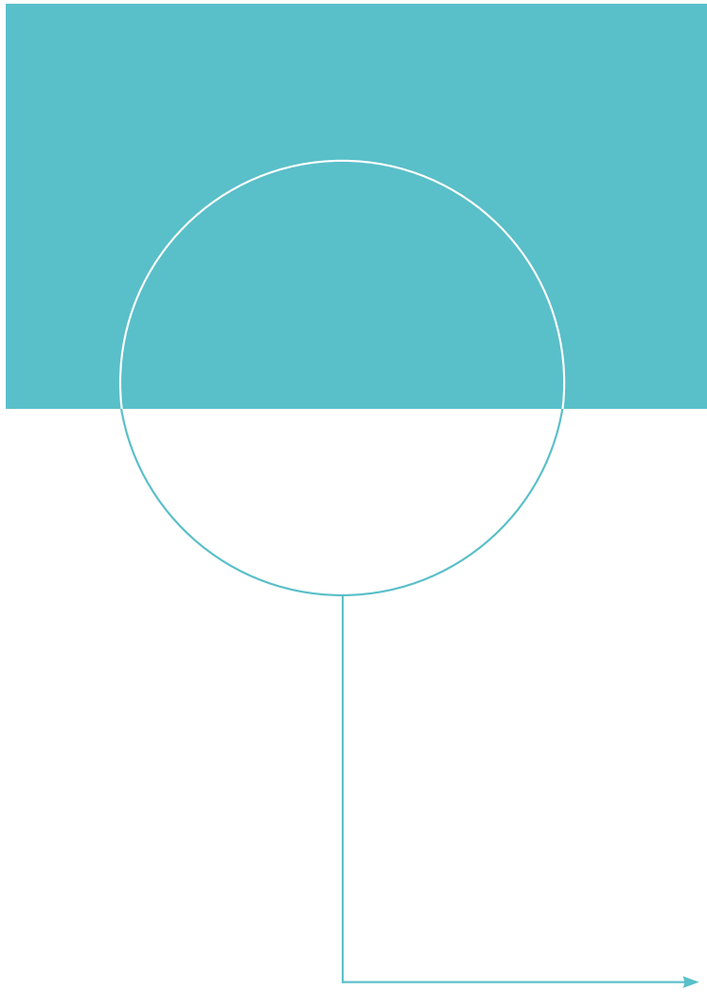

Master's thesis

2019

Peter Varenkamp

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology and Electrical
Engineering
Department of Information Security and Communication
Technology

Peter Varenkamp

iPhone Acquisition Using Jailbreaking Techniques

May 2019

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

NTNU

Norwegian University of
Science and Technology

iPhone Acquisition Using Jailbreaking Techniques

MISEB

Submission date: May 2019

Supervisor: Prof. Stefan Axelsson, IIK

Co-supervisor: Police Superintendent Kurt H. Hansen (MSc), PHS

Norwegian University of Science and Technology
Department of Information Security and Communication
Technology

Acknowledgement

I would like to thank my supervisors, Police Superintendent Kurt H. Hansen and Prof. Stefan Axelsson for their patience and engagement.

Especial thanks to Police Superintendent Kurt H. Hansen, who has supported me since the specialization course.

P.V.

Figure 1: Apple iPhone [1]

Figure 2: Absinthe Jailbreak [2]

[1] https://www.teltarif.de/img/jpg/smartphone/apple/iphone-x-11.jpg
[2] https://cdn5-capriofiles.netdna-ssl.com/wp-content/uploads/2012/05/greenpois0n-absinthe-.jpg

Abstract

Digital devices are a part of most peoples lives today. Using digital devices leaves traces. These traces can be urgent to solve a criminal case. Knowing this, forensic work has the goal to get as much data from a device as possible. Only physical image from a data storage is a 100% copy and can make sure that all data has been secured.

Forensic work with digital evidence was in the first time done with opening a personal computer, removing the hard disk and secure with write protection. It was not so difficult to connect directly to the interface of the hard drive and performing a physical image.

That changed with the first smart phones that were not produced with data storage that could be removed without a high technical effort. The smart phones used data storage that had not their own interface and were soldered with the logic board.

In computer forensic investigations the fast technological changes make it more difficult to get all or most digital data in the same way we did before. One reason is that manufacturers produce more secured devices as the customer demands it. Another reason may be to make the system more stable. On the other hand, we will always search how we can get all digital information from the device as possible, especial erased data that may be urgent for the case.

Apples iPhone is one of the most popular smart phones and has about 14 percent market share in first quarter of 2018. Only Samsung sells more smartphones with 20 percent market share at the same time. The most sold smart phones work with different distributions of Android and had actually a market share up to 85 percent (BusinessReport, 2018).

Apple has continued improving the security mechanism of its products. This fact makes it more difficult or impossible to get access to the iPhones and extract all information that were stored on it. Commercial Forensic Software work sometimes with own programs that use security breaches to get deeper access to a device. Jailbreaking is not offered from commercial vendors. But they describe their programs are able to extract more data from a jailbroken device.

The aim of my master thesis is to answer the question if iPhones acquisition using jailbreak techniques can be a forensic way? To answer the research question, five depending sub question were answered. At the time I began working at the master thesis in middle 2018, I have first to answer if there is a way for jailbreaking with a current iOS (apples operating system), that was 10 and 11? Otherwise, it wouldn't have any sense to continue with my research. Fortunately, the answer to this question was yes. During writing this master thesis, I have to change and revise some parts multiple times to be up to date. Reasons have been that new jailbreaks, new iOS-versions and new iPhones released in this time.

List of Appended Papers

In the specialization course I wrote about different ways to create a physical backup from a Mac Computer. Some parts of this paper are used in this master thesis. These parts were customized to this thesis or updated if possible.

Varenkamp, P. Forensic acquisition of Apple Mac computers, specialization course (IMT4215 12.2017 report).

Table of Contents

Acknowledgement **i**

Abstract **iii**

Table of Contents **vi**

List of Tables **vii**

List of Figures **viii**

Abbreviations **ix**

Glossary **1**

1 Introduction **1**
1.1 Target Group 4
1.2 The Significance of Open Source Knowledge in Forensic 4
1.3 Overall Problem 5
1.4 Limitations 5
1.5 Research Questions 7
1.6 Master Thesis Outline 8

2 Literature Research and Background **9**
2.1 Jailbreak 9
2.1.1 The ”right” Jailbreak 11
2.1.2 Available Jailbreaks for iOS 11 and 12 12
2.1.3 Differences between Jailbreaks 12
2.1.4 Jailbraking risks 13
2.1.5 Apple ID 14
2.1.6 Passcode 14
2.2 Forensic definition and explanation of forensic soundness 15
2.3 Open Source in forensic 16
2.4 Physical and logical acquisition 17
2.4.1 Physical 17
2.4.2 Logical 17

2.4.3 Differences for forensic manner . . . 17
2.4.4 Challenges with decryption . . . 18
2.5 Apples new File-system APFS . . . 18

3 Methodology **20**
3.1 Research Methods . . . 20
3.2 Research Approach . . . 20
3.3 Research Design . . . 21
3.4 Experiment . . . 21
3.5 Other Methods . . . 22

4 Experiment **23**
4.1 Configuration . . . 24
4.1.1 Preparation and recommended settings . . . 26
4.1.2 Jailbreaking . . . 27
4.1.3 FilzaJailed . . . 30
4.2 Different methods of acquisition an iPhone . . . 32
4.2.1 Command-Line . . . 32
4.2.2 iTunes . . . 34
4.2.3 Phone Paw 5.8.0 . . . 35
4.2.4 Forensic programs . . . 36
4.3 Searching for changes through the jailbreak . . . 40
4.4 Results . . . 41

5 Discussion **47**

6 Conclusion and Further Work **53**
6.1 Conclusion . . . 53
6.1.1 Research Questions and Subquestions . . . 53
6.2 Further Work . . . 57

Bibliography **58**

List of Tables

1.1 All types of iPhones, 2007-2018 3

4.1 Hardware Configuration 24
4.2 iPhone 4 24
4.3 iPhone 4s 25
4.4 iPhone 5 25
4.5 iPhone 5s 25
4.6 iPhone 7 25
4.7 iPhone X 26
4.8 iPhone X 256GB 26

List of Figures

1 Apple iPhone ii
2 Absinthe Jailbreak ii

1.1 Increasing number of avaliable iPhone Apps from the year 2008 until 2018 . . 2

4.1 Overview from the root directory with FilzaJailed 31
4.2 UFED with 3. extraction method, only available for jailbroken iPhones 37
4.3 Startmenu iOS Forensic Toolkit 39
4.4 Content of the tar archive created with iOS Forensic Toolkit 40
4.5 Overview from the root directory with iDevice Manager, after AFC2 was installed to the jailbroken iPhones 42
4.6 Overview from the system partition at the root directory to the acquired image from an iPhone 5 (iOS 9.3.3) with X-Ways Forensics 44
4.7 Overview number of extracted files with XRY after jailbreaking the iPhone X . 45
4.8 Overview number of extracted files with XRY before jailbreaking the iPhone X 45

Abbreviations

AFC Apple File Conduit

AFC2 Apple File Conduit

APFS Apple File System

CPU Central Processing Unit

DFU-Mode Device Firmware Update Mode

GB Giga Byte

MB Mega Byte

MHz Mega Hertz

IPSW IPSW is a file format for iOS firmware

GPS Global Positioning System

GUI Graphical User Interfacem

Hash Digital fingerprint from a file

HFS Hierarchical file system

HFS+ Hierarchical file system

IBM International Business Machines Corporation

IPA iOS App Store Package

iOS Internetwork Operating System

IT Information Technology

IP Internet Protocol

ID Identification Number

MMS Multimedia Messaging Service

MD5 Message-Digest Algorithm 5

MSAB Micro Systemation Aktiebolag

Mac Mac is the abbreviation of Macintosh

FTK Forensic Toolkit

OS Operating System

PC Personal Computer

PDA Personal Digital Assistant

RAM Random-access memory

SATA Serial Advanced Technology Attachment

SMS Short Message Service

SSD Solid State Drive (electronic data storage)

SSH Secure Shell

URL Uniform Resource Locator

USB Universal Serial Bus

UDID Unique Device ID

UFED Universal Forensic Extraction Device

WLAN Wireless Local Area Network

XRY XRY is a forenc program from the company MSAB

Wi-Fi Wireless Fidelity (Company consortium, that certifies equipment with radio interfaces)

Glossary

AFC/AFC2 is a service that gives access to an iOS filesystem over USB

Command-Line User-Interface for commands (Windows)

Data Compression is the process of modifying, encoding or converting the bits structure of data in such a way that it gets smaller size in bytes.

Hacker are called persons that try to get access to a closed system. For this they use known or self discovered vulnerabilities or programming errors to bypass the existing security measures.

Image-types are different methods a container with data is created. It depends on the image-type which program can work with it.

OpenSSH The SSH protocol is a method for secure remote login from one computer to another.

Pairing is a connection between two devices

Terminal User-Interface for commands (Mac and Linux)

Chapter 1

Introduction

1924 Bell tested already mobile radio telephony. The first mobile call has been offered 1946 from the Bell Telephone Company. Calls were done with vehicle mounted Terminals (Forst, G., 2017).

In 1973 Motorola made the first phone call from a mobile phone. The device weight about 1,1 kg, Ten years later the first mobile phones were sold in the U.S. at almost 4.000 $ (Brown, C., 2018). In the next few years the mobile phones essentially got smaller and got a better battery performance. In the beginning Mobile phones were nothing else than a telephone we were able to talk with others. Next step was in 1992, mobile phones were able sending text messages with at most 160 signs from a mobile phone, called short message (Defree, S., 2018).

1992 IBM debuted a prototype of a hand held device that was a combination between a phone and a PDA with a touchscreen. The device was sold in 1993 as Simon Personal Computer. Nokia released with the Nokia 9000 Communicator in 1996 a phone that had a lot of functions like Internet, SMS, MMS, fax, e-mail, Blue-tooth and more.
Due to the product features both devices would now fall under the term smartphone (Steimels, D., 2012).

In 2007 the iPhone with the product name 2G was introduced by Steve Jobs to the public. It was a very small computer that could be carried in a jacket pocket. It had a touch display, a digital camera and also could be used as phone. It had an own operating system, called iOS and was delivered with a 4 and 8 GB storage (Dernbach, C., 2012).
From this point until today the iPhone growed up to a pocket computer that also can be used as phone. Today mobile phones can contain all kind of data like mail, chats, pictures, videos, GPS-data, Contacts, passwords, etc..

Apple is a closed system, this means that users can only do things with their iPhone that are allowed by Apple. e.g. installing a program, called app(lication), is generally only available by using the app store. The app store was introduced in 2008 by Apple. Beginning with some apps, there are today more than 800.000 apps available, as you can see the Figure 1.1 (Statista, 2018c).

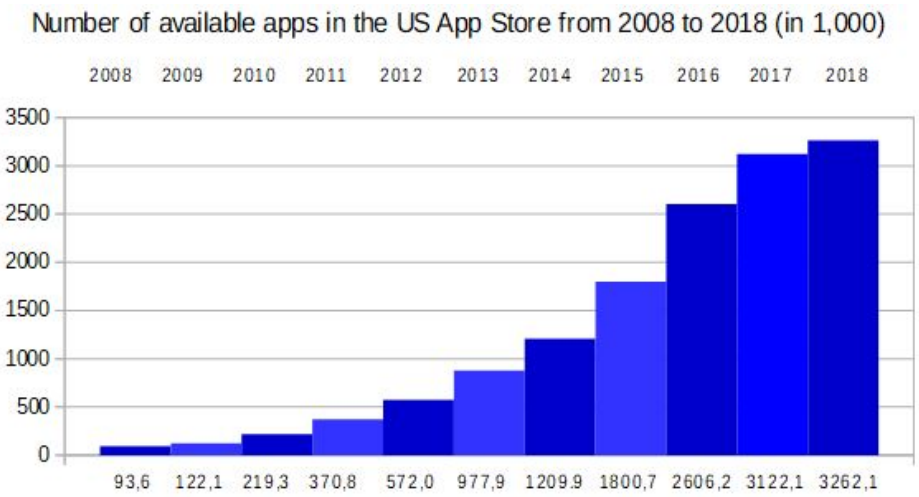

Figure 1.1: Increasing number of avaliable iPhone Apps from the year 2008 until 2018

Apple decides which Apps are available for their iPhones. Apples Operating System is called iOS. This operating system was programed specially for every iPhone type. The user is realy only user and can not root the system. This is quite different to operating systems like Windows from Microsoft, Linux distributions or Android that is used for other Smart phones. These operating systems were programed to be used universal with a variety of different devices (Hoffmann, C. , 2017).

From the beginning iPhones got only one hardware port. It is a special port only for the iPhones to load the batteries and connect to the data-port from a iPhone via USB to another device e.g. PC or Mac. First it was a 30-pin to USB connector. Introducing iPhone 5, the connector was changed to 8-pin, named lightning connector.
A simple way to exchange or store data to an external storage does not exit. It is not possible to use an additional memory card in a iPhone, because there is no slot for it like a lot of phones and the most smart phones have.
Apple has hardware encryption for his iPhones since iPhone 3GS with iOS 4. The iPhone Operating System was changed more times every year since appearance. Since iPhone 4s it was not possible any more to make a physical acquisition from this device in the usual way. Only with jailbroken devices (Chapter 2.1) it was possible in some cases to create a physical backup under certain circumstances (Sanford, G., 2019).

In the beginning Apple was only used from a small group of people. It was not from higher interest how to acquire an Apple device in a forensic way for law enforcement..
In the last 20 years Apple devices hold more and more entry into private households and companies. Reasons may be that it has become fashionable to own such a device or the fact that it is easy to use. Most sold product from Apple is the iPhone, it was sold more than 100 Million parts every year in the last 3 years (Statista, 2018b).

To have an overview I have listed all types of iPhones that have released until today, as shown in Table 1.1, staring with iPhone 2G in 2007. iOS-version 12.1.4 and higher means that until today the coming up version for this iPhone are available until Apple stops the support.

Type	Released	iOS (GSM)
2G	2007	1.0 - 3.1.3
3G	2008	2.0 - 4.2.1
3GS	2009	3.0 - 6.1.6
4	2010	4.0 - 7.1.2
4s	2011	5.0 - 9.3.4
5	2012	6.0 - 10.3.3
5s	2013	7.0.1 - 12.1.4 and higher
5c	2013	7.0.1 - 10.3.3
6	2014	8.0 - 12.1.4 and higher
6+	2014	8.0 - 12.1.4 and higher
6s	2015	9.0 - 12.1.4 and higher
6s+	2015	9.0 - 12.1.4 and higher
SE	2016	9.3 - 12.1.4 and higher
7	2016	10.0.2 - 12.1.4 and higher
8	2017	11.0 - 12.1.4 and higher
8+	2017	11.0 - 12.1.4 and higher
X	2017	11.1 - 12.1.4 and higher
Xs	2018	12.0 - 12.1.4 and higher
Xs Max	2018	12.0 - 12.1.4 and higher
Xr	2018	12.0 - 12.1.4 and higher

Table 1.1: All types of iPhones, 2007-2018

From the first iPhone (2G) that had a one core CPU ARM1176 with 412 MHz, 128 MB RAM and a storage with 4, 8 and 16 GB until today the newest iPhone (Xs) got a quad core CPU A12 Bionic with 2490 MHz, 4 GB RAM and up to 512 GB storage. That shows how much stronger the current model is than the first iPhone. This opend the way to make the devices more secure with hardware encryption. That was built in first to the iPhone 3Gs that could be used with iOS 4 (iPhone-Tricks.de, 2018).

