Android vs iOS phone forensics: tools and techniques

Marina Dodevska[1], Vesna Dımıtrova[1], Jovana Dobreva[1], Elissa Mollakuqe[1]
[1]Faculty of Information Sciences and Computer Engineering, Skopje, North Macedonia

{marina.dodevska}@students.finki.ukim.mk
{vesna.dimitrovajovana.dobreva}@finki.ukim.mk
{elissamollakuqe}@gmail.com

Abstract. With the rapid development of technology, the demand for mobile devices is increasing more than laptops, because their main features are large memory, great cameras, low price, and easy availability. Today, we keep too much information on our devices which is very important for our life with this there is possibility that our device has been stolen. A mobile device is very important in investigation making mobile forensics very important for court proceedings and criminal investigations. The paper highlights the importance of specialized forensic tools in mobile forensics, catering to different operating systems (Android and iOS) and offering a combination of free and paid options. These tools serve various functions such as data acquisition, examination, recovery, and extraction. The paper discusses and present a selection of free and paid tools used in mobile forensics, categorizing them based on operating system compatibility, cost, and functions. It provides a summary of each tool's features and their significance in forensic investigations. The paper also concludes by emphasizing the need for professionals in the field to stay updated with the latest advancements to enhance their capabilities in uncovering crucial information, protecting data, and maintaining the integrity of digital investigations.

Keywords:mobile forensics, mobile devices, tools, android and iOS

1 INTRODUCTION

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase mobile device usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS, and MMS messages. Smartphones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

There is a growing need for mobile forensics due to several reasons and some of the prominent reasons are:

- use of mobile phones to store and transmit personal and corporate information
- use of mobile phones in online transactions
- law enforcement, criminal, and mobile phone devices

As a field of study, forensic examination of mobile devices dates from the late 1990s and early 2000s. Early efforts to examine mobile devices used similar techniques to the first computer forensics investigations: analyzing phone contents directly via the screen and photographing important content. However, this proved to be a time-consuming process, and as the number of mobile devices began to increase, investigators called for more efficient means of extracting data. Enterprising mobile forensic examiners sometimes used cell phones or PDA synchronization software to "back up" device data to a forensic computer for imaging. Sometimes, simply performed computer forensics on the hard drive of a suspect computer where data had been synchronized. However, this type of software could write to the phone as well as read it, and could not retrieve deleted data.

2 Related work

The Internet we can find more research on the topic of mobile forensics, more specifically Theodoula-IoannaKitsaki, Anna Angelogianni, Christos Xenakis, and ChristoforosNtantogian in their research [2], performed forensic analysis on two categories: code and disk analysis with the intent to examine all aspects of forensic analysis on Android applications.

The results of this work showed that various user's personal information is stored insecurely and provides important forensic evidence. It is evident that leakage of crucial information such as a users' credit card information and transactions, could seriously violate the user's privacy. Even in cases where the leaked information seems less crucial, such as user's favorite bus routes, their privacy hence, their safety could be seriously harmed. The need to develop new security techniques and implement them correctly is imperative. Kyle D.Lutes, and Richard P.Mislan in their research[3] talk about the challenges in mobile forensics like carriers and manufacturers, data preservation, power and data connectors, operating systems and communication protocols, security mechanisms, and unique data formats. They have concluded that there, are no one tool for investigators to use to retrieve evidence from these devices so that it can aid in investigations. The most likely deterrents to a vendor of forensic tools from creating one single solution are the number of carriers and hardware manufacturers; the challenge of preventing a phone from receiving incoming messages while at the same time keeping it powered; the hundreds of electrical and data connectors currently in use; the many operating systems and communication protocols being used; the security mechanisms in place on some phone; and the unique data formats used by vendors forstoring relevant information. Utkarsha Shukla, Bishwas Mandal, and K.V.D.Kiran in their research[4], they talk about techniques, challenges and several tools in mobile forensics, and they have concluded that LANTERN can

