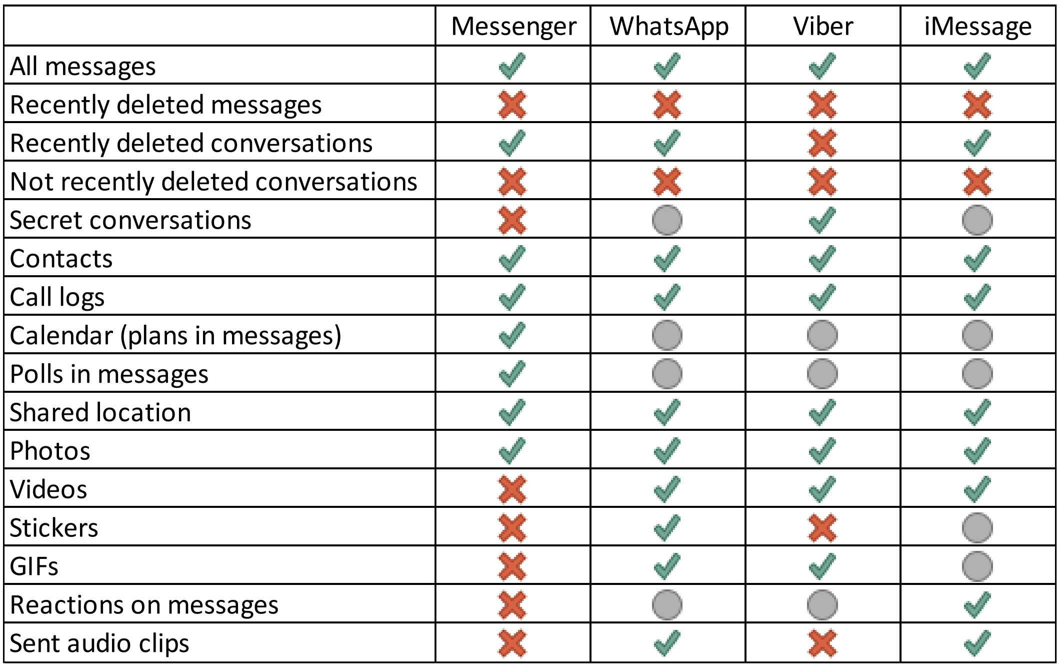
9 Evaluation of results

The results of this study indicate the types and the amount of information that can be obtained from the specific applications, which are installed on the personal mobile device. Some findings might serve as a warning for the users of presented applications because they are informed about the data, which are saved and stored by various applications in the memory of their phones.

Evaluation of results for each category of applications is presented by a table, which summarizes findings for each app revealed in chapter 7. The check mark serves as an indicator of the presence of specified information in the performed extractions. Red cross, on the other side, signifies the absence of the listed information. Grey circle means that the application does not support the specific function, and as a result this type of information could not be examined by the author.

9.1 Applications for Communication

The table below demonstrates analyzed applications for communication and sums up the discoveries that were described in chapter 7. (Figure 9.1.1)



	Messenger	WhatsApp	Viber	iMessage
All messages	✓	✓	✓	✓
Recently deleted messages	✗	✗	✗	✗
Recently deleted conversations	✓	✓	✗	✓
Not recently deleted conversations	✗	✗	✗	✗
Secret conversations	✗	●	✓	●
Contacts	✓	✓	✓	✓
Call logs	✓	✓	✓	✓
Calendar (plans in messages)	✓	●	●	●
Polls in messages	✓	●	●	●
Shared location	✓	✓	✓	✓
Photos	✓	✓	✓	✓
Videos	✗	✓	✓	✓
Stickers	✗	✓	✗	●
GIFs	✗	✓	✓	●
Reactions on messages	✗	●	●	✓
Sent audio clips	✗	✓	✗	✓

Figure 9.1.1 Evaluation of results - Applications for communication (source: author)

From the table it is evident that the UFED Physical Analyzer and the UFED 4PC were able to extract from WhatsApp most of the information in comparison with the other applications for communication. Both forensic tools had access to all messages, contacts, call logs, and shared locations in all presented apps for socializing. The finding, which the author found as the most surprising one, is the ability of the forensic tools to extract audio clips from the messages in the WhatsApp and the iMessage. Another curious finding is the ability to reveal secret conversation in Viber, but not in Messenger. An interesting discovery was that Viber made it possible for viewing only photos, that were received by the user, but not those that were sent from him. A great number of avatars from group chats in Viber made the search and sorting in the Images tab more complicated.

9.2 Applications for Browsing

The table below summarizes the results of the forensic analysis, which were described separately for each application in chapter 7. (Figure 9.2.1) Data from four applications for browsing were obtained from three types of extractions. The largest amount of information disclosed by the UFED Physical Analyzer and the UFED 4PC was revealed from the Safari web browser. The second application that uncovered most of its data was Google Chrome. Opera Mini turned out to be the application with the least available information. Interestingly, only Google Chrome and Safari browsers contained domains of the deleted web pages in their cookie files. In the future this fact can be used for comparing web history and cookies using the date they were accessed, which can later serve as evidence of deleting some visited web pages. Surprisingly, the information about visited web pages in the private mode was not discovered in any of the web browsers, which implies that the user can be sure that his web history in this mode is not saved on the phone and, as a result, is not available for extraction. The users of Google Chrome and Safari browsers might want to be more careful when saving their login credentials for the future autofill, as they can be extracted by the selected software forensic tools.