The technology in smart phones is progressing faster and faster. A smart phone today combines features of a mobile phone, navigation system, high resolution camera and computer with touch displays having its own power supply that can be taken anywhere. Again and again, new devices have improved hardware but also new, innovative technologies on board. In the meantime, these smart devices are increasingly infecting the office computer. This allows them to map all or a large part of the applications required in the office. In addition, they have the ability to connect the possibilities telecommunication options with those of office computer. This was achieved with a simple operating system and a user-friendly Graphical User Interfacem (GUI).

Apple is going on to secure their iPhones. That makes it increasingly difficult for a forensic investigator to get access to most or all on a iPhone stored data. Especially with serious crimes it is necessary to save all existing data. This master thesis will search for answers if that the use of jailbreak techniques will be a method to achieve this goal.

1.1 Target Group

This master thesis will have a literature research part in Chapter 2 and a practical part in Chapter 4 where some iPhones with current and older iOS (Apples operating system) will be jailbroken. The next step will be performing different backups before and after jailbreaking the IPhones. This will be tested for validation and forensic soundness.

The results may be helpful for forensic examiners and investigators to get an idea about jailbreaking to a current iPhones may bring more information that can helping to solving a case. It also gives interesting approaches for experts in computer science.

In daily work there is generally not the needed hardware available or not enough time to make experiments which could answer the reserach question. Jailbreaking software was created from programmers and not from official companies. This means that there are not many official ways to get information about jailbreaking. At least this is my experience.

1.2 The Significance of Open Source Knowledge in Forensic

Jailbreaking smart phones was until today not offered from any official company. That may have legal reasons. Programmers who work mostly anonymous have searched for a security breach and some of them have found a way to jailbreak Apple devices. Open source knowledge is a concept with freely available software tools including their source code. Open source knowledge give us tools with all information belonging to this programs. Open source knowledge means to get this information that was found out from or programmed by other, to use, modify and share is allowed. The idea is solving a problem in a collective way. Known Open Source programs are Linux operating systems, Open Office, Firefox and much more..
Forensic work is constantly reaching its limits because it faces new phenomena again and again. Often it is the only way to use existing open source tools or to modify them for own purposes. But even if there is a program for the purpose, the result can only be tested double checked with an alternative programtool. This is also known in the forensic as Dual Tool Verification.

This practical work to this master thesis would not possible without Open Source Tools. Starting with a jailbreak that is open source, going on with Linux command line, OpenSSH, WinSCP, AFC/AFC2, are Open Source too.
Also when commercial software like forensic acquistion tools UFED and XRY (Chapter 4.2.4) were used Open Source Tools are indispensable when the goal is to acquire data from the system partition from an iPhone.

1.3 Overall Problem

The overall problem will be named and explained here in details.

Documentation:

The documentation about available jailbreaks is limited to installation guides and some experiences written by some user. Information or documentation about forensic work with jailbreaks are only in small dimensions available and mostly older. I didnt found any documentation about forensic work with jailbreaks on current devices like iPhone 7 and newer with iOS 11 and newer. On the Web-pages from Elcomsoft there were a lot information listed about jailbroken iPhones in connection to there iOS Forensic Toolkit, tested with jailbreaks up to iOS 12.1.2.

Support:

There is not really support for jailbreaking. On the most home pages where the needed jailbreak were found was limited to instructions how to perform the jailbreak and some hints if errors occurred. Many pages can be found in the internet to problems that occurred when jailbreaking an IPhone, especially in some blogs. Once jailbroken there is support from different forensic providers to their products to acquire data from a jailbroken iPhone.

Verification:

To be sure that a program has worked without an error can be only tested with a second tool, named ”Dual Tool Verification” (Årnes,A., 2017). Current iPhones can not be acquired with Open Source tools or other non-commercial tools before they have been jailbroken. To compare the results from the acquisitions before and after jailbreaking two commercial programs were needed. Another problem was that once jailbroken the iPhone it could not be reset to the same condition before, to test another jailbreak with the same device.

Ways for acquisition and viewing data from jailbroken iPhones:

Acquistion from jailbroken iPhones were done using the command line from a Mac, Linux and Windows Computer. To acquire non-jailbroken iPhones commercial programmes have been used, Chapter 4.2.
To view the content from the acquired data also some open source tools are available.

1.4 Limitations

The work for this master thesis was limited in some aspects as explained in the following:

Personal Limitations:

This master thesis is a work from one student. The time for the research is limited to 900 hours. The research to get knowledge about current jailbreaks and to perform backups needed more time than expected. Even until the first iPhone was jailbroken needed some more choices than expected.

XRY and UFED are costwise commercial tools. Fortunately, there was an opportunity to work a limited time with this two forensic tools . For this additional time had to be taken for driving to places where it was available.

Using the command line for acquisition was also far more time-consuming than expected. More than 1 hour was needed to transfer 1 GB data storage during the acquisition with command line.

Technical Limitations:

Apples iPhones are not only restricted in use. The restriction concerns also to the ways the iOS to an iPhone can be installed. The installed iOS-versions can only be changed with an update to a higher version, that has been released by Apple. As a rule that are one or two newest iOS-Versions. It took some effort to get iPhones that had an iOS that was needed to work with the jailbreaks. Apple notifies users of iOS updates and prompts them to update the mobile phone. The update can be postponed or confirmed later. Once confirmed, the process can not be stopped any more. This accidentally happened during the experimental work with one iPhone 7 that was updated from iOS 11.4.1 to 12.1.3. There was no way to get back or to use the device for jailbreaking during the experimental work.
Thanks to a big platform it was possible to get some of the needed iPhones with iOS versions that could be jailbroken. This part was more difficult as expected, needed more time and money as planed.
XRY, UFED and iOS Forensic Toolkit are expensive commercial tools. Fortunately there was the opportunity to work a limited time with this forensic programs.

Theoretical Limitations:

Jailbreaking is something special. A new jailbreak mostly uses a new found security break. There is no documentation about jailbreak and how it works. There are different versions of jailbreaks which will not give completely root access. Some were not useful for forensic work, because they do not give the needed access to the devices or were not able to install such programs like OpenSSH or AFC that are needed to get external access to the mobile phones. After the jailbreak was performed XRY and UFED did not recognized anyone of the jailbroken iPhones as jailbroken. It was unexpected that this would happen and took also some time to find out the reason and fix it.

1.5 Research Questions

This master thesis is based on a single research question.

Research Question:

Can jailbreaking be used as a technique to create reliable, verifiable and forensically sound images from an iPhone to provide evidence robust enough to be valid in a court proceeding?

To answer the research question is depending on the answers to the following five sub-questions. The results from literature research (Chapter 2) and experimental work (Chapter 4) will leave to answer the sub-questions and finally to the research question in the discussion (Chapter 5).

Question 1:

Can iPhones be jailbroken in a way that will open methods for forensic acquisition?

Question 2:

Can iPhones be jailbroken in a way that will open methods for forensic acquisitionHow will jailbreak influence the result from the acquisition in perspective to the content of saved data?

Question 3:

Will more extracted files have information that can be evidence in a case?

Question 4:

Are the results valid and reliable for court proceeding?

Question 5:

Can jailbreaking an iPhone for acquisition be a forensically sound method?

1.6 Master Thesis Outline

- **Chapter 1:** The introduction provides general information to this master thesis and my intention using jailbreak techniques for acquisition.

- **Chapter 2:** Some background information that will be helpful to understand the master thesis. A collection of knowledge from literature research that was made to write this master thesis.

- **Chapter 3:** The methodology and research methods will be explained. The chosen research approach and design will be explained

- **Chapter 4:** Includes in part one preparation and practical work to jailbreak some different iPhones using different techniques. In the second part different ways will be used to perform a backup from the jailbroken iPhones. Results will be presented in a textual way.

- **Chapter 5:** The results are discussed in this chapter.

- **Chapter 6:** The results are compared against the research questions in a conclusion.

Chapter 2

Literature Research and Background

Preparing this master thesis some further literature research, utilizing the resources from the institutional repositories of universities, such as the search engine Oria of the NTNU University Library and the world wide web was done.

During the literature search, there was only some paper found that dealt with jailbreaking as a forensic technique for acquisition. Jailbreaks and acquisitions were done with older devices like iPhone 4 to perform a physical backup (Hoog, A. and Strzempka, K., 2013).

An article was found where the command line was used to acquire an iPhone 6, that was already jailbroken (mac4n6.com, 2016).

There was no information found that dealt to jailbreak an iPhone as a forensic method with newer devices like iPhone 7 and higher with iOS 10 a higher with iOS 10 and up. Only on webpages from providers (e.g. Elcomsoft, Cellebrite, XRY, etc.) of forensic tools for iPhone acquisition descriptions were found that from jailbroken iPhones until iPhone X up to iOS 12 more data could be extracted.
There was also no information found where it was investigated if jailbreaking a current iPhone has altered evidence files.

Below I listed some relevant findings on this topic.

2.1 Jailbreak

Jailbreak means to break out from a prison. This term is also used in combination with electronic devices that have restriction in configurations / administration. Such restrictions we can find mostly on smartphones and gaming consoles. Jailbreak uses a way to repeal a part or all restrictions. The closed system from Apples iPhones is the prison that a user wants to break out with a jailbreak to be free as a root can be (Aschermann, T. , 2017).

The first jailbreak to an iPhone was published 2007 for the iPhone 2G from the iPhone Dev Team with the Hacker using the synonym Joy Freeman (saurik). From this point a lot of jailbreaks from this Team and other Hackers were published. To install an additional a program

(app) after jailbreaking another software tool is needed. The most used program to do this with jailbroken iPhones is Cydia that comes until today from Hacker (saurik) Jay Freeman (Rentrop, C., 2018).

The differences between available jailbreaks will be explained in the next paragraphs.
These differences are not critical to the question of getting root access or not. Each jailbreak has the goal to get root access to the iPhone. To get access to the data, especially performing a physical backup, a way is needed to export or save an image or a copy from the accessed data. One way is to get a connection e.g. with OpenSSH to the iPhone that makes it possible to log in as root to the iPhone and uses its own command line. OpenSSH is a program that uses the SSH protocol for secure remote login from one computer to another. Another way is to install a program to the iPhone that lets connect the iPhone via USB giving access to all stored data in the same behavior as root has.
That means the used jailbreak must be able to perform such a connection or to install a program that is able to connect as root to the iPhone. Programs to doing this are e.g. OpenSSH, AFC, AFC2. AFC/AFC2 (Apple File Conduit) is a service that gives access to an iOS filesystem over USB-Port. These programs can only be installed using a jailbreak that includes such a program or using Cydia to install it.

Apples iPhones have a closed system that allows user only to do what Apples restriction allows him. The user has not and can‘t get root privileges to the system. He is not allowed to modify the settings of the operating system. Apple and other manufacturers have made user restricted operating systems. It is justified to make their smartphones more secure and stable.
The Idea of a jailbreak was to find a way to break out from the jail of user restrictions. This leads to the option to install from Apple not authorized software to change user rights or the system settings. It opened also ways to install cracked programs without paying money for them.

Since the first iOS until today all iOS version number from 1 to 12 had at least one version that could be jailbroken. For iOS 12.1.3 and higher there is no jailbreak available at the time of writing, 1. May 2019.

Any found security breach that was used for a jailbreak is on the other hand a door that has been closed by Apple. That means it will be more difficult for new jailbreaks in future.

One other reason is the decreasing interest for jailbreaks, because some features or apps that were not available before for the older iOS-versions, now are a part of Apples operating system or available as app for free in the Apple store. As a result, the number of offered apps in Cydias App Store has reduced because it is no longer worthwhile to program and offer apps there. During writing this part the message was published that Cydia App Store will be closed from 31.12.2018 (Becker, L., 2018).

Cydia App Store was not really closed. Means that after 31.12.2018 there is no way for programmers to sell their apps in this store. Before this date commercial apps and free apps can be downloaded further. That should reduce the interest to program new apps and offer them as download in Cydia. It may be the first step before Cydia App Store will be really closed to be a part of IT-science.

To get full access to a device is very important for forensic work. Jailbreaking can open ways to get access to all system files that give us more information about the device, the user, passwords and may be a way to get a physical image from the data storage. A physical image from the data storage can also show ways to recover deleted files.

2.1.1 The ”right” Jailbreak

First problem was to find a ”real” jailbreak, because there were offered a lot of fake jailbreaks, called scums. There is not any official platform to get information of available jailbeaks. No wondering why, cause there are not real business partner where jailbreaks are offered as a software product. To get an overview to current available jailbreaks only two good sources were found:

- `https://www.theiPhonewiki.com/wiki/Jailbreak`
- `https://canijailbreak.com`

Something new for me was that a large number of jailbreaks were offered in the internet. At the first look it seemed that each iPhone and iOS-version can be jailbroken. But some of offered jailbreaks are scams. Also fake news were found, telling about released jailbreaks that can jailbreak current devices and iOS-versions in reality could not be jailbroken at this time.YouTube videos were found showing how an iPhone with the newest iOS-version can simple be jailbroken. Information where to download the jailbreak and following the instructions how to install it were posted. In the first look it seemed to be a good idea to jailbreak the iPhone this way. But there were jailbreaks offered that did not work and other were sold, but could be downloaded from the right page for free. Some sides may bring malicious software or trojan horses on the iPhone executing them (Theiphonewiki.com, 2018).

The problem was to know when you will get working or fake jailbreaks. As there are no official sides where all serious information to jailbreaks are stored.
iPhone Wiki is not a platform information could be trusted blind, but it was the best way to get the first information and a good overview about all ”real” jailbreaks. To be sure this information is right it must be proofed on trusted sources.
Such a way was to have a look to web pages from well-known computer magazines that have tested jailbreaks that can be trusted.
The next problem was to get the right iPhone type that has installed the iOS-Version that can be jailbroken. That was also a hard part in practical work. Thanks for a big internet market place where also second-hand iPhones were offered. A lot of needed iPhones were found there. It was simple to find an iPhone 7 or X, but in most cases, there was no information about the installed iOS-version.

That meant that the sellers had to be written, asked for information to the installed iOS-version and waiting for answers. And at least a little bit luck was needed to win the auction.

One way to get an iOS-version that can be jailbroken can also be an update to a higher version. This can be a way if for a current iOS-version a jailbreak was found and Apple has not released a newer version before. Mostly the time window to do this is open only for a short time until Apple releases a new iOS-version.

Another problem was that iPhones could probably be jailbroken with only one jailbreak. If the jailbreak did not work it is not recommendable to install another jailbreak to the same device. That may cause to problems with the operating system. It is not simple or may not possible to deinstall a jailbreak. It also did not help to reset to factory settings, because the jailbreak is a part from the operating system that will not be changed in this way. The only way is to install a new operating system, that will delete all data and may update to a version that can not be jailbroken.

2.1.2 Available Jailbreaks for iOS 11 and 12

Searching for jailbreaks first the semi-untethered Electra jailbreak was found that should be able to Jailbreak iPhones from 5 until X with iOS 11.1. until iOS 11.4.1.
Electra can be installed using the Cydia Impactor or Safari browser.
Electra can be downloaded under `https://coolstar.org/electra/`
Second jailbreak was LiberIOS that was able to jailbreak iOS-versions from 11.0 11.1.2.
Meanwhile there is a third jailbreak available named Unc0ver. It is a semi-untethered jailbreak working with all iOS-versions 11 and 12.0 until 12.1.2 for the same devices like electra does. Pwn20wnd, a former member of the Electra Jailbreak team released Unc0ver Jailbreak tool.

All available jailbreaks for iPhones until today are shown e.g. on:
`https://www.theiphonewiki.com/wiki/Jailbreak`
`https://canijailbreak.com/`

2.1.3 Differences between Jailbreaks

Jailbreakes using a security breach to get into the system with root privileges. To do this there are different ways that depends on the security breach and the jailbreak.

A Jailbreak can be untethered, tethered and semi-tethered. The main difference is that an untethered jailbreak will work if the device was turned off and has been restarted. An iPhone with a tethered jailbreak will not reboot again without any action. A semi-tethered will boot again, but the jailbreak must be installed again to run (Benjamin, J., 2011).

There are different ways how to jailbreak an iPhone.

- Executable files

My first experience with jailbreaks were using an executable file. To perform the jailbreak the iPhone had to be connected using one USB-port from a Computer. Executing the file has jailbroken the iPhone and installed Cydia to the iPhone.
Another way to jailbreak with executable files was to change the OS installing file, the IPSW-file of an iPhone. This works adding the jailbreak to the IPSW before installing an operating

system to the iPhone.

This method can not be used for forensic work, because the installed operating system will be deleted and a new one installed. All data would be lost.