extract more data as compared to any other tool in the market and MOBILedit seems to be one of the most trusted tools for mobile phones as its generated reports are trustworthy. Also, the challenges dealt with forensicsare also noticed by the offenders because of which the network security expertsmust have that skill to deal with those challenges manually or with some automationsystems developed. The main objective in this researchis to present, describe andcategorize the current most relevant security issues andsolutions for Android-based mobile devices (especiallyAndroid-based smartphones). One of the most important strategies presented in this paper is based on the search for risky settings made by the high-level user. To search, identify and mitigate these risks is very important because a considerable number of attacks are based on user misconfiguration. In future work, they intend to implement a specific solution to search for possible user misconfiguration and to suggest corrections for the high-level user in order to increase the device security level. Thus, this solution will be able to reduce the number of vulnerability points caused by poor user configuration, increasing the security level of the mobile device. This paper [6] show the functionality of the software Oxygen Forensic Suite 2011 and Phone Elcomsoft Password Breaker. Besides, it shows the difficulties of a forensic investigation of an iPhone. The authors concluded that the advantage of Oxygen Forensic Suite is that it can break through the passcode lock. However, forensic analysis is not possible on an encrypted device without the examiner knowing the password. Elcomsoft Proactive provides software for this purpose, Phone Elcomsoft Password Breaker. The recovery of the password works, but (depending on the length and composition) may take a very long time. Negative aspects of open source tools are the missing reporting and documentation functions of an investigation for further court usability. In our research, we will provide a brief overview of the techniques and tools used in the forensics of Android and IOS mobile devices.

3 METHODOLOGY

Mobile devices may be attacked on several levels. This includes the possibility of malicious applications, network-level assaults, and the exploitation of device and mobile OS vulnerabilities [7]. Mobile security threats include theft of login credentials for corporate networks. Indeed, mobile phishing attacks, which use texts and emails to trick recipients into clicking on malicious URLs, have been up 85% in the last year.
Cybercriminals have increased their focus on mobile devices as their importance has grown. As a result, cyber threats targeting these devices have broadened. There are many different types of mobile security threats. Although new attacks regularly come to the attention of cybersecurity experts; these are the most common ones:

App based threads: Mobile websites can download malware onto our mobile devices without our permission or awareness. Phishing is a typical way attackers get us to click on links to sites containing mobile threats. For example, a hacker might set up

a website that looks legitimate (e.g. like our banking site) to capture our login credentials.
Network threats: Mobile devices are usually connected to at least two networks. and sometimes more. These include cellular connection, Wi-FI, Bluetooth, and GPS. Each of these points of connection can be exploited by hackers to take over a device, trick the user or penetrate a corporate network
Physical threats: Mobiles are small and easy to steal. Unfortunately, they also get lost pretty often. Without adequate device security, a stolen mobile device is a treasure trove of personal and financial information for a crook.
Organizations that provide mobile devices to their employees or let them use their personal devices for work must first establish strong security measures and implement mobile security best practices.

4 TYPES OF MOBILE OPERATING SYSTEMS

” There are numerous mobile device operating systems available today, and two ofthe mostwidely adopted are the iPhone's OS, Apple iOS, and Google's open source OS, Google Android. These two mobile OS take different approaches to the mobile operating system” [8].

4.1 ANDROID FORENSICS

The primary motive of forensic analysis is to extract necessary data from the device. Hence, for effective forensic analysis, it is imperative to know what kind of data is stored on the device, where it is stored, how it is stored, and the details of the filesystems on which the data is stored [1]. This knowledge is very important for a forensic analyst to take an informed decision about where to look for data and the techniques that can be used to extract the data. In order to perform forensic analysis on any system (desktop or mobile), it's important to understand the underlying file hierarchy.
A basic understanding of how Android organizes its data in files and folders helps a forensic analyst narrow down his research to specific locations. If you are familiar with Unix-like systems, you will understand the file hierarchy in Android very well. Android file hierarchy is a customized version of this existing Linux hierarchy. To see the complete file hierarchy, you need to have root access.

Bypassing Androidlock screens Lock

Bypassing Android lock screens Lock screens are the most challenging aspect of Android forensic examinations. Frequently, the entire investigation depends on the examiner's ability to gain access to a locked device. There is no magical solution that will work every time on every device. There are many methods used to secure a device: None/Slide, Pattern, PIN, Password, Smart Lock (Trusted Face, Trusted Loca-

tion, Trusted Device). Other security options may exist; as Android is open source, the possibilities are only limited by the developer's imagination.Recovering data deleted from a phone's internal storage Data recovery is a powerful concept within digital forensics. It is the process of retrieving deleted data from a device or SD card when it cannot be accessed normally. Being able to recover data that is deleted by a user could help solve several civil and criminal cases.

Recovering deleted data on Android

Recovering deleted data on Android involves two scenarios:

- Recovering data that is deleted from an SD card, such as pictures, videos, ect.
- Recovering data that is deleted from a device's internal storage, such as SMS, dialed numbers, browsing history, application data, chat logs.

While recovering the data from a removable SD card is easy, recovering data from internal memory involves a few complications. SQLite file-parsing and file carving techniques aid a forensic analyst in recovering the deleted items that are present in the internal memory of the Android device. Checking for any installed backup apps on the device is recommended as it saves both time and effort.