	Chrome	Firefox	Opera Mini	Safari
Web History	✓	✓	✓	✓
Web Bookmarks	✓	✓	✓	✓
Webpage deleted from history	✓	✗	✗	✓
Searched items	✓	✓	✓	✓
Saved password	✓	✗	●	✓
Private mode	✗	✗	✗	✗
Reading list	✗	✓	●	✓

Figure 9.2.1 Evaluation of results - Applications for browsing (source: author)

9.3 Applications for Maps & Navigation

Results of the examination of applications for navigation were not very promising. From the table below is obvious that only application Waze was properly saving locations and kept all its data in the form that could be recognized by the UFED 4PC and the UFED Physical Analyzer. (Figure 9.3.1) Google Maps and Apple Maps were able to capture the last viewed place. Therefore, three applications out of four might require more profound analysis that can consist of further decoding and examination of the applications' databases for unrevealing the visited locations and the tracker used for recording the routes.

	Google Maps	Mapy.cz	Waze	Apple Maps
All locations	only one	✗	✓	only one
Saved locations	✗	✗	✓	✗
GPS track	✗	✗	✓	✗

Figure 9.3.1 Evaluation of results - Applications for maps & navigation (source: author)

Conclusion

This bachelor’s thesis has focused on two phases of the forensic process, specifically data acquisition and data analysis. Data acquisition has been described in the theoretical part of the thesis and includes four types of extractions. In practical part were performed three types of available extractions from an iPhone 6. The performed study provides considerable insight into information that is stored by various types of applications on our mobile phones. The forensic tools from the Cellebrite UFED family have shown the excellent performance of extracting data and their consequential analysis. The author has obtained satisfactory results demonstrating the opportunities for obtaining personal details from applications, which people use in their everyday life. One of the conclusions the author has come to is the fact that Cellebrite UFED provides powerful tools for both phases of the forensic process. They were able to extract a wide range of information from the applications for communication and browsing. However, almost no data were extracted from the applications for maps and navigation.

Examination of applications for socializing showed that the least information was obtained from the Messenger. WhatsApp, on the other hand, was able to provide the author with an extraction that was rather rich in content. An interesting finding was the ability to acquire voice recordings, which were sent in WhatsApp and iMessage. The application for browsing, which has a standard set of functions and was discovered as the safest from the four examined applications, is Firefox. At the same time, most of the information was retrieved from the Safari web browser. From the four applications for maps and navigation, only Waze offered the widest range of a set of data.

As a result, applications for communication and browsing gave the opportunity to extract a substantial amount of valuable personal data that can be used by forensic investigators for solving criminal cases. The findings from this thesis offer the advantage not only to mobile forensics branch but also to ordinary people, who have now a better understanding and knowledge of types and amount of information that can be extracted from different mobile applications.

Bibliography

Apple: iTunes [online]. 2018 [accessed 2018-11-10]. Available at: https://itunes.apple.com/us/genre/ios/id36?mt=8

AYERS, Rick, Sam BROTHERS, and Wayne JANSEN. Guidelines on Mobile Device Forensics. National Institute of Standards and Technology [online]. 2014 [accessed 2018-10-09]. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf

CARRIER, Brian. Defining Digital Forensic Examination and Analysis Tools. International Journal of Digital Evidence [online]. 2002 [accessed 2018-10-09]. Available at: http://citeseerx.ist.psu.edu/viewdoc/citations?doi=10.1.1.14.8953

Cellebrite 4PC Manual: 4PC Help. 2018.

Cellebrite Advanced Services. Cellebrite [online]. 2018 [accessed 2018-10-15]. Available at: https://www.cellebrite.com/en/cas-sales-inquiry/

Cellebrite PA Manual: PA UFED Physical Analyzer Help. 2018.

Cellebrite UFED Series. SC Media UK [online]. 2015 [accessed 2018-10-15]. Available at: https://www.scmagazine.com/review/cellebrite-ufed-series/

Forensic Express. MOBILedit [online]. 2018 [accessed 2018-11-30]. Available at: https://www.mobiledit.com/forensic-express

MAHALIK, Heather, Rohit TAMMA, and Satish BOMMISETTY. Practical Mobile Forensics. Second Edition. Birmingham: Packt Publishing, 2016. ISBN 978-1-78646-420-0.

MAJEED, Asma, Haleemah ZIA, Rabeea IMRAN, and Shahzad SALEEM. Forensic analysis of three social media apps in windows 10 [online]. 2015 [accessed 2018-10-15]. Available at: https://www.researchgate.net/publication/301198324_Forensic_analysis_of_three_social_media_apps_in_windows_10

Oxygen forensics [online]. 2018 [accessed 2018-11-30]. Available at: https://www.oxygen-forensic.com/en/

Product Updates. Cellebrite [online]. 2018 [accessed 2018-10-17]. Available at: https://www.cellebrite.com/en/support/product-releases/

Products Certified Resseler. Digital shield [online]. 2018 [accessed 2018-10-17]. Available at: https://digitalshield.net/products

SACHOWSKI, Jason. Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise. Boca Raton: CRC Press, 2018. ISBN 9781138720930.

UFED4PC User Manual. RCFL [online]. 2014 [accessed 2018-10-23]. Available at: https://www.rcfl.gov/rocky-mountain/copy_of_documents-forms/customer-satisfaction-survey/view

XRY - Extract. MSAB [online]. 2018 [accessed 2018-11-30]. Available at: https://www.msab.com/products/xry/