- Impactors

Cydia Impatcor is a program that can be installed on Windows, Linux and Mac machines. To install a regular IPA-file (iOS App Store Package) the app-store or iTunes can be used. IPA files are compressed self extracting files for iPhones. IPA-files are installing format for iPhones and iPads. The content is a program that can run on a iPhone or iPad.
E.g.7-Zip can be used to have a look into the content from an IPA-file a compressing program.

There are impactor programs from other ancestry only for installing a special jailbreak. One example is Pangu jailbreak that has its own Impactor named php helper.

- Browser

Using the Safari browser is one option to install a program to an iPhone. That is only for some jailbreaks or applications available.
If the URL is known you can key it into the browser to open the homepage. Another way is to search for a link to get there.
On the homepage, you have only to type install jailbreak and follow the instructions. In some cases, another program has to be installed or used that will bring the jailbreak to the iPhone.
Sometimes Links were offered from fraudulent providers and you will get not perform the desired a jailbreak.After the device is jailbroken a way to get access to all data from the iPhone is needed. That means to get a connection with root privileges to the device. One way is using a connection via SSH. The SSH protocol is a method for secure remote login from one computer to another. Well known for this task is OpenSSH. But there some more that can be used like WinSCP.

2.1.4 Jailbraking risks

Jailbreaking a smart phone will have some risks which should be considered:

- National law performing jailbreaks should be respected: United States, Norway, Germany and a lot of other countries it is not forbidden to jailbreak a device. There are other countries where it is unclear or may be forbidden by law. It is urgent to proof this before downloading or working with a jailbreak to get not punished.
- The warranty may be lost
- Hardware may be damaged, e.g. through overload
- Danger of Malware infection increases

- The device may work unstable or freeze. E.g. with a jailbreak for iPhone 3GS the baseband firmware was changed and made some devices unusable.
- May be losing Data.
- Unknown apps installed with Cydia have unknown impacts of access.
- Current jailbreaks during installation need Internet access. The reason for that is a verification to the used account and password from Apple to install an app outside from the Apple Store. At the moment the device is connected to the internet, remote deletion or blocking to the iPhone can be triggered (Mead-Green, R., 2017).

2.1.5 Apple ID

Apple ID is the e-mail-address that is used to create an account to get access to Apple services e.g. Apple App Store, iCloud, Faxe Time, etc.. To jailbreak iPhones with iOS-versions 9 until 12 with the Cydia Impactor an Apple ID and matching password its a must. All what is needed to get the new Apple-ID is to create a new Apple account. One e-mail address and some private data were asked for.

A new Apple-ID can be created at following Apple page: `https://appleid.apple.com/account#!&page=create`

My first Idea was jailbreaking with Cydia Impactor will need Apple-ID and password from the user-account that is connected to the iPhone. In jailbreak descriptions have not be found any information to get the correct answer if my Idea was right. Following this idea before performing the first jailbreak the to the iPhone connected user-account was changed to another Apple account.

At that moment the account was changed, Apple checked the apps that are connected to the new account and erased all apps that were not listed. That would be dreadful to loose a lot of information with the deleted apps. In this case it is urgent not to change the connected account in iPhone settings.

To find out if the to the iPhone linked Apple-ID has to be used to jailbreak with Cydia Impactor, first a jailbreak with the to the iPhone connected Apple-ID was done. In the second test a new created Apple-ID was used. Both jailbreaks were successful. As a result there was no need to use the Apple-ID which is connected to an iPhone. Any Apple-ID with the matching password could be used.

2.1.6 Passcode

To jailbreak an iPhone access to the mobile phone is needed. The iPhone must be unlocked and connected to a trusted computer to perform the jailbreak. When a passcode is activated the passcode is also needed to perform the jailbreak.
Testing a passcode manually its not helpful. One reason is that more than 3 wrong entered passcodes will lead to a time-out and at least will lock the phone after more tries. In this case it

can not be unlocked even with the right passcode. If the user has set an option, the phone can also be reset into Factory settings after several attempts. In this case the decrypted data will be lost forever (Help.apple.com, 2018).

If the passcode is unknown, there were some options to get it. Finding a solution to get the code were always brute force attacks using a security breach. Brute force operates like manual testing the pass code. The main difference that runs automatic without counting the attempts because of the used security breach. Explaining all available options would leave to far and may be a topic for another master thesis.
The difference of manual entering the passcode is that an exploit is used that will not lock the phone. That means that iPhones will not erased, also if the user has set this option in his own settings. Brute force tools operates like an external keyboard and they are much faster than a manual typing could do (Information Security Newspaper , 2018).
The safest way seems to be using GrayKey-Box, that shall open all kind of iPhones and iOS versions. This box should be able to open an iPhone with a six-digit pin in 11 hours. The GrayKey Box is very expensive the cheapest release is available for 15.000 US$ (Beiersmann, S., 2018).
There were some less expensive solutions. One is offered from Cellebrite that is a service. To get the service type and iOS-version from the iPhone are requested. If the device is supported it must sent to Cellebrite. Approximately 3.000$ had to be paid for this service (Gallagher, S., 2018).

With IP-Box, working until iOS 10.3.3, IP Box working until iOS 10.3.2 and MFC Dongle, only supported until iOS 7 and some iOS 8 versions this work could be done for a few hundred Dollar (Fonefunshop.com, 2018).
I have used the IP-Box and the MFC Dongle to unlock iPhones with iOS 7. It worked reliable. A four digit code could be found quickly with the option of most known codes if there was a match to that numbers. If not, it could take some days. The MFC Dongle could be set to e.g. 0000 as start digit but it will take time if the end code is9999. Another option is to set any other wanted startcode or range if e.g. a part of the code was known.

To protect iPhones from any attacks using the lightning port the USB mode was disabled after the device was left idle for a week starting with iOS 11.4. With iOS 11.4.1 the USB Restricted Mode started after just one hour. This can be activated and deactivated from the user with the passcode from the iPhone. Starting with iOS 12 the USB Restricted Mode was basically set. When the USB Restricted Mode was activated, the lightning port could only be used for charging the device. That means that in this case all described methods before, including the GrayKey-Box, would not run any more (Schmerer, K. , 2018).

2.2 Forensic definition and explanation of forensic soundness

The term forensic comes historically from the Latin word forum that means marketplace. In ancient Rome, court proceedings, investigations, verdicts, and penitential executions were carried out on the market square. Over time the word has changed to the today known word forensic.
In the actually use forensics is a collective name in scientific and technical use that includes

those areas in which systematically criminal acts are identified, analyzed and reconstructed in a way that it can be presented to court as an evidence.
Terms computer forensics or also called as digital forensics has been used in recent years for the methods of detecting and determining criminal offenses in the field of computer crime. Digital forensics is the recovery and investigation of data found in digital devices (Carrier, B, 2001).

In the actually use forensics is a collective name in scientific and technical use that includes those areas in which systematically criminal acts are identified, analyzed and reconstructed in a way that it can be presented to court as an evidence.
Terms computer forensics or also called as digital forensics has been used in recent years for the methods of detecting and determining criminal offenses in the field of computer crime.

Forensic acquisition can be done with multiple methods. Anyway data must be collected, stored and analyzed that is acceptable by the law and can so be used as evidence.
Forensic soundness is given when digital data was not corrupted, destroyed or changed during the investigate processes neither on purpose or by accident.
Sometimes we need to make a simple copy to get the needed data. If we do that the copy changes the timestamps of our files.
Opening a file to have a look at the content may change the content too. To have forensic soundness it must be declared why and what we have changed (MCKemmish, R., 2008).

Acquired data could be of evidential value. Every handling with the data can have real impact on legal proceedings. It is essential to handle digital evidence as every other physical evidence and maintain a clear, documented chain of custody. From the moment evidence is obtained it must be documented chronologically how it has been handled, by whom, and for what purpose (Varenkamp, P., 12/2017).

2.3 Open Source in forensic

A lot of open source tools are used in forensic work. There are enough tools to perform a completely investigation with open source tools. Sometimes for a specific problem there may be only an open source tool that can be used, because there are no commercial programs available to do the work. Commercial programs also have included open source tools that process a part of the work or use open source data bases.
To be sure that a commercial program has worked without an error we need the dual tool verification. Commercial tools are mostly expensive. An open source tool is a good way to verify the results.

Commercial tools give us results mostly without explaining how it came about. Open source tools provides their own code to the examiner (Altheide, C. and Carvey, H., 2011a).

Open Source sounds same like free software. The main difference for forensic use is that free software can be either, open source and closed source. The free software may also only be free for private use and may to be paid for commercial use like forensic work. Free Tools are also used for forensic work in compliance with the legal conditions (Peterson, C. , 2017).

2.4 Physical and logical acquisition

2.4.1 Physical

A physical copy is a completely backup of all sectors starting on the first and ending at the last sector. Physical acquisition needs a physical access to the data storage.
Physical copy can be used like the original storage. That means all stored data including deleted data was copied to an image-file (Britz, M., 2013).

Such a copy can also be done from volatile data, like random access memory.

2.4.2 Logical

Unlike a physical copy, the logical copy is only possible with a program or tool that can interpret the file system of the volume being backed up. Only then the directories and files become available and can be logically backed up. In the case of physical backup, this does not matter because the data carrier is backed up bit by bit. It is therefore also possible to secure encrypted hard disks using this method. Only when processing this data, the data must be decrypted and the file system must be recognized. Even if detection of the file system has not success, the search and recovery of data is still possible (Hoog, A. and Strzempka, K., 2013).

The logical copy can contain also system files when the permission allows such an access. In this context is also spoken from an advanced logical extraction. Such a data extraction from a iPhone is in general only with jailbroken devices possible. Otherwise there will not be access to the system partition (Cellebrite, 2019).

2.4.3 Differences for forensic manner

The decisive difference between a physical and a logical copy is that you will not get any as deleted marked data that was stored as file on the data drive. That includes random access memory that is temporally stored on the data storage and other temporally stored data from programs or apps that can contain passwords, key, chat conversation and much more. Recovering files is only possible if we have a physical device or a physical copy from the data storage.
To get all data from a data storage there is no other method than making a physical copy.
As far as it is permissible and possible a physical copy should be made. Only a physical image contains exact the same data as the original. In most cases you are not able to keep the original data storage. If you are working for prosecution on a case and have only a copy from some files or a logical volume it may happen you find new hints to deleted files or to files that you have not copied. Without a physical copy you were not able to finish your work. On the other hand you need a court order, that allows you to make a physical image. Sometime a court order allows only to copy certain files with relevance to a case (Varenkamp, P., 12/2017).

2.4.4 Challenges with decryption

Even if there is a way to perform a physical backup from an encrypted data storage, the data will be unusable if you have not the encryption keys. If you have success to a running operating system you will see the system files encrypted and may be the data partition files too. In this case, the folder and files may be copied to an external data storage.
E. g. performing a physical backup on an unlocked and running Microsoft system with Windows 7 until 10 that has activated encryption with an encryption program will give you an image with decrypted data. This is because the system must have decrypted files to run them.
I used this way to perform physical backups from devices using Windows 7 until 10 (today). A programm or a command line can be used to do this. The privileges from an administrator are needed to have physical access to the data storage and start the physical backup. Descriptions how this can be done will be found with the used programs.

My idea is to connect to the jailbroken iPhone as root and use the command line from the iPhone. This may open an access to the unencrypted data storage from the device.

Elcomsoft with Elcomsoft iOS Forensic Toolkit has found a way to get physical access to jailbroken iPhones up to iOS 12 and to perform a physical backup from the system and data partition. Elcomsoft show an example using an iPhone XR with iOS 12.1. I have not found a jailbreak that was verified or came from a reliable source.
However Elcomsoft iOS Forensic Toolkit also works with iOS 11-version. This fact first made hope for that the physical copy can open a way to restore deleted data with file carving methods. In the description from Elcomsoft it becomes clear that this is not possible and probably will not be any more. The reason is, when files on a encrypted Apple partition were deleted, the encryption key will be deleted to. At the end the physical backup will give access to the same data as a completely copy from the system and data partition (Katalov, V., 2019).

2.5 Apples new File-system APFS

In a short summary we take a look at the new file-system from Apple with the information from the article Decoding the APFS file system. Digital Investigation (Hansen, K.H., Toolan, F., 2017).
In order for the user to be able to use his operating system to ensure that the programs run correctly and that the correct data is retrieved in the event of a click, something is needed that most users will not notice. It is the file system that accomplishes these tasks. Since 1998, the file system HFS+ provides for it on the Mac. HFSX was used with the first presented iPhone in 2007. The only difference to HFS+ was that it was case sensitive. That means that the operating system strictly distinguishes between upper and lower case of a file name. Due to the ever faster hardware, the file system could not keep up with the increasing speed of SSD storage media. That's why Apple has equipped since iOS 10.3.3 their iPhones with a new file system. This new file system is called APFS and is intended to play out its advantages, especially in the fast SSD storage media. This happens among other things that files are not stored multiple times than linked and it just looks like they exist several times. In addition, we keep the old file and changes made afterwords are saved separately. When accessing the file, so the old file is called with the changes and displayed as the current file. This new technology makes the internal copy

process much faster.
What has the file-system APFS changed for forensic data acquisition?
First, the file system does not matter in a physical backup, as a 1 to 1 copy is created bit by bit. For a logical copy, the forensic backup program must be able to recognize and display the file system.
If we want to forensically evaluate the physical backup, we need tools that recognize the file system. Otherwise, we would only be able to search for files and restore them. The recovery of deleted data has become more and more difficult in recent years, particularly with the introduction of SSD memories, since they also reorganize using read-only protection while deleting data.
Scientific experiments have enabled the APFS file system to recover containers from previous recovery points. By comparing levels, previous existing folders / files as well as changes in the status of this object could be detected.
This seemed to be good news for the forensic worker because the recovering of deleted directories and files would work much better with the new file system APFS. This can only be helpful with not encrypted file systems as described at Point 2.4.4 (Varenkamp, P., 12/2017).
And this seems to be the point. Until APFS every file on the data partition was encrypted with a unique key. As described before, with APFS a file is stored only one time on the partition. The main difference is now that there are not different files, but the changes that were saved in the same way like the files. Deleting one changed example from the original files will delete only the differences and the belonging encryption key. At the end the result for a way to recover files is the same. It seems not that there will be a way in the future to recover files from the encrypted data partition of an iPhone regardless to the file system (Apple.com, 2018).

Chapter 3

Methodology

The previous Chapter 2 gives an introduction to the points that have been researched for a better understanding and to answer the research question. In this chapter, the methodology and research methods will be explained. The chosen research approach and design will be explained.

3.1 Research Methods

On this point, the validity using different jailbreaks with different devices that also have other iOS-version will be discussed. To answer the research question I have done a literature search to use the information for the experimental work. To get answers different tools will be used that should give an insight into what happens jailbreaking an iPhone and performing a backup image from the data storage. That includes advantages and disadvantages that may occur under circumstances. Literature research and experimental work should give together the needed results. The results will be discussed to get answers to underlying questions and at least to the research question.

3.2 Research Approach

The research approach used in this thesis is qualitative and will perform hands-on experiments in a laboratory environment. The results of the experiments will be analysed and compared to shows us the differences.
A qualitative approach is well known to be used in social and empirical researches but also applicable to be used for a technical research.
A qualitative approach is well known used in social and empirical researches but also applicable to be used for a technical research. Therefore I discarded my first idea using a quantitative approach. A quantitative research approach is collecting data like numbers or values that are measurable in a systematic way. It can be used to answer questions on relationships within measurable variables (Leedy, P. and Ormrod, J., 2015).
Even as the used method may give an option to count if more or less files have been acquired with a jailbroken or not jailbroken iPhone that would not be a measuring instrument that can be used to answer the research question. The qualitative research approach will be used in a

deductive way to confirm or reject the theory. A deductive way starts with a theory that is here to use a jailbreak as a forensic method to get full access to the data storage of an iPhone. This theory was used to develop the hypothesis that jailbreaking can be used as a technique to create reliable, verifiable and forensically sound images from an iPhone to provide evidence robust enough to be valid in a court proceeding. To answer the research question I need to design a research strategy (Dudovskiy, J. , 2019).

3.3 Research Design

This thesis will use a qualitative research strategy. The used design is the case study. It will start with data collection from a literature search using keywords. The found details in literature will be used in the experimental environment.

Another part will use an experimental design. Experimental research in this thesis will proof if given answers from the literature research stayed the same to today devices and operating systems. This evaluation proofs the information from the literature research to confirm them and will give us new information and may show differences between literature research. The results will follow a confirmation or rejection of this Theory.

3.4 Experiment

Experimental research is one of the fundamental research methods. An experiment is a scientific tool that can be used to check the theory in real environment (Moy, T., and Tyrkus, M. J. (Eds.), 2016).
Two variables must be proofed against each other to get answers. That means at least two methods are needed to be compared to each other. Finding answers to my questions and to answer at least the research question I will perform first a forensic acquisition with in Chapter 4.1 mentioned different iPhones and different iOS-versions. These iPhones will be jailbroken and acquired again. The acquisitions will be done with different tools to find out if this leads to different contents. The results will be compared to each other to see how the jailbreak influences the results and if different tools lead to different contents. Then I will have a look if files which were acquired additionally from jailbroken iPhones have information that can be an evidence. Data can be an evidence if there is information stored which make statements to a case. I will search to find traces if data has been changed in a way that forensic use of jailbreak will make inadmissible. For this, I will only look on files that have changed during or after the jailbreak. Therefore I will sort files using timestamps entry last changed. If this concerns to files on these data partitions changes should double checked by using an MD5 hash logarithm to see if the content has changed too. This part does not work with data from system partitions, because there was no access to these files before a jailbreak. At this point, changed files will be checked to their functionality that may give hints if they can influence the evidence.