4.2 IOS FORENSICS

iOS is one of the most popular mobile operating systems developed and created by Apple Inc. Apple iOS devices include: the iPad, iPod Touch, and iPhone. iOS is the 2nd most popular mobile OS after Android [10]. Apple mobile devices are powerful and beautiful. But with all great and wonderful things, there are those who take these inventions and turn them into objects of evil and wrongdoing. A good foundation in iOS forensics is to have a grasp of the Apple ecosystem and its effect on forensics. A good foundation in iOS forensics is to have a grasp of the Apple ecosystem and its effect on forensics.

Acquiring Data from iPhone, iPod touch, and iPad

This procedure can work on locked and unlocked phones. There are two ways to acquire this data from locked phones. In the first way, you locate the Mac or Windows computer that was synced to the device. The operating system of the computer will dictate where the pairing certificates are that allow the device to sync, regardless if it’s locked or unlocked. The second way is to send the locked device to Apple to unlock the phone and allow the investigator to acquire the logical data. Apple will do this only for law enforcement, and a search warrant will be necessary to have Apple remove the passcode. All that is required for Apple to remove the passcode is the device and a court order. To unlock phones where the examiner has the syncing computer, as in the first example, you need to retrieve the syncing property list.

Logical Data Analysis

The telephone data and third-party applications that are on the iDevices can be a treasure trove of information. An iPhone investigation isn't just getting the call logs and the text messages; there is a complete user history in the application data—from social networking, which is the fastest growing technology, to the advent of mini-blogging. A lot of this data resides on the logical portion of the phone and is in plain text. Some applications can also geolocate, which will help pin down people's locations at specific times. Again, this data is on the phone and easily located and parsed. Bad guys will always find ways to exploit these apps to further their ambitions. You should always have at least an iPod touch handy to populate data from and see how information is placed on the device and therefore educate yourself based on the investigation at hand.

GPS analysis

Geo-location data is important to forensic examinations to place the device or individual at a specific place at a specific time. This can be invaluable information to assist in solving crimes and also to possibly locating perpetrators of crimes. There can be a lot of geodata on an iDevice. Images can also provide a lot of data, which can be very beneficial to an investigation when placing the device at a specific location on a specific date and time. GPS is becoming more and more important in our lives, and it is being used more than ever. The iDevice can store a lot of this information and aid an investigator.

4.3 Toolsused in mobile forensics

These tools cater to different operating systems (Android or iOS), offer a combination of free and paid options, and provide various functions such as data acquisition, examination, recovery, and extraction. The choice of tool depends on the specific requirements and preferences of the user in terms of operating system compatibility and desired functionality. The following table -Table 1 and Table 2. lists several free and paid tools used in mobile forensics.

Table 1.Free tools used in mobile forensics

Tool	**Operating system**	**Function**

Andriller link: https://andriller.software.informer.com/	Android	A software utility with a collection of forensic tools for smartphones. It performs read-only, forensically sound, non-destructive acquisition from Android devices.
Autopsy Link: https://www.autopsy.com/	Android	Used to examine extractions done by other tools and can recover deleted data from supported filesystems
Skype Xtractor Link: https://sourceforge.net/projects/skypextractor/	Android	A forensic software utility for reading and extracting information from the Skype Internet telephone software user data files.
Linux Memory Extractor Link: https://github.com/504ensicsLabs/LiME	Android	A tool that allows the capture of volatile memory (RAM) from a running Linux device. It is the first tool of its type that also supports memory capture from Android devices

The table 1 and 2 demonstrates the importance of employing specialized forensic tools to ensure effective data protection and security. These tools enable investigators to extract evidence, analyze digital artifacts, and reconstruct events, ultimately supporting legal proceedings and the preservation of data integrity

Table 2. Paid tools used in mobile forensics

Tool	**Operating system**	**Function**

Mobiledit Link: https://www.mobiledit.com/	IOS	With MOBILedit Forensic you can view, search for or retrieve all data from a phone with only a few clicks. This data includes call history, phonebooks, text messages, multimedia messages, files, calendars, notes, reminders, and raw application data.
Elcomsoft IOS Forensic toolkit Link: https://www.elcomsoft.com/eift.html	IOS	Allows for physical acquisition on iOS devices like iPhones, iPad, or iPods.
iPhone Backup Extractor Link: https://www.iphonebackupextractor.com/	IOS	Can extract files from iPhone backups and iCloud for your iPhone, iPad, or iPod Touch data.