3.5 Other Methods

The research was started with the idea to find out how the jailbreak really works as an experimental part of this thesis. To get an answer to this question the best way seemed to be reverse engineering. With reverse engineering jailbreak can be examined to get knowledge about the implemented functions. In other words reverse engineering can be used to get information how jailbreak exactly works. This expected to be the best way to get an answer if and in which way system files can be changed by executing jailbreaks. That came soon to the result that this would go over my experience and would expect to take so much time that it could be a project for a future work or another master thesis that deals with such a research question. Another point is, only the work of one jailbreak is known, after reverse engineering was done. As known from the past there have been released a lot of different jailbreaks from different developer. There are three jailbreaks for iOS 11 and 12 available. Jailbreaks does often not release in only one version. This means getting answers how jailbreaks work needs reverse engineering for all versions of jailbreaks. For iOS higher than 12.1.2 a jailbreak has not released until the writing moment 13. May 2019. That means that there might release another jailbreak that also works in the needed way. This are the reasons why I have discarded this idea and changed my point of view to find out what data was changed on file and data partitions.

Chapter 4

Experiment

With the information of my literature research, I know that I will be able to jailbreak a lot of iPhones 5 until X with iOS 10 and nearly all version of iOS 11. iOS 12 also can be jailbroken until version 12.1.2 today. The upper versions that are 12.1.3 and 12.1.4 were not supported yet. The newest devices that are XR, XS and XS Maxx cannot be jailbroken as I have done the experiments in March/April 2018. As I know from the beginning of my research that can change every day. The first iOS 11 jailbreaks released at the beginning of 2018. At the beginning of 2019, the last jailbreaks for iOS 11.3 and 11.4 were available.
To backup mobile devices, there are a lot of free and commercial tools available. In this experiment, I used the command line, iTunes, Phone Paw, UFED Physical Analyser, XRY, and iOS Forensic Toolkit to see what differences occur to the result of an acquisition after the used iPhone has been jailbroken.

4.1 Configuration

Component:	Description
Description:	MacBook Pro (15,middle 2010)
Operation System:	OSX Yosemite 10.10.5
Operation System:	BOOTCAMP with Windows 7
Processor:	CPU Intel Core i7 2,66 Ghz
RAM:	8 GB RAM 1067 Mhz DDR3
Data Storage:	SSD Samsung 860 Evo 500 GB
Graphic Card:	Intel HD Graphics 288 MB
Processor:	Intel(R) Core(TM) i7-4510U CPU @ 2.00GHz
Description:	PC (Selfmade)
Operation System:	Windows 10
Processor:	AMD 9250 Eight-Core CPU
RAM:	16 GB RAM
Data Storage:	SSD Samsung 860 Evo 500 GB
Data Storage:	HDD Seagate 1TB
Description:	Fritz Router 7390
Operation System:	Firmware FRITZ!OS 6.85
Software:	Mac OSX Yosemite 10.10.5, Windows 7 Professional 64 bit, Windows 10 Pro 64 bit, Command line / Terminal, winscp portable 5.11.2, OpenSSH, AFC2, iDevice Manager (iPhone Explorer) 8.5.3, iTunes 12.9.4, Phone Paw 5.2.0, UFED Physical Analyser ,XRY, iOS Forensic Toolkit 4.1, FTK (Forensic Toolkit 7.0), X-Ways Forensics 19.6

Table 4.1: Hardware Configuration

Used iPhones:

Component:	Description
Model:	iPhone 4
Model Number:	A1332
Manufacturer Part Number:	MD128DN/A
Capacitance:	8 GB Space
Operating System:	iOS 7.1

Table 4.2: iPhone 4

Component:	Description
Model:	iPhone 4s
Model Number:	A1387
Manufacturer Part Number:	MD235D/A
Capacitance:	16 GB Space
Operating System:	iOS 6.1.2

Table 4.3: iPhone 4s

Component:	Description
Model:	iPhone 5
Model Number:	A1429
Manufacturer Part Number:	ND297DN/A
Capacitance:	16 GB Space
Operating System:	iOS 9.3.3

Table 4.4: iPhone 5

Component:	Description
Model:	iPhone 5s
Model Number:	A1457
Manufacturer Part Number:	ME436DN/A
Capacitance:	32 GB Space
Operating System:	iOS 11.0.1

Table 4.5: iPhone 5s

Component:	Description
Model:	iPhone 7
Model Number:	A1457
Manufacturer Part Number:	MN8X2RM/A
Capacitance:	32 GB Space
Operating System:	iOS 11.2.6

Table 4.6: iPhone 7

Component:	Description
Model:	iPhone X
Model Number:	A1901
Manufacturer Part Number:	MQAC2ZD/A
Capacitance:	32 GB Space
Operating System:	iOS 11.3.3

Table 4.7: iPhone X

Component:	Description
Model:	iPhone X
Model Number:	A1901
Manufacturer Part Number:	MQAF2ZD/A
Capacitance:	256 GB Space
Operating System:	iOS 12.1.2

Table 4.8: iPhone X 256GB

4.1.1 Preparation and recommended settings

Before jailbreaking an iPhone or any other device is very urgent to perform a backup. An intervention in the system of a device can lead to the fact that access to the device and the data is no longer possible. Another effect can be for example that the device does not work stable, freezes or may restart without reason. Sometimes the only way to fix this problem may be a new installation from the OS. In this case, all data that was stored on this iPhone will be lost. As described before, the decryption keys will also be deleted and the data can not be recovered anymore. An iPhone backup can be done with a lot of tools e.g. iTunes, PhonePaw etc. (Chapter 4.2)
Regardless which tool was used to perform the backup, most programs are able to scan different backups. However, depending on the used tool there might be different ways to back up the device, this causes that the backup could contain not all data that could have been acquired with another tool or method. Therefore it is important to perform the backup with the right tool if you want to have specific data. Under certain circumstances, the wanted data can only be acquired if the device has a jailbreak. If the iPhone should be jailbroken, it must be checked if a jailbreak for the iPhone that should be jailbroken is available. This depends on the hardware and also on the installed iOS.

To be sure the jailbreak installation can be successfully done it is helpful to check some settings before.

- The storage must have enough free space for installing the jailbreak.
- The flight mode should be set.

- An Internet connection is needed to install jailbreaks like Meridian, Electra and Unc0ver. One way for jailbreaking was to visit some special web-pages where the jailbreak could be installed online. The other way was using the Cydia Impactor or another impactor. To install a jailbreak with Cydia Impactor an Apple account and matching password was needed too. For this, an anyone Apple user account with matching passcode can be used. A developer account can also be used but was not required. Another reason why the iPhone had to be connected to the internet connection can be to install additional programs with Cydia.

- The option Find My iPhone should be deactivated, to do this the Apple-ID and password that was a associated with the iPhone will be asked. If the last owner has activated Find My iPhone before the iPhone was ensured, he is able to delete or lock the phone from another device until it was deactivated. Find My iPhone is a program to search a lost device and has also the options to lock or erase the lost iPhone. To do this Find My iPhone can be used from any other Apple device or with log in to the iCloud. If the user has started one command before the Find My iPhone was deactivated, a short connection to the Internet will be enough to start lock or deleting the iPhone. There is no way to stop this action.

- If an iPhone was connected first time to a PC, a question will be displayed at the screen from the connected iPhone if this connection to the PC will be trusted. To get access from the PC to the connected iPhone it has to be confirmed.

- During the execution of a jailbreak, the access to the iPhone should not be interrupted. The jailbreak will be installed to the system partition. An interruption will stop the installation, but can also leave to an error in the system partition files. That can lead to an unstable system or more. To make sure that the connection will not be interrupted, the automatic screen lock must be deactivated. One way is to deactivate the code lock and touch ID too. On older iOS-version it was possible to deactivate the automatic screen lock from an unlocked device without knowing the passcode. To do this with current iOS versions like 11 and 12 the passcode from the iPhone is needed.

Every jailbreak has its own installation instructions. Even if there are often nearly the same, one different point can be the reason why the installation fails. I made good experiences to read and follow the instructions from the jailbreaks I have installed.

Another point needs also attention that occurred during the experiment. One iPhone that was connected to the internet started to update to a higher iOS version. After denying the update installation a screen appeared to enter the passcode. After entering the passcode, the update started and it was not possible to abort it. The reason was that instead of entering the passcode the update had to be denied again. This was written in little letters at the bottom of the screen.

4.1.2 Jailbreaking

Jailbreaking is a method that opens ways to get full access to the data storage from an iPhone. Jailbreaking will install a program to the system partition into the root directory. That will be a change to the system partition. To jailbreak a device a security breach must be known or found

that will open a method to get access as root to the device. To find such a useful security breach and develop a jailbreak that works is a difficult work. It needs very good knowledge about the operating system of an iPhone and a big effort to implement this in a jailbreaking program. But to do this first a useful security breach must be found. That can take a lot of time and may end without success. When a security breach was found and used for a public jailbreak, Apple will search to close the used security breach as soon as possible, that may be the following iOS version. This causes that a jailbreak may only work with one iOS version. Jailbreaking opens ways to connect as root to the device. Root is the master of the OS and able to delete, install or execute programs. That means that there are no limitations. To get full access to the data storage of an iPhone or other smartphones may not be enough to jailbreak the device. There must be also a way to connect to the device as root that opens full access to the data storage. One way is to use a program that was installed with the jailbreak that can connect to the device. OpenSSH is e.g. such a program that is installed by default with e.g. Electra and Unc0ver jailbreaks. Another way is to install a program using Cydia. With Cydia, such a needed program can be searched and installed too. Cydia works like the Apple Store and offers Apps that can be downloaded and installed without the Apple Store on jailbroken iPhones.

To jailbreak iPhones with iOS 11 and 12 today (April 2019) there are 3 jailbreaks available. LiberIOS is able to jailbreak iOS-versions from 11.0 11.1.2. Electra and Unc0ver can jailbreak all iOS11-versions. Electra released before Unc0ver. Electra has one version that can only be used with a developer account and one that can be used with every Apple account. I used the one without a developer account, that worked without any problems. Unc0ver uses the same exploits as Electra and can jailbreak too all iOS11-versions and also iOS 12.0 -12.1.2.

The jailbreaking part of the experiment was also performed with the Meridian jailbreak. The Meridian was used to jailbreak an iPhone 5 with iOS 9.3.3. That jailbreak was done to have a look at one of the last iOS devices that have the old file system HFS+. All other devices with iOS 11 were jailbroken with the Electra jailbreak. To jailbreak an iPhone X with iOS 12.1.2 the Unc0ver jailbreak was used. This was during the experiment the single tool I found to jailbreak an iPhone with iOS 12.

All these 3 jailbreaks were installed in the same way, using an impactor. Another tested method was to visit the jailbreaking page with the Safari browser and to follow the instructions. To install Electra or unc0ver jailbreak with the Safari browser another tool had to be used. Installing e.g. unc0ver with the Safari browser was possible with the ignition tool by visiting the page https://www.ignition.fun/. For this way, there was not an apple account necessary. Both methods worked only when the iPhone has a connection to the internet.

To install the jailbreaks during the experiment the current Cydia Impactor 0.9.51 was used. The Cydia Impactor had to be started without administrative rights to work. Using administrative rights, the installation of the jailbreak was not successful. The impactor ”installed” the jailbreak or other IPA-files from a PC to the USB-connected iPhone. The files that contain the jailbreaks are IPA-files. This is an apple installing format. The impactor searched after start for a connected iPhone and displayed it when it was connected. The jailbreak-files have been downloaded from the respective provider of the jailbreak. In most cases, there will also be a link to the homepage (http://www.cydiaimpactor.com/) where the current version of the Cydia Impactor can be downloaded. The Cydia Impactor is available for Mac, Windows and Linux

distributions. After the Cydia Impactor was started and has recognized the USB-connected iPhone that should be jailbroken, the jailbreak IPA-file must be put with drag and drop to the Cydia Impactor. At this point, an Apple user ID and password were asked. The first idea was that the Apple-ID and passcode that was associated with the iPhone has to be used. Testing other Apple-IDs with their passcodes come to the result, that they also worked without a problem. This showed that it was no matter where the Apple-ID came from. It had only to be a registered valid ID where the passcode matches to. When such an ID with the matching passcode was entered correct and confirmed with OK, the jailbreak installation started immediately. Otherwise, an error has been displayed that the Apple-ID or password was entered incorrectly. After the jailbreak was installed a new app will be found on the home screen. Before starting the jailbreak app it had to be confirmed under ”Settings>General>Profiles & Device Management” from the iPhone. To do this an internet connection was inevitable. After confirming the state from the jailbreak app changed to ”trusted”. The internet connection should now be interrupted as soon as possible. The last owner can use his account to start deleting or blocking the device from another computer with the option ”Find My iPhone”, as described before.

An internet connection was not required in the past with jailbreaks like pengu9 and evavisi0n. These are executable files that can be executed without an Apple Account that must be confirmed by an Apple server. The way how a jailbreak can be installed seem to depend on the used security breach.

Now the jailbreak Apps have been started without having an internet connection again. After starting the app the jailbreak has been executed. During the jailbreak, Electra created a snapshot from the APFS filesystem before installing Cydia. At this point, it has been displayed ”APFS Snapshot Created An APFS Snapshot has been successfully created! You may be able to use SemiRestore to restore your phone to this snapshot in the future”. In the next step, Cydia was installed on the iPhone. Electra and unc0ver installed Cydia with OpenSSH by default during the procedure. For this, it is useful to know that some jailbreaks have an included app like OpenSSH and some not like the Meridian jailbreak. It can also be a problem if there was a second app installed that worked in the same way. That can lead to conflicts which can crash the system in the worst case. If the jailbreak does not have such a program and there is no way to install a program like this, it makes no sense to jailbreak the device for an acquisition. An acquisition can only be done with a working Cydia and a program that can connect to the seizing computer.

After the iPhone was jailbroken Cydia was started, Cydia went to ”Refreshing Data” and wanted to install updates. This can be confirmed with ”Ignore” (Temporary) because the updates have not been needed for the following experiments. To have a look if OpenSSH or another needed program was installed with Cydia, the Cydia search glass was used to find it. When the result showed OpenSSH and a green hock to the right, OpenSSH was already installed. If OpenSSH or another program was not installed or should be deinstalled this can be done at that point too. But this way can also be used to search and install another program that is able to connect to your phone in the same way.

Remarkable is that an Electra and unc0ver have such a comfortable way to be deinstalled. That may also open a way to install another jailbreak on the same device. To deinstall the Electra Jailbreak I used SemiRestore11/Rollectra. That seemed to work. It seemed because it showed

me that it worked, but after the jailbreak was deinstalled there was no way to look into the root directory if really all parts have been deinstalled. Unc0ver has also a de-installation routine that can be configured in the settings after starting the program. This has not been tested (John, A., 2019).

Some jailbreaks did not install Cydia by default. In my experiment, Cydia was not installed with the Meridian jailbreak. Cydia can also be installed manually on the iPhone through SSH. To load Cydia on a device with the Meridian jailbreak can be done with the following command:

tar -xf /meridian/dpkg.tar -C/

The two older iPhones were jailbroken with Pangu and evasi0n jailbreaks. Both do not need an internet connection or an Apple account to be executed. After downloading the self-executing file was started on a Windows computer. Pangu and evasi0n have jailbroken the connected device after executing. Evasi0n was used for the iPhone 4S with iOS 6.1.2 and Pangu for the iPhone 4S with iOS 7.1. Pangu has installed AFC2 by default.

4.1.3 FilzaJailed

Searching how to jailbreak an iPhone something different was found that seemed to be to good to be true for forensic work because it promised to work without a jailbreak and giving access to the root directory. FilzaJailed is based on tfp0 Exploit of Ian Beer (iHelplounge, 2017). On the homepage from FilzaJailed (https://filza.org/) is told that it is not a jailbreak. With FilzaJailed I was able to get access to the file system from an iPhone 7. After installing and starting the App, it can be used browsing to all data like with a jailbroken device. The files can be changed, deleted or copied. FilzaJailed can browse the directories without an additional program, but the only way to bring the files you want to the other device is using the existing transport routes. Installing additional programs with FilzaJailed was also not possible. These are programs like mail or chat that are able to send copied and pasted files to another client. This significantly limits the methods to acquire files but may be a way to copy certain needed files.

FilzaJailed is not available in the Apple Store. To install filza with an iPhone that has an internet connection only the Safari browser is needed. Typing the URL brings you to the homepage. There is a detailed description how to download and install filza. FilzaJailed says that it can be installed on any iPhone and iPad with iOS 10, 11.0 11.2.1 and 11.3 11.3.4. Downloading the IPA-file and installing with Cydia impactor is also a way that worked.

To install FilzaJailed I used an iPhone 5S with iOS 11.0.1 and an iPhone 7 with iOS 11.3.3. were used. Both were installed visiting the homepage from FilzaJailed. The only difference between the two installations was that different install bottoms had to be used. For iOS 11.0-11.2.1 and 11.3. until 11.3.4. there will be installed ”HappyCast” and for iOS 11.3.- 11.3.4 ”FilzaJailed iOS 11.3.x” will be installed, when the download was confirmed. Sometimes it failed with the report that the download is not possible at the moment. In this case, it took some tries until it the download started. In one test it worked on the next day. It seemed that the server was overloaded on that day. After the app was downloaded it could not be started, because it is from a not trusted developer. To change this the following steps have to be done:

- Start settings and got to general.
- Scroll to ”Profiles & Device Management”.
- Tap 2 times on I-MD Holdings (Hong Kong) Limited until you will be asked to trust the app. Confirm trust. On the place I-MD Holdings (Hong Kong) Limited you will now find the way to delete the app.
- Go back to the app and start it typing on it.

The installation for iPhone with iOS 11.1 wanted to install some other unknown apps too. After starting the app the next pages have been with Chinese letters. Some tries were not successful. At least FilzaJaileds version ”HappyCast” could not be installed in this way.
The installation for to an iPhone 7 iOS 11.3.3 with Filza iOS 11.3.x was successful. After finishing the installation browsing through the whole data structure, including the root directory was possible. A screenshot from the view at the root directory was made as shown in Figure 4.1.

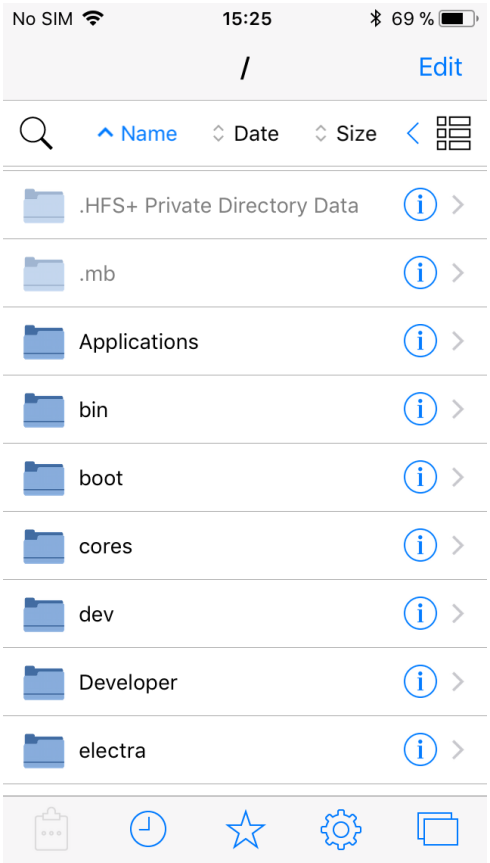

Figure 4.1: Overview from the root directory with FilzaJailed

On the Homepage from filza.org it is told that it is not a jailbreak. But how can a program give root access without a jailbreak? In the research to FilzaJailed there was an article that says that FilzaJailed uses an async_awake exploit.
The main difference was that FilzaJailed was not installed at the root directory like jailbreaks

were. FilzaJailed was installed in the Applications Folder like any other App. FilzaJailed does not have a way to install additional programs. Maybe that these are the reasons why FilzaJailed should not be a jailbreak. In my opinion, a program that uses an exploit to give higher access including reading and write to the root directory is also a jailbreak or nearly the same.
Actually, May 2019, there is information from the homepage that FilzaJailed now also works also on iOS 12 until 12.1.2, but it was not tested here. It can be found under the new name GeoFilza at the same homepage.

4.2 Different methods of acquisition an iPhone

At this point, it will be searched to perform in a first step a backup from the iPhones before the devices with all in Chapter 4 used tools will be jailbroken. In a second step, the iPhones will be jailbroken and with some of these devices, a backup will be performed again. The difference between these acquisitions should give information to answer the research question.
For the jailbreaking part, all in Chapter 4.1 listed iPhones were used. It had been realized that it would take to much time to back up all these devices twice with all used tools. Another point was the limited time which was available to use XRY, UFED and iOS Forensic Toolkit. This was the reason why the selection for this part had to be reduced. Reducing the selections was done by focusing on the newer devices, beginning with iPhone 7.

4.2.1 Command-Line

To back up, an iPhone with the command line can only be done with jailbroken devices. There was no way found to perform a backup in such a way with a non-jailbroken iPhone. To connect from the command line to the jailbroken iPhones SSH were used. If SSH was not installed with the jailbreak, but Cydia was present a tool that supports SSH could be installed. In this case, OpenSSH has been installed with Cydia. To do this Cydia had to be started. The magnifying glass in Cydia was used to search for such a program. If the needed package was found it was also displayed with a green hook when it was already installed. If the package was not installed it could be chosen and installed at this point. To deinstall the package it could also be removed with Modify.

To connect the acquisition PC and the iPhone had to be in the same network and IP-range. From the command line, the connection was started with the command ”ssh root@[iPhone ip]”. When the iPhone was reachable the root password has been asked. If not, it happened that WLAN connection had been off or disconnected. The root password is alpine when factory settings haven’t been changed. After the connection was successful proceeded the command line from the connected iPhone was displayed. All commands have now been executed from the connected iPhone and not from the acquisition computer. That means that only commands could be executed that are known to iOS from the connected iPhone. Connected as root to the iPhone the directories could be seen and changed to the root directory using the command ”cd”. Listing the content from the root directory showed the whole directory tree. The content has shown all files and directories that have been stored on the system and data partitions.

To see the partitions following command was used:

”*cat /etc/fstab*”.

As a result, I was able to see the partitions stored on the data storage from the connected iPhone. The next output has been displayed e.g. with an iPhone X (iOS version 12.1.2):

root# cat /etc/fstab
/dev/disk0s1s1 / apfs ro 0 1
/dev/disk0s1s2 /private/var apfs rw,nosuid,nodev 0 2
/dev/disk0s1s3 /private/var/wireless/baseband_data apfs rw,nosuid,nodev,nobrowse 0 2

APFS-filesystem was first time published by Apple 27.03.2017 with iOS-version 10.3. APFS replaced the HFS+ Filesystem from this point. APFS has been explained under Chapter 2.5. Having a look to devices before iOS 10.3 with the same command the only difference was that ”apfs” was replaced with ”hfs”.

The main difference between the iPhone 4 to newer iPhones is that the system and data partitions are not encrypted. Beginning with iPhone 4S the data-partition (/dev/disk0s1S2) is encrypted. A physical copy will bring encrypted data from the data partition that must be decrypted to get visible data that could be analyzed. All data that is on the data partition can be reached from the root directory under the path /private/var. That means that on this path all directories and files from the data partition are stored.

To acquire a device with the Unix command line utility ”dd” can be used with Mac, Linux-PC and from iPhone. Devices using Windows-OS do not have such a command on board. There are programs like WinDD that can be installed to fix this problem. For the acquisition from an iPhone, this command on the Windows PC was not needed. As described before, after connection to the iPhones the commands are executed from the iOS of the iPhones.

In a first test, an iPhone should be connected to the acquisition computer with the guest WLAN registration that had limited rights over the Fritz router. Using the guest registration to connect as root to a jailbroken iPhone has not worked. With the unlimited WLAN account, the connection as root was successful.
The IP-address of the iPhone needs to be known to be able to connect to this device as root. To see all devices that have been connected to the used network with a windows machine the following command was used:

ipconfig /all

Another way to have a look to the connected network are the WLAN settings from the connected iPhone by typing on the information symbol. The IP addresses from the iPhone and router were displayed.

With the next command physical backups from an iPhone 4 (iOS 7.1) and iPhone 5 (iOS 9.3.3) have been performed:

ssh root@[iPhone ip] dd if=/dev/rdisk0 bs=1M | dd of=imagename.dd

For example with an iPhone 5S, I used this command:

ssh root@192.168.165.63 dd if=/dev/rdisk0 bs=1M | dd of=iPhone5s.dd

The image was stored at the point of the directory the acquisition computer has been last. To save the image in another directory one way is to change the directory with the command cd or to write the absolute output path in the command line.

t took about 18 hours to image an iPhone 5S with 16 GB internal space and about 9 hours for the iPhone 4 with 8 GB internal space using this way. That has been more than 1 hour for 1 GB. And it took several attempts until the full image was written without aborts. One reason was that the router first has disconnected all connections every midnight until these settings have been switched off. Other reasons have been energy saving settings. Using the under Chapter 4.1.2 described recommended settings helped to fix this problem. At least the images were written completely.

To acquire the partitions separately the next commands were used:

ssh root@[iPhone ip] dd if=/dev/rdisk01s1 bs=1M | dd of=partition1.dd
ssh root@[iPhone ip] dd if=/dev/rdisk0s1s2 bs=1M | dd of=partition2.dd

On the next step tries with the same commands to acquire an iPhone 7 (iOS 11.2.6) and X (iOS 11.3.3), had not worked.

It was displayed that it has failed to open /dev/rdisk0 because this operation is not permitted. Searching for a way to perform a full disk image with the command line and the used iPhone 7 and X failed. But even as it were possible the data partition is encrypted and had to be decrypted to see the content. There is no way to recover deleted encrypted files that could be stored in physical backup from such a device. That means that physical images will have at least the same content as logical images have.

To get the logical content from the data partition following command was used:

ssh root@[iPhone ip] -p 4242 tar -cf - /private/var/' > datapartition.tar

The whole content from the data partition is stored under the path */private/var*. With this command, the whole logical content stored at the data partition from the connected iPhone was being copied and saved into a compressed tar-file.

4.2.2 iTunes

iTunes is a free program from Apple that gives access to the Apple Store to apps, music, videos, Apple TV and iCloud.
All this can be synchronized with iTunes to a PC, iCloud or another Apple device. iTunes is also

a backup tool. The backup can be used to restore the files to the backup iPhone or to another iPhone, maybe a new one. For this, it must not be the same type. A backup from an iPhone 7 e. g. can be recovered to an iPhone X. This is my experience done several times in the last years to bring all my data from an old iPhone to a newer one. That had not worked every time at once. Sometimes some error codes occurred and the procedure had to be restarted. Mostly it was a problem with the USB-port or the iPhone cable.

A backup with iTunes can be done into two different ways irrespective of where the backup will be stored. The difference between the two ways is to save the backup with or without a passcode. My first meaning was that the only difference is to make the backup safer from abuse. On iTunes, there was no explanation for this point. For forensic work, there is a very big difference between these two ways, because only the option with passcode contains the saved passwords, Wi-Fi settings, website history and health data from the phone. This information has been found at the Apple support pages on the internet (Apple.com, 2018).

Knowing this it makes sense to perform an encrypted backup with a passcode when using iTunes.

The backup files are stored in container e.g. under following paths:

Windows 7 -10:
C:\User\Username\AppData\Roaming\AppleComputer\MobileSync\Backup

Mac (Macintosh Computer with Yellowstone):
/Users/Username/Library/Application Support/MobileSync/Backup

4.2.3 Phone Paw 5.8.0

FonePaw is a program which primarily advertises data restoring by accidentally deleted data or system recovery without data loss. For this, it has functions for backup an iPhone or data in the ICloud. It also can be used to open and restore data from iTunes backups.

The functionality is limited to:
Media

- Records
- Photo stream
- Photo Gallery
- App Photos
- App Videos
- App Audio

Message and Contacts

- Message

- Message Attachments
- Contacts
- Call Running
- Voice Message
- WhatsApp
- WhatsApp Attachments

Memos and others

- Notes
- Calender Reminders
- Voice Memos
- Safari Bookmarks
- Safari History
- App Documents

There is not a function to backup other apps or files. Deleted files from these categories are also extracted and displayed as deleted. Deleted files can be restored in the same way like not deleted files.

4.2.4 Forensic programs

Three commercial programs were used to perform backups or physical copies from the iPhones. UFED, XRY and iOS Forensic Toolkit are completely forensic programs and had a separate tool that worked only for acquisition.

4.2.4.1 **UFED Physical Analyser** (Cellebrite)

UFED Physical Analyser is a forensic product from Cellebrite[1] for mobile devices. It is a licensed Software product that runs on Windows machines. iPhones can be extracted in two ways. For iPhones 2G until 4 with a physical modus and Advanced Logical Extraction are available. Advanced Logical Extraction in UFED combines logical and file system extraction to one extraction modus (Cellebrite, 2019).
Only with the jailbroken iPhone 4 a physical backup could be perform successfully. This physical backup was only done to know that the experimental environment works as it should.
A test if a jailbroken iPhone 5, 7 and X can perform a physical backup was not possible. Starting the Physical Mode the iPhone had to be restarted to change into the DFU-Mode. That makes no sense because from a restart the tethered jailbreak did not work anymore. And there was no

[1] `https://www.cellebrite.com`

way to activate the jailbreak in DFU-Mode.

Starting the Advance Logical acquisition the name, UDID and the iOS-version have been displayed. It was recognized that the iTunes backup was set before to be encrypted and pointed out to contact Cellebrite that can handle this if the passcode is unknown.

Two methods could have been selected. Method 1 wanted to extract call history, SMS, MMS, app data, data files and notes. Therefore the backup had to be encrypted with a passcode as known from iTunes backup.
Method 2 could be have been used to perform a limited extraction of the data, including data files and locations.
One goal to jailbreak an iPhone for acquisition is to get as most data as possible. This cause the interest is to perform method 1.
With his method, an iPhone 5S, 7 and X were acquired. UFED has not given a hint that the acquired iPhones have been jailbroken. Even in the extraction report was no indication that the iPhones were jailbroken.

To have a look if the jailbroken devices have more data extracted than the non-jailbroken devices the extraction results were viewed. A comparison of the data provides no difference. An acquisition from a jailbroken iPhone must have as result in more data because all data from the system partition will be additionally included.
Looking for a reason there was a hint found in a Cellebrite user forum that AFC or AFC2 had to be installed to get full access to the jailbroken device over USB.
After AFC2 was installed, UFED offered a third way for acquisition, as shown in Figure 4.2.

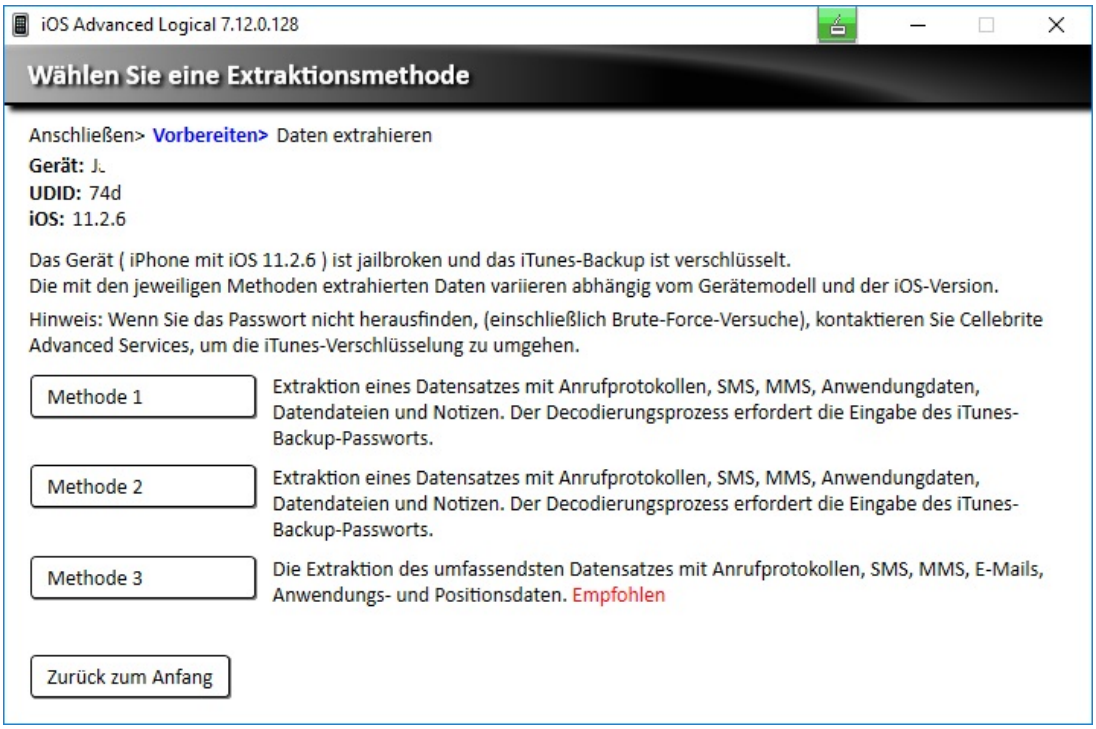

Figure 4.2: UFED with 3. extraction method, only available for jailbroken iPhones

Obviously UFED has recognized that the connected iPhone was jailbroken. The third acquisition method says to give to extract comprehensive records from call history, MMS, SMS, application data, e-mails and position data. The main differences are that there will be extracted comprehensive data sets, e-mails and position data from a jailbroken device.
The iPhones 7 (iOS 11.2.6) and X (iOS 12.1.2) were know acquired again using the 1. and 3. method.

4.2.4.2 **XRY** (Micro Systemation)

XRY is a forensic product from Micro Systemation Aktiebolag (MSAB)[2] for mobile devices. The MSAB Office version XRY 7.9.1 was used that is a licensed Software product running on Windows machines.

After the same iPhones that were used with UFED were connected to the USB-port from the Windows machine, XRY had automatically recognized all used iPhones types. If this would not have worked a manual selection was also possible. iPhones with same types have different versions that could be manually set. That may be for example be an iPhone 7 with an older and newer hardware version. There are also different hardware types sold in Japan and China. The Model-Information can be found on the iPhone under Settings-General-About.

XRY will show all to the PC connected devices, even when more are connected. XRY is able to acquire until 4 devices at once.
After selecting and confirmation the iPhone the extractions starts. During the extraction, a report is displayed that shows the working steps. One step is to prove if the connected iPhone is jailbroken. XRY had not recognized that the tested devices have been jailbroken. After the backup was completed the Apple iTunes backup password has been asked when the backup decryption has been activated.
All extractions were performed successfully.
As XRY had not recognized that the iPhones have been jailbroken, the same problem occurred that I had before with the UFED acquisition.
To fix this problem with UFED I have installed AFC2 with Cydia to the tested devices. This fixed also the problem with XRY. XRY now recognized that the acquired iPhones 7 (iOS 11.2.6) and X (iOS 12.1.2) have been jailbroken and displayed this in the working report.

4.2.4.3 **iOS Forensic Toolkit** (Elcomsoft)

iOS Forensic Toolkit is a forensic program from Elcomsoft[3] that uses the command line with a graphical GUI. After starting the program it recognized the connected iPhone and displayed the model, serial number, iOS-version, and the device-ID. Using specified letters different ways of logical and physical methods of acquisition could have been selected. Using letter ”B” the logical acquisition a backup in i-Tunes-style has been performed. Using other letters device information, copying media files, shared files from installed apps and crash logs could be selected.

[2] `https://www.msab.com/`
[3] `https://www.elcomsoft.com/`

For physical acquisition the files system have been acquired when letter ”F” was selected. With letter ”D” the screen lock could been disabled and with ”K” the keychain has been decrypted, as shown in Figure 4.3.

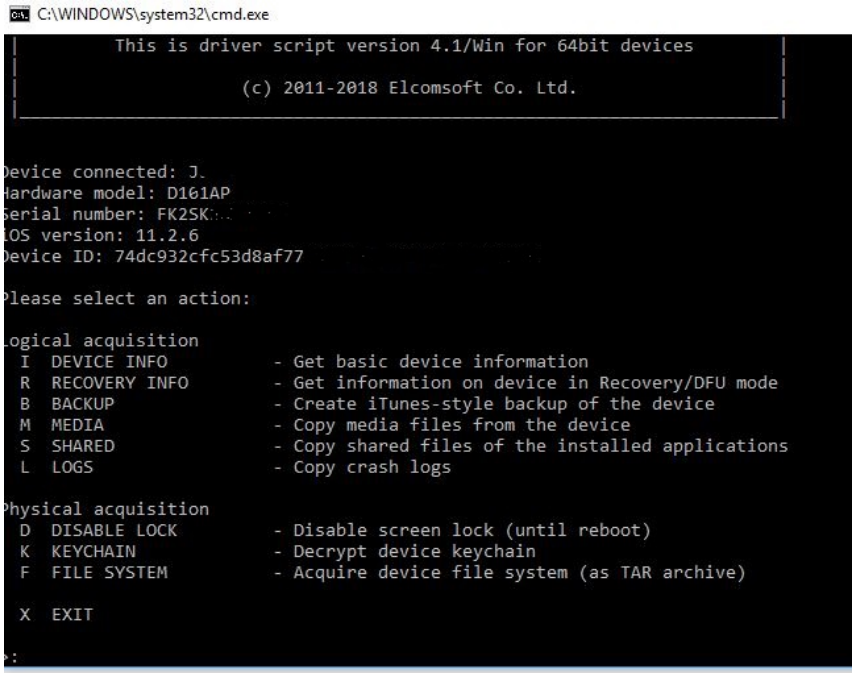

Figure 4.3: Startmenu iOS Forensic Toolkit

After starting the physical acquisition with ”F” the file can be named and the root password will be asked before the acquisition really started. During the acquisition the size of the acquired image was displayed. To finish the acquisition e.g. with iPhone 7 and X that had both 32 GB internal space each took less than 1 hour. As a result, a compressed tar archive has been stored into the application directory that includes all files and directories that have been acquired from the data storage of the acquired iPhone. The content, as shown in Figure 4.4,can be viewed for e.g. with 7-zip.

F:\Elcomsoft\iOS-Toolkit-4.10-Win\iOS-Toolkit-4.1-Win\iPhoneX.tar\

Name	Size	Packed Size	Modified
.	0	0	2019-05-14 12:20
.fseventsd	111 899	116 224	2019-05-14 12:20
.mb	0	0	2017-09-30 05:28
Applications	108 452 102	110 838 272	2019-02-07 10:28
bin	6 155 689	6 169 600	2019-05-14 13:31
boot	0	0	2018-06-10 10:51
cores	0	0	2016-07-28 00:23
dev	0	0	2019-05-14 09:46
Developer	0	0	2016-07-27 20:23
jb	2 430	2 560	2019-05-14 12:19
lib	0	0	2018-06-10 10:52
Library	103 512 863	104 141 824	2019-05-13 15:31
mnt	0	0	2018-06-10 10:52
Network	565 132	580 096	2019-03-01 03:11
private	21 475 115 327	21 520 513 024	2016-10-12 07:56
sbin	1 110 081	1 113 600	2019-05-14 12:20
System	3 789 282 792	3 816 050 688	2016-12-21 01:02
usr	581 569 077	582 077 440	2019-05-14 12:20
.bit_of_fun	0	0	2019-02-07 09:25
.cydia_no_stash	0	0	2018-11-07 18:03
.file	0	0	2016-07-28 00:23
.installed_unc0ver	12	512	2019-05-14 12:20
ent	252	512	2019-02-13 11:32
etc	11	0	2016-09-21 12:05
tmp	15	0	2016-09-21 12:05
User	11	0	2019-05-14 12:20
var	11	0	2016-09-21 12:05

Figure 4.4: Content of the tar archive created with iOS Forensic Toolkit

The physical acquisition with this tool has acquired the whole file system from all tested jailbroken iPhones including iPhone X Starting the physical backup the ”pairing.plist” and ”keychaindump.xml” have been stored first to the acquiring machine. After the backup was completely the iOS Forensic Toolkit has decrypted the data partition using the encryption key that was extracted with the data from the keychaindump.

Apples Secure enclave was introduced with devices that had the A7 chip architecture. Apples Secure Enclave is a hardware part in the iPhone architecture that works like an own computer to prevent access to biometric data like face-ID, fingerprints and also to the stored password. Apples Secure Enclave has been also bypassed only with iOS Forensic Toolkit.

4.3 Searching for changes through the jailbreak

To find out if files from the data partition have been changed in connection to the jailbreak the Forensic Toolkit was used. First step used only files that have been extracted with XRY and UFED before the iPhone has been jailbroken to compare these files with those that will be extracted after the jailbreak. To get only the files that have been extracted in all cases they were filtered in a way that only files that are double with the same name are shown. The reason was that only the files that were extracted before the jailbreak was done could be compared to the

jailbroken device. For the next step, only the files were needed that have been extracted with all used methods twice. In the next step, the logical files were hashed that were saved from the iPhone 7 (iOS 11.2.6) and X (iOS 12.1.2) with XRY and UFED before and after jailbreaking the device with the MD5 logarithms. In the next step were selected that files with the same MD5 hash were not displayed. In this way only files that were changed after the jailbreak was displayed, if changes have happened.

The files from the system partition haven t been reachable for me before the jailbreak was installed. Cause this, another way was searched find out what changes have happened through the jailbreak to the files from the system partition. For this, the files were sorted with the ”last changed” attributes by timeline.

4.4 Results

Jailbreaking all in the experiment used iPhones were possible to all used iPhones. All jailbroken devices have worked without any problems. That means that not one device worked unstably, was freezing or something else that could happen after jailbreaking. Sometimes a part from the jailbreaking procedure had to be repeated until the jailbreak worked. That may also be an issue to an iPhone 7 that had more often this problem than the other devices and the procedure had to be repeated several times.
There were mostly two ways to perform the jailbreak to the newer devices that had iOS 10 and up. One way was to use the Cydia Impactor, the other using safari. When these two ways were available, both worked. To use Safari, the iPhone must be connected during the download to the internet. Using an impactor, the iPhone and the PC that executes the impactor needed only a connection to start the jailbreak. Only the jailbreak with Cydia Impactor needed a simple Apple account with and the matching passcode for this account. A developer account could also be used but was not needed during the experiment.
Since the first iOS until today every iOS version number from 1 to 12 had at least one version that could be jailbroken.
Nearly all versions of iOS 11 could be jailbroken with Electra and unc0ver that uses the same exploits as Electra but should provide more stability and features. Only for iPhone X the version 11.0, 11.02. and 11.03 could not be jailbroken. For iOS 11 versions Electra and Unc0ver were tested, that included a jailbreak with an own way for de-installation.
iOS 12 until 12.1.2 can also be jailbroken with unc0ver working for iPhones 6s to X. Using unc0ver an iPhone X with iOS 12.1.2 has been jailbroken without any problems. Starting the uncOver jailbreak offered some more options that could be selected including the deinstallation from the jailbreak (John, A., 2019). Here the default settings were used that also had installed Cydia.

FilzaJailed was something special because it has been installed in the same way as a jailbreak using a security breach. FilzaJailed only worked on devices with iOS 10, 11.0 11.2.1 and 11.3. 11.3.4. and should now work also with iOS 12 12.1.2. The installation worked with the Cydia impactor or by visiting the homepage from FilzaJailed. With FilzaJailed all files could be browsed and accessed, including the system files and the root directory. Files could be copied, pasted and send them with on the iPhone available mail or chat programs to another device.

With FilzaJailed there was no option to connect to a seizing computer and to copy data right there. FilzaJailed was installed in the Application directory and not in the root directory where the jailbreaks have been stored.

To acquire the devices before and after the jailbreak different tools were used.
iTunes and command line is free. PhonePaw is available in the smallest home version from 30 € up. XRY, UFED and iOS Forensic Toolkit are much more expensive tools for professional use.

With the command line, a physical backup could be performed with an iPhone 4 including both partitions with their physical content. With this physical image deleted files could have been recovered from on both partitions. The used commands worked in the same way with an iPhone 5 and iOS 9.3.3, but the data partition was encrypted. This means that without decryption there was no viable data from that partition.
From the devices with iOS 10 and higher, a physical backup could not be performed in such a way. Even as root, searching to run these commands gives the output that it was denied. It may be a restriction in connection to the new file system APFS or a hardware restriction.
The only way that worked to get all stored data from the jailbroken iPhone with iOS 10 and higher without a forensic program was to copy all directories with their content. One way to do this was by using OpenSSH and command line. With the command line, the contents could be copied also to a compressed image. This prevents the data from being changed after the copy. Another used method was to install AFC2 with Cydia to a jailbroken iPhone. The iPhone could now be connected over the USB-port for using with e.g. iDevice Manager (iPhone Explorer) to a Windows-PC. With this program, the content from both partitions can be viewed as one directory tree including the root directory, shown in Figure 4.5. With iDevice Manager, all logical content could have been copied to the examination PC.

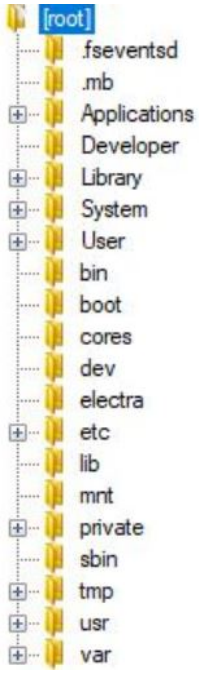

Figure 4.5: Overview from the root directory with iDevice Manager, after AFC2 was installed to the jailbroken iPhones

Using iTunes and PhonePaw has only extracted from these tools supported data. That means that all other data that might be on such a data storage from an iPhone will not be saved in any way.
There was a difference when using iTunes or PhonePaw between a backup with a decryption key and one without. When saving a decrypted backup, more data is saved from the iPhone. The next data and settings will only be saved if the iTunes backup was performed using the ”Encrypt iPhone Backup” method on iCloud or on the PC:

- Deposited passwords from Safari and other Apps
- Health data from the health App
- WiFi settings
- Website history from Safari

The extracted data with PhonePaw uses the same way as iTunes and is able to extract data from iTunes backups too. PhonePaw is able to show and restore deleted files. One reason is that databases do not delete data immediately, rather mark them as deleted. As a result, the data remains in the database but the user has no longer access. Even with pictures and videos on an iPhone that was moved to the other folder before they were finally deleted. However, they can be found in this folders and also be restored by the user through the Photos app in the ”Recently Deleted” folder. Only when they are deleted from this folder, they are deleted with the decryption key. There is no way after this point to restore or recover these files.
It depends on the iOS-version and app settings if deleted data or files have been moved, marked as deleted or have been deleted indeed. Using iTunes and PhonePaw to backup an iPhone there was no difference found between a jailbroken and a non-jailbroken device comparing the data content.
With the forensic programs XRY and UFED, a full physical backup could not be performed with devices starting with iPhone 4S and newer. With older devices, until the iPhone 4, there were ways to perform a physical backup from the whole data storage, including both partitions. Using an iPhone 5S with iOS 9.3.3, physical backup from the whole data storage could be performed using the command line with a Mac or a Linux distribution. As expected system partition was not encrypted but the data partition was encrypted. That means that only the system partition was physically imaged in a useful way. The encrypted data-partition only could be used after decryption. Doing this, only the logical files will be decrypted. Other deleted files could only be restored with their own decryption key. But these keys were deleted at the moment, the file was deleted. At least the content from the physical backup of the decrypted data-partition is the same that a logical backup has.

XRY and Cellebrite have first not recognized any of all tested iPhones as jailbroken. The reason was that both forensic programs need that an AFC or AFC2 program was installed on the iPhone to get access to the data storage using USB-connection. Access over OpenSSH was not supported by these programs. This is not mentioned and can result that it may not be noticed when a jailbroken device backup was performed using one of these programs. That means to be sure if the iPhone is jailbroken or not it must be investigated manually. After installing AFC or AFC2, what is depending on the used iOS, XRY and UFED detected that the two again tested

iPhones were jailbroken.
During the extraction, XRY was listing the performed extraction points. One of the shown extraction points has been the device state. The difference from a non-jailbroken to a jailbroken device with installed AFC2 was here that the device status now was shown as jailbroken.

After AFC2 was installed to the iPhones UFED opened a third extraction method that was not available before. When UFED shows 3 extraction methods it has obviously recognized that the connected iPhone was jailbroken.
Elcomsoft iOS Forensic Toolkit was the only tool that was able to perform physical backups from both partitions of all tested iPhones, including iPhone X with iOS 12.1.2 and to decrypt the data partition. The tool uses, therefore, the encryption key, that is stored on the not encrypted system partition. The main difference between a jailbroken and non-jailbroken iPhone from the forensic side is the access to the system partition. Using XRY, UFED, iOS Forensic Toolkit, and Command-Line both partition could be accessed and data extracted.

A jailbroken iPhone will give access to the whole data structure to an iPhone including the root directory. A Snapshot to the content from a jailbroken iPhone 5 (iOS 9.3.3) shows the system partition that could be backed up physical using the command line. The result from such a physical acquisition contains the system partition and the encrypted data partition. Having a look at the image with an e.g. X-Ways Forensics to see the content will only detect the system partition. Opening the system partition will show the content, as shown in Figure 4.6.

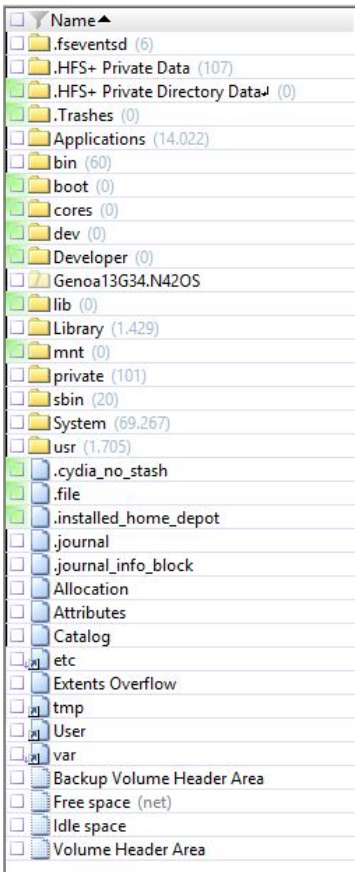

Figure 4.6: Overview from the system partition at the root directory to the acquired image from an iPhone 5 (iOS 9.3.3) with X-Ways Forensics

Connecting to the iPhone without an active jailbreak gives only access to the data partition over the USB-Port. Having a look at the data structure the data partition can be found under the path /private/var. Using XRY and UFED had the advantage that the files have been extracted after the acquisition. This opened a way to have a fast look at the different contents between a jailbroken and non-jailbroken device. In all types of classes, there have been multiple files more extracted. This overview comes from XRY and shows two extraction results from an iPhone X (iOS 12.1.2) before and after the jailbreak, in Figure 4.7 and in Figure 4.8.

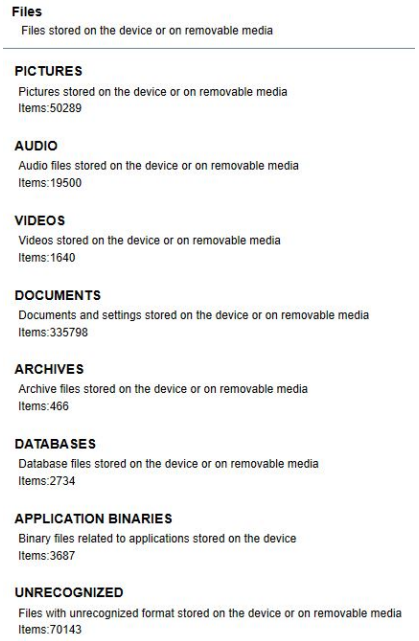

Figure 4.7: Overview number of extracted files with XRY after jailbreaking the iPhone X

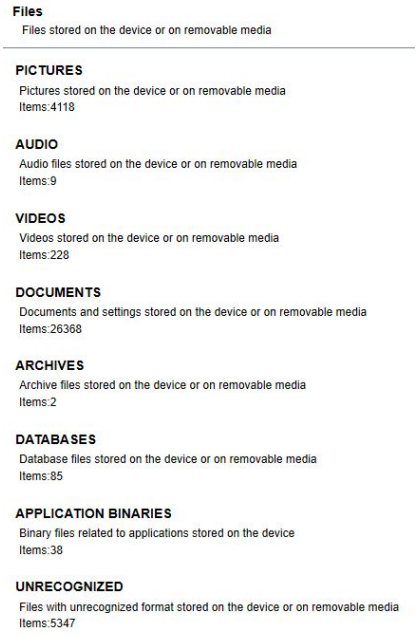

Figure 4.8: Overview number of extracted files with XRY before jailbreaking the iPhone X

Before jailbreaking 4.118 pictures, 9 Audios, 228 Videos, 26368 Documents, 2 Archives, 85 Databases, 38 application binaries, and 5348 unknown files have been extracted.
After jailbreaking 50289 pictures, 19500 Audios, 1640 Videos, 335798 Documents, 2 Archives, 2734 Databases, 3687 application binaries, and 701434 unknown files have been extracted.

The extraction results with UFED have shown the same effect. Even with UFED, the extraction from the jailbroken iPhones had, as a result, a lot of more extracted files after the iPhones were jailbroken. The results also depending on the individual content from the seized iPhones. All with UFED and XRY additional extracted files must come from the system partition. This is the reason why further listing the numbers of extracted files that were extracted more after jailbreaking will not contribute to answering the research question.
A physical backup from system partition opened access to all files that are stored there, regardless of their protection class. E.g. decrypting all keychain items can only be done with a physical acquisition from the system partition. Other files stored on the system partition like hidden files or app data may also not be copied using the logical extraction from the system partition.
At least the iPhones 7 (iOS 11.2.6) and X (iOS 12.1.2) were used to compare the data before and after the jailbreak was performed. But this time to have a look if jailbreaking has altered data in an inadmissible way for forensic work?

FTK and X-Ways Forensic were used to do this. First, only files were compared that have been extracted from the non-jailbroken and jailbroken devices too. See only the files that have been changed all files that have been double with the same MD5-hash were hidden. The idea was that only files that were changed after the jailbreak was shown. The result was that not one file was displayed. This method was not usable for the system partition, because this partition was only accessible after the jailbreak was performed.

The idea to have a look to the timestamps turned out to be unfit because the system is not frozen after the jailbreak. That means that a lot of files have been changed after the jailbreak. But jailbreaking without changing the system partition is not possible. Having a look to a jailbroken system partition at the root level will show that there is a folder with files that belong to the jailbreak. E. g. the Electra jailbreak will be found in the folder named electra like the jailbreak is named. Cydia was installed in the application folder.
The result is the same as known with jailbreaks and physical acquisition with an iPhone 4 and before. The only changes that occurred when jailbreaking the iPhones were changes to the system partition. As well it could be verified, no changes to files were found that may have contained evidence data.

Chapter 5

Discussion

This chapter the research question and sub-questions will be discussed.

Research Question:

Can jailbreaking be used as a technique to create reliable, verifiable and forensically sound images from an iPhone to provide evidence robust enough to be valid in a court proceeding?

To answer the research question the following sub-questions have been answered.

Question 1:

Can all iPhones be jailbroken in a way that will open methods for forensic acquisition?

The use of methods like exploits and jailbreaks are not new in forensic acquisitions. Acquiring iPhones were done with different techniques like jailbreaking in the past. Some of these techniques with forensic products like UFED have used exploits to get escalated privileges to an iPhone, bypassing or e.g brute forcing (Chapter 2.1.6) the device.
During the literature research, there was only some paper found that dealt with jailbreaking as a forensic technique for acquisition. Jailbreaks and acquisitions were done with older devices like iPhone 4 to perform a physical backup. There was no information that dealt with newer devices like iPhone 7 and higher with iOS 10 a higher with iOS 10 and up were jailbroken for forensic acquisitions. Only webpages from providers of forensic tools for iPhone acquisition were found with descriptions from jailbroken iPhones until iPhone X up to iOS 12 more data could be extracted using these tools.

Before handling with evidence in such a way a backup from the iPhones with the in Chapter 4.2 listed tools was done. Only using command line there was no option to backup the devices

before jailbreaking.

During the experimental time all in Chapter 4.1 listed iPhones could have been jailbroken with different jailbreaks. To jailbreak iPhones that had installed iOS-versions 10 until 12 with Cydia Impactor, an internet connection and the Apple account was required. The reason behind that was using this tool the jailbreak only could be installed when the Apple account and password has been verified to an existing account with matching password from the apple server. There is no need to use the account from last user as feared before the experiment. It works with an account that was created only for the experiments and should work with any other existing account in combination to the matching password.

Even when additional programs must be installed it is required to connect the iPhone during this time to the internet.
From point of forensic view an internet connection is risky, because the last owner who may be an offender could connect to the ”iCloud” and lock or delete the iPhone when the services ”Find My iPhone” was activated on this device.

Another problem occurred, because iPhones searched for updates during the connection to the internet. In one case it was asked to update an iPhone to a higher iOS version. After denying the update the passcode has been asked. Entering the passcode started the update and could not be stopped any more. The iOS was updated to 12.1.3. The reason was the passcode has been asked for the update that had to be denied again at the bottom from the display without entering the passcode.
The update to iOS 12.1.3 could not be jailbroken during the experiment, because there was no jailbreak available for this iOS-version.

From the forensic point of view, there is the approach not to change a piece of evidence more than it is required for the forensic work.

Some jailbreaks had not installed Cydia by default. Therefore Cydia had to be installed in a second step using the Cydia App Store.

Other jailbreaks were available but not able to install Cydia or additional needed programs. These jailbreaks have been unusable for any acquisition.

To use jailbreaking for an acquisition of a connection between the iPhone and the acquisition computer is required. One option is using a network connection with a WLAN environment to connect the iPhone. If the jailbreak has not installed a program like OpenSSH, it had to be installed using Cydia. Such a connection was required to connect from the command line (Windows) or terminal (Mac) to a jailbroken iPhone.

Software like Phone Paw, UFED Physical Analyser, XRY and iDevice Manager are using the USB-port to connect to the iPhones.

Searching for jailbreaks, another way to get access to the system files up to the root directory was found, offered by the program FilzaJailed. The program has been installed in the same way like a jailbreak but pretends not to be a jailbreak even as it uses an exploit to be installed into

the application folder and not into the root directory where all other tested jailbreaks have been installed. After installing and running FilzaJailed browsing through all directories including the root directory has been possible. Even writing and deleting files was successful. The only way to acquire files was copy and paste and sending with a communication tool that has already been installed. This was limited by file size from the already installed programs. Besides, it was very laborious to copy and paste file for file.

To perform the acquisitions different tools have been used. First tested tools which have been the command line on a Windows machine and terminal on a Mac computer. There was no method found for acquisition before the device has been jailbroken. The iPhones were connected using their WLAN on a Fritz router.
Once jailbroken a physical acquisition to an iPhone 4 (iOS 7.1) was done to test if the used environment worked. The data storage was saved successful as an image to the acquisition computer. Opening the image showed the completely physically content with both partitions.

Following devices iPhone 4S (iOS 6.1.2) and 5 (iOS 9.3.3) has been used for acquisition. The data storages had been stored successfully as an image to the acquisition computer. Opening the images with X-Way Forensics showed only the HFS+ system partition, cause the data partition was encrypted. To get non-encrypted content from the data partition, the files have been copied logical to a compressed image.

Taking this way took several attempts, because the started acquisition was canceled unexpectedly due to the different transfer sizes. To fix this problem the Auto-Lock from the iPhone and the auto network interruption from the router were deactivated. After changing these settings the acquisitions were saved completely. The acquisition transferred less than 1 GB/1 h.

All other in Chapter 4.1 listed devices that were iPhone 7 and X, a physical acquisition could not be started with the command line or terminal window. Searching to run this command gave the output it is denied.

PhonePaw and iTunes had no optional methods for backups with jailbroken iPhones.

UFED and XRY first had not recognized that the acquired iPhones 5S, 7 and X have been jailbroken. Both forensic tools supported advanced acquisitions from jailbbroken iPhones. Searching for a reason why these tools have not recognized the jailbreaks, there was a hint found in Cellebrite-User-Forum that AFC or AFC2 had to be installed to get full access to the jailbroken device over USB. After AFC2 was installed UFED and XRYs had recognized the jailbreaks and acquired the iPhones in an advanced way.

Elcomsoft iOS Forensic Toolkit was the only tool that performed a physical backup from all tested iPhones. But as described from Elcomsoft the content has been decrypted with the decryption keys that were stored in the keychain-file. From keychain only decryption keys from existing files could be extracted. As a result the content from the data partition is the same like it was done with a logical copy. Physical backup from the system partition opened access to all files which are stored there, regardless of their protection class. Elcomsoft iOS Forensic Toolkit has been able to bypass Apples Secure Enclave and extracted biometrically and stored passwords.

Summarized, the question can be answered as follows. Not all iPhones could be jailbroken, because there are no jailbreaks for all version of devices and/or iOS-versions available. Even when jailbreaks are available, they can only be used when they offer a way to connect to the iPhone with root privileges or give another method to acquire the data storage.

Question 2:
How will jailbreak influence the result from the acquisition in perspective to the content of saved data?

Answering this question different tools are listed in Chapter 4.2 were used for acquisition.

First tool was the command line (Windows) and Terminal (Mac). Without a jailbreak I was not able to acquire any of the iPhones. After jailbreaking the devices, these iPhones have been connected via WLAN to same network that was used by the acquiring computer. The acquiring computer was now able to connect to the devices with root privileges. Now root password had to be entered, that is ”alpine” when default settings weren't changed. To acquire all at Chapter 4.1 listed devices have been used. First method was to use the command ”dd” that should create a physical copy from the data storage of the connected iPhones. As expected and known from the literature research the iPhone 4 could have been imaged this way. That means that both partitions and their content were physically available. The same result was also performed with iPhone 4S and 5. After the acquisition only the system partition could be analyzed, because the data partition was encrypted. The only way to acquire the contents from an encrypted partition was to copy these files. The copy-command started with additional parameter that copied the files in a compressed folder to avoid changes after the acquisition was finished. After the image was finished, the image-files was hashed using the MD5-logarithm. With this ”fingerprint” from the image file can be chekced whether the file has been unchanged. Using the iPhone 7 and X (iOS 11 and higher) this acquisition method could not be performed. Searching to acquire physically leaved to the output that this is denied.

The acquisitions with iTunes and Phone Paw had not leaved to any differences between the contents of the jailbroken and the non-jailbroken devices. There were no additional files extracted after jailbreaking.

Using the forensic tools UFED, XRY and Elcomsoft forensic Toolkit for the experimental phase would be expensive. For all three tools licences were needed that cost thousands of €. Fortunately, there was a way to use UFED and XRY without spending money for it, otherwise this part wouldn't have been possible. Elcomsoft provided a 2 weeks limited version where only a dongle had to be paid.

Acquisitions from jailbroken iPhones 7 and X with UFED and XRY expectantly lead to the same result as before without a jailbreak. Exactly the same number of files have been extracted with jailbroken and non-jailbroken iPhones. The jailbreak should give also access to the system

partition. Because system files should have been extracted additional. First notice was that all devices haven't been recognized as jailbroken. In Cellebrites user forum was told that installing AFC or AFC2 should fix this problem. For iPhones 7 and newer AFC2 should be installed. After AFC2 was installed with Cydia all devices have been recognized as jailbroken. During the second acquisition, UFED opened a third acquisition method. Both forensic tools acquired and extracted a significantly higher number of files than before with the non-jailbroken iPhones.

iOS Forensic Toolkit had performed logical acquisitions in iTunes style and also physical acquisitions from all jailbroken iPhones within this experiment. The physical acquisitions included encrypted data partitions. Staring the physical backup the pairing.plist and keychaindump.xml have been stored before to the acquisition computer. After completing the acquisition the data-partition was decrypted by the encryption key from the keychaindump.xml. Only files which havent been finally erased were decrypted. As a result, the content from the decrypted data partition contains the same content as a logical acquisition.
iOS Forensic Toolkit was the only tool during this experiment that was able to bypass Apples Secure Enclave where biometric data like face-id, fingerprints and passwords were stored.

To answer this question the results between the used acquisition tools have been different. But the results were not depending on the jailbreaks that were used in the experiment. The used jailbreaks gave all root permission and have installed Cydia. OpenSSH was mostly installed by default during the jailbreak installation. With OpenSSH or software which operates in the same way iPhones could be connected as root using the same network. For acquisitions using the USB-port, AFC had to be installed with Cydia to acquire an iPhone with root permission. Depending on the used acquisition tools, after jailbreaking the data storage could be acquired physical to all whithin the experiment used iPhones up to iOS 12.1.2.

Question 3:

Will more extracted files have information that can be evidence in a case?

Evidence can be all data that is able to give information to the case. After jailbreaking much more files have been extracted as shown in the results (Chapter 4.2). Additional files have been e.g. databases, audio-files, pictures, videos, documents, biometric data and passwords. These files could contain information may be used as evidence to a case.

Question 4:

Are the results valid and reliable for court proceeding?

To proof the validity different iPhones types with different iOS-version were acquired before and after the iPhones were jailbroken. The best way would have been to perform all steps before and after jailbreaking the device a second time. In this case the results had to be identical if

there were no other impacts. To do this an iPhone need to be reset in the same condition before jailbreaking. But even when Electra and evasi0n jailbreaks were able to be deinstalled they will leave traces. Installing a new iOS to an iPhone is restricted by Apple. Only one for the selected devices from Apple-authorized iOS-versions can be installed. These are the reasons why there was no method found to proof this step during this experiment. This limitation will make it more difficult to recap the experiment in the same way for others.

After jailbreaking the whole content from the data storage have been accessed with the command line, iDevice Manager, WinSCP, UFED, XRY and iOS Forensic Toolkit. A physical acquisition from iPhones that have been newer than iPhone 4 was possible up to iOS 9.3.3. But contentwise only the system partition could be used, because the data partition was encrypted and had to be decrypted for further analysis.

The validity and reliability were proofed with different tools and showed that used jailbreaks have given access to both partitions from the data storage of all tested iPhones.

Question 5:
Can jailbreaking an iPhone for acquisition be a forensically sound method?

A jailbreak is an intervention into the system partition of an iPhone. Forensic work wants to change digital traces as little as possible. But sometimes things have to be changed, damaged or even destroyed to get the required information. Each handling with the data can have real impact on legal proceedings. It is essential to handle digital evidence as every other physical evidence and maintain a clear, documented chain of custody. In compliance with these rules, a change of data can be a forensical sound method, but changes need explanations. Having forensic soundness it must be declared why and what has been changed. Therefore it is important that the installation from the jailbreak has not altered evidence files.

To be sure that jailbreaking has not altered data in an inadmissible way the acquired files from an iPhone 7 and an iPhone X were used. Files acquired before jailbreaking were compared to the files that have been acquired after a jailbreak was installed. FTK and X-Ways Forensics were used for further analysis. Only files that have been found in both acquisitions were compared. To find out if files have been changed the setting was used that all files with the same MD5-hash were hidden. No files have been displayed that were changed.
Comparing the system partition was not possible, because there was no access to this partition before jailbreaking the iPhones. It is unreasonable that the jailbreak has changed the system partition, but there were no hints that this has changed files that could contain evidence data.

Chapter 6

Conclusion and Further Work

6.1 Conclusion

In this chapter will be tried to answer the research question that is mentioned in Chapter 1.5 and discuss if the goal of this project has been reached.

The answer is based on literature research (Chapter 2), experimental work (Chapter 4) and discussion of the results in Chapter 5.

6.1.1 Research Questions and Subquestions

This master thesis is based on a single research question:

Research Question:

Can jailbreaking be used as a technique to create reliable, verifiable and forensically sound images from an iPhone to provide evidence robust enough to be valid in a court proceeding?

The provided results and information should enable interested readers to get an idea of how a jailbreak can be used as a forensic technique for forensic acquisition. The used literature research and experimental work focused on current devices and iOS-versions that could be jailbroken until writing time, 17.05.2019. But also aspects that have relevance for forensic work have been considered here.

During the literature research, no paper was found that concerned with forensic acquisition from current iPhones and iOS-versions. Certainly not under consideration to create reliable, verifiable and forensically sound images.

Forensic investigators worldwide have to acquire iPhones to get answers to different cases. In law enforcement the acquired information can be used to solve criminal acts. iPhones protect data in a way that makes it more difficult to get access to all stored information. But a single

information can be the reason why serious crimes can be solved or not. That can be e.g. GPS-data that tells where somebody has been, with time-stamps telling about the time the crime has happened. Stored passwords, passcodes, biometric data and other information could give access to e-mail accounts, iCloud and other places where additional data is stored.

In forensic science, a lot of methods were developed that are used in the daily work to secure physical and digital traces.

Acquiring an iPhone a forensic investigator will come to his limits when he wants to get data from the system partition, key-chain or Secure Enclave. There were no Open Source Tools to acquire an iPhone without a jailbreak. Even expensive forensic tools cannot help to come over that limitation. But it is known from the documentation to the forensic tools e.g. XRY, UFED and especially iOS Forensic Toolkit, that files stored on the system partition only can be extracted when a jailbroken iPhone has been acquired. This refers to iPhones that have already been jailbroken when they were secured.
But can a seized iPhone be jailbroken as a method for forensic work? To answer this question in a way that gives valid answers for forensic work, the research question has been formulated. To answer the research question five sub-questions have been answered.

Subquestion 1:

Can all iPhones be jailbroken in a way that will open methods for forensic acquisition?

Not all today available iPhones can be jailbroken, because there are not jailbreaks for all iPhones available. Even when a jailbreak is available it can only used as method for forensic acquisition when additional programs like OpenSSH or AFC2 can be installed with the used jailbreak. Focusing to iPhones 7 until X, nearly all versions of iOS 11 and 12 until 12.1.2 can be jailbroken. Three different jailbreaks were available to jailbreak iOS 11. Electra has been tested to jailbreak iPhones with iOiOSS 11.0.1, 11.2.6 and 11.3.3. and unc0ver for iOS 12.1.2. LiberiOS has not been tested because only iPhones with iOS 11.0 until 11.1.2 could be jailbroken with this tool. Independently from the used iPhone or installed iOS can be said that a jailbroken iPhone offered additional methods for acquisition when also needed additional programs have been installed.

Subquestion 2:

How will jailbreak influence the result from the acquisition in perspective to the content of saved data?

A jailbreak gives access to the data storage from an iPhone with escalated privileges. This lead to the result that data partition and also all files stored in the system partition could be acquired, that was not possible before.
Elcomsoft iOS Forensic Toolkit additional enables bypassing Apples Secure Enclave and extracted biometric and stored passwords from jailbroken iPhones. It is not clear how that worked,

because Apples Secure Enclave is something like a separate mini computer Apples had integrated in the hardware to an iPhone that had A7 chip architecture to prevent access to there stored biometric data like face-ID, fingerprints and passwords. The data stored in Apples Secure Enclave was not accessible with any other used tool. It seems that Elcomsoft iOS Forensic Toolkit work with an additional exploit.

Subquestion 3:

Will more extracted files have information that can be evidence in a case?

After jailbreaking, a lot of files have been extracted containing information that is able to give information to the case. The additional files have been e.g. databases, audio-files, pictures, videos, documents, biometric data and passwords. These are information that according to experience can solve a case or will help to do this. The extracted passwords can also open ways to get information that are stored on other places, e.g. iCloud, e-mail-accounts, chat-accounts, etc..

Subquestion 4:

Are the results valid and reliable for court proceeding?

To proof the validity different iPhones and iOS-versions have been jailbroken with different jailbreaks. For acquisition have been used six tools. Three of them are commercial forensic tools. There were also used free tools like command line and iTunes. Independently from the used iPhone or installed iOS can be said that only with the XRY, UFED, iOS-Foresic Toolkit, command line and iDevice Manager opened a way to acquire additional the system partition after the iPhone was jailbroken.
For acquisition OpenSSH was used with command line. XRY, UFED and iDevice Manger needed AFC2 which was installed to the iPhone to get access to the whole content from the data storage.

XRY and UFED have an included extraction tool. The content from the images was extracted during the acquisitions. With both tools every acquisition was performed a second time and subsequently compared.

The validity and reliability were proofed with different tools and showed that the used jailbreaks gave access to both partitions from the data storage of all tested iPhones.

To be valid on court proceeding local legal aspects and the chain of custody have to be respected.

Subquestion 5:

Can jailbreaking an iPhone for acquisition be a forensically sound method?

A jailbreak is an intervention into the system partition from an iPhone. It installs a software to the system partition and changes it to an unknown way for the operating system. After jailbreaking files and folder can be found in the root directory comparing to the jailbreak. Forensic work wants to change digital traces as little as possible. But sometimes things have to be changed, damaged or even destroyed to get the evidence. Every handling with the data can have real impact on legal proceedings. It is essential to handle digital evidence as every other physical evidence and maintain a clear, documented chain of custody. In compliance with these rules, change of data can be a forensically sound method, but the change has to be declared. To have forensic soundness it must be declared why and what has been changed. Therefore it is important that the installation from the jailbreak has not altered evidence files.

The hypothesis is based on not changing existing data.

To proof if jailbreaking had altered data in an inadmissible way same files have been compared that were acquired before and after jailbreaking an iPhone 7 and X. This way shows us if one from these double existing files had another MD5-hash. If so that were a proof the content has changed through the jailbreak or another influence. Another influence can be ruled out if the same result exits with a second tool. FTK and X-Ways Forensic were used to proof these influences. As result no proofed file has been changed.

Finally, the research question can be answered with yes. To be valid on court proceeding the legal aspects and the chain of custody have to be respected.

In my work as a forensic investigator in Germany, there was a case where a video was made from a criminal offense. This offense was filmed by the offender with an iPhone 4 and deleted afterwards. The only way to get this video back was a physical acquisition from the seized iPhone. To do this the iPhone has been jailbroken with the approval from the prosecutor. The details of this work have been noted in the forensic report. The video from the offense was found and used as evidence at court and led to the conviction of the offender. That jailbreaking has been used as a method to get physical access to the iPhone has not been discussed during the court proceeding.

Since the iPhone 4S has encrypted data-partition it seemed not to have sense to use this method any longer. The practical work in this research has shown that the method even with current devices and iOS-versions led to secure further data that could be considered as evidence.

In this thesis, the methods of jailbreaking current iPhones were examined and also highlighted the different methods and compared results. It has shown that after jailbreaking current devices a lot of more files have been extracted. These files had stored information like GPS-data, timestamps, passwords, passcodes, biometric data, etc, that could be urgent to solve a case. Not only old knowledge has been updated, therefore. It has been tried even to investigate whether the jailbreak has changed the evidence or not. Only then such evidence can be robust enough to be valid on court proceedings. The answer to the research question should also be an answer if jailbreaking could be a forensic method.

In my opinion, under the premise that forensic work should secure as much as evidence as possible the jailbreak should be a self-evident method in crime investigation under respecting legal aspects and the chain of custody.

6.2 Further Work

Within this research and experiments, not all methods have been considered. One method to get further information on how the used jailbreak works are reverse engineering. The missing knowledge about the full potential of a jailbreak can be a problematic point at court. With reverse engineering, the necessary information could be obtained.
The knowledge from reverse engineering could also help to set up new forensic tools that can be used in the same way as jailbreaks before but will have detailed information on how it works. In best cases, a bunch of software tools like OpenSSH and AFC2 that can be installed without an internet connection would be perfect.

During writing the master thesis and experimental work new iPhones, iOS-versions, jailbreaks and tools have released. Changes in this regard may require a re-examination in the future.

Bibliography

Årnes,A., 2017. Digital Forensics, 1st Edition. Wiley, ISBN: 978-1119262381.

Altheide, C. and Carvey, H., 2011a. Digital forensics with open source tools. Syngress, ISBN: 978-1-59749-596-8.

Altheide, C. and Carvey, H., 2011b. Digital Forensics with Open Source Tools. Syngress, ISBN: 1597495868.

Apple.com, 2018. Macos security. Website, last checked: 17.12.2018.
URL https://www.apple.com/business/resources/docs/macOS_Security_Overview.pdf

Aschermann, T. , 2017. Jailbreak - was ist das? Website, last checked: 15.08.2018.
URL https://praxistipps.chip.de/jailbreak-was-ist-das_12321

Becker, L., 2018. Cydia store macht dicht: App-store-alternative fr jailbreaker ist geschichte. Website, last checked: 18.12.2018.
URL https://www.heise.de/mac-and-i/meldung/Cydia-Store-macht-dicht-App-Store-Alternative-fuer-Jailbreaker-ist-Geschichte-4250857.html

Beiersmann, S., 2018. Graykey: 15.000-dollar-gert knackt angeblich jegliche iphones. Website, last checked: 11.06.2018.
URL https://www.zdnet.de/88328833/graykey-15-000-dollar-geraet-knackt-angeblich-jegliche-iPhones/

Benjamin, J., 2011. Untethered jailbreak vs. tethered jailbreak vs. semitethered jailbreak what's the difference? Website, last checked: 12.11.2018.
URL https://www.idownloadblog.com/2011/10/22/untethered-jailbreak-vs-tethered-jailbreak-vs-semitethered-jailbreak/

Britz, M., 2013. Computer Forensics and Cyber Crime, 3rd Edition. Pearson, ISBN: 978-0132677714.

Brown, C., 2018. The first mobile call was made 45 years ago today. Website, last checked: 11.09.2018.
URL https://www.androidauthority.com/first-mobile-call-motorola-851651/

BusinessReport, 2018. The top 5 best selling smartphones worldwide. iol business report. Website, last checked: 16.12.2018.
URL https://www.iol.co.za/business-report/technology/the-top-5-best-selling-smartphones-worldwide-15245741

Carrier, B, 2001. Defining digital forensic examination and analysis tools. Website, last checked: 11.09.2018.
URL https://www.dfrws.org/sites/default/files/session-files/paper-defining_digital_forensic_examination_and_analysis_tools.pdf

Cellebrite, 2019. Supporting new extraction methods and devices. Website, last checked: 28.05.2018.
URL https://www.cellebrite.com/en/productupdates/supporting-new-extraction-methods-and-devices/

Chiu, K., 2018. ios 12 jailbroken hours after release by alibabas cybersecurity division. Website, last checked: 10.10.2018.
URL https://www.abacusnews.com/big-guns/ios-12-jailbroken-hours-after-release-alibabas-cybersecurity-division/article/2164868

Defree, S., 2018. 1st text message to a mobile phone is sent, december 3, 1992. Website, last checked: 15.09.2018.
URL https://www.edn.com/electronics-blogs/readers--choice-2017/4402146/1st-text-message-to-a-mobile-phone-is-sent--December-3--1992

Dernbach, C., 2012. Die geschichte von apple. Website, last checked: 25.10.2018.
URL http://www.mac-history.de/zeitleiste-die-entwicklung-von-apple-seit-1976

Dudovskiy, J. , 2019. Deductive approach (deductive reasoning) - research-methodology. Website, last checked: 14.03.2019.
URL https://research-methodology.net/research-methodology/research-approach/deductive-approach-2/

Fonefunshop.com, 2018. iphone unlocking tools). Website, last checked: 15.12.2018.
URL https://www.fonefunshop.com/professional-unlocking-solutions/Unlocking-Tools/Iphone-Unlocking-Tools/

Forst, G., 2017. The first car telephones. Website, last checked: 15.12.2018.
URL http://www.wb6nvh.com/MTSfiles/Carphone1.htm

Gallagher, S., 2018. Cellebrite can unlock any iphone (for some values of any). Website, last checked: 18.07.2018.
URL https://arstechnica.com/information-technology/2018/02/cellebrite-can-unlock-any-iphone-for-some-values-of-any/

Hansen, K.H., Toolan, F., 2017. Decoding the apfs le system, digital investigation. Website, last checked: 07.12.2018.
URL http://dx.doi.org/10.1016/j.diin.2017.07.003

Help.apple.com, 2018. Help.apple.com. Website, last checked: 11.12.2018.
URL https://help.apple.com/iphone/11/?lang=de#/iph14a867ae

Hoffmann, C. , 2017. Android is open and ios is closed but what does that mean to you? Website, last checked: 10.11.2018.
URL https://www.howtogeek.com/217593/android-is-open-and-ios-is-closed-but-what-does-that-mean-to-you/

Hoog, A. and Strzempka, K., 2013. Logical Acquisition - an overview, 3rd Edition. Syngress, ISBN: 978-1-59749-659-9.

iHelplounge, 2017. Install filzajailed on ios 11 with full root access. Website, last checked: 15.07.2018.
URL https://www.ihelplounge.com/install-filzajailed-on-ios-11-with-full-root-access/

Information Security Newspaper , 2018. A hacker figured out how to brute force iphone passcodes. Website, last checked: 18.08.2018.
URL https://www.securitynewspaper.com/2018/06/23/a-hacker-figured-out-how-to-brute-force-iphone-passcodes/

iPhone-Tricks.de, 2018. iphone-tricks.de8. Website, last checked: 10.12.2018.
URL https://iPhone-tricks.de/die-geschichte-des-apple-iPhone

John, A., 2019. Switch between ios 12 unc0ver jailbreak and electra jailbreak. Website, last checked: 14.05.2019.
URL https://www.techacrobat.com/switch-between-unc0ver-jailbreak-and-electra-jailbreak/

Katalov, V., 2019. Technical and legal implications of ios file system acquisition. Website, last checked: 15.12.2018.
URL https://blog.elcomsoft.com/2019/02/technical-and-legal-implications-of-ios-file-system-acquisition/

Leedy, P. and Ormrod, J., 2015. Practical Research, 11th Edition. Pearson Education UK, ISBN: 9780133741322.

mac4n6.com, 2016. Imaging on the cheap! Website, last checked: 28.05.2019.
URL https://www.mac4n6.com/blog/2016/3/23/ios-imaging-on-the-cheap

MCKemmish, R., 2008. Advances in Digital Forensics IV, volume 285 Edition. Springer,UK, ISBN: 978-0-387-84927-0.

Mead-Green, R., 2017. The pros and cons of iphone jailbreaking. Website, last checked: 01.12.2018.
URL https://www.macworld.co.uk/feature/iphone/is-jailbreaking-my-iphone-or-ipad-safe-3491721/

Moy, T., and Tyrkus, M. J. (Eds.), 2016. American law yearbook. Farmington Hills, ISBN: KF178.W4722.

Peterson, C. , 2017. How i coined the term 'open source'. Website, last checked: 11.11.2018.
URL https://opensource.com/article/18/2/coining-term-open-source-software

Rentrop, C., 2018. iphone-jailbreak: Alles, was man wissen muss. Website, last checked: 21.08.2018.
URL https://www.heise.de/tipps-tricks/iPhone-Jailbreak-Alles-was-man-wissen-muss-4038814.html

Sanford, G., 2019. apple-history.com / iphone. Website, last checked: 23.10.2018.
URL https://www.apple-history.com/iphone

Schmerer, K. , 2018. iphone: ios 11.4.1 bringt usb restricted mode. Website, last checked: 21.08.2018.
URL https://www.zdnet.de/88337051/ios-11-4-1-bringt-usb-restricted-mode/

Statista, 2018a. Apple iphone - verkaufszahlen bis q3/2018, statista. Website, last checked: 04.11.2018.
URL https://de.statista.com/statistik/daten/studie/12743/umfrage/absatz-von-apple-iPhones-seit-dem-jahr-2007-nach-quartalen/

Statista, 2018b. Apple iphone sales by year 2007-2018. Website, last checked: 20.12.2018.
URL https://www.statista.com/statistics/276306/global-apple-iphone-sales-since-fiscal-year-2007/

Statista, 2018c. Apps - anzahl im us app store 2018. Website, last checked: 15.09.2018.
URL https://de.statista.com/statistik/daten/studie/157934/umfrage/anzahl-der-apps-im-iTunes-app-store-seit-2008/

Steimels, D., 2012. Wie alles begann: Die geschichte des smartphones. Website, last checked: 10.09.2018.
URL https://www.pcwelt.de/ratgeber/Handy-Historie-Wie-alles-begann-Die-Geschichte-des-Smartphones-5882848.html

Theiphonewiki.com, 2018. Scam jailbreaks and unlocks - the iphone wiki. Website, last checked: 04.08.2018.
URL https://www.theiphonewiki.com/wiki/Scam_Jailbreaks_and_Unlocks

Varenkamp, P., 12/2017. Forensic acquisition of apple mac computers, specialization course. NTNU, IMT4215 report.