The table 1 and 2. presents a comprehensive overview of various forensic tools utilized for data extraction and analysis, categorizing them based on their operating system compatibility, cost, and functions. **Andriller,** listed as a free tool for Android devices, offers a wide range of forensic tools. It allows investigators to perform read-only, forensically sound acquisitions from Android devices without causing any data damage or alteration. **MOBILedit Forensic**, a paid tool designed for iOS devices, provides a convenient solution for viewing, searching, and retrieving comprehensive data from iPhones. It enables access to call history, phonebooks, text messages, multimedia messages, files, calendars, notes, reminders, and raw application data. **Elcomsoft iOS Forensic Toolkit**, also designed for iOS devices and available for a fee, specializes in physical acquisition. It offers the capability to acquire data from iPhones, iPads, and iPods, making it a valuable tool for forensic investigators. **Autopsy**, a free tool compatible with Android devices, plays a significant role in forensic examinations. It allows investigators to analyze extractions conducted by other tools and recover deleted data from supported file systems, facilitating the retrieval of crucial information. **Skype Xtractor**, a free forensic software utility, focuses on extracting data from Skype user data files associated with Android devices. This tool proves valuable in reading and extracting information from Skype conversations, aiding forensic investigations. **Linux Memory Extractor**, another free tool, introduces a unique capability for capturing volatile memory (RAM) from both running Linux devices and Android devices. This feature enables investigators to access and analyze important data stored in memory. **The iPhone Backup Extractor**, available for a fee, is specifically designed for iOS devices. It facilitates the extraction of files from iPhone backups and iCloud, enabling investigators to retrieve and analyze data from various iOS devices effectively.

In summary, the Table 1 and Table 2 showcases a diverse range of forensic tools catering to different operating systems. These tools serve essential functions in data acquisition, examination, and analysis, empowering forensic investigators to retrieve valuable evidence and insights from smartphones and their associated platforms.

5 CONCLUSION

The rapid advancement of mobile devices has also increased the need for forensic examination of smart devices. The forensic process represents a great challenge for forensic scientists because there are a large number of devices with different operating systems on the market. Therefore, while the process lasts, it is necessary to have the right tools for work, as well as previous experience, which would facilitate the whole process. The presented table highlights a selection of forensic tools used for data protection, extraction, and analysis in the context of mobile devices. These tools cater to different operating systems, including Android and iOS, and offer various functionalities to aid forensic investigations. The availability of both free and paid tools provides options for investigators with different budgetary considerations. Free tools like Andriller, Autopsy, Skype Xtractor, and Linux Memory Extractor offer valuable capabilities, such as non-destructive acquisition, data recovery, and memory capture. On the other hand, paid tools like MOBILedit Forensic and Elcomsoft iOS Forensic Toolkit provide advanced features like comprehensive data retrieval and physical acquisition, which can be crucial for in-depth investigations.
It is worth noting that the field of data protection and forensic investigation is constantly evolving, with new tools and techniques being developed to address emerging challenges. Therefore, it is essential for professionals in this field to stay updated with the latest advancements and adapt their practices accordingly. By leveraging the capabilities of the mentioned tools and keeping up with industry developments, forensic investigators can enhance their ability to uncover crucial information, protect sensitive data, and contribute to the overall integrity of digital investigations.

6 REFERENCES

1. RohitTamma , Donnie Tindall –“*Learning Android Forensics*”, Pact Publishing, ISBN: 1782174575, 9781782174578, 2015, 322 pages
2. Kitsaki, Theodoula-Ioanna&Angelogianni, Anna, Ntantogian, Christoforos,Xenakis, Christos. *A Forensic Investigation of Android Mobile Applications*. 10.1145/3291533.3291573, 2018
3. Kyle D. Lutes,Richard P. Mislan, Labrmisla Purdue, *Challenges_in_Mobile_Phone_Forensics,* Link: https://www.academia.edu/32800214/Challenges_in_Mobile_Phone_Forensics?sm=b
4. Anna Vojcuk, *Perlustrationon_Mobile Forensics Tool* link: https://www.academia.edu/67022461/Perlustration_on_Mobile_Forensics_Tools?sm=b

5. Cavalcanti, K. R. P., Viana, E., &Lins, F. A. A. *Security Issues and Solutions for Android-based Mobile Devices*. International Journal of Computer Science and Information Security (IJCSIS), 13(9) Link: https://www.academia.edu/16385115/Security_Issues_and_Solutions_for_Android_based_Mobile_Devices?sm=b
6. Thomas Höne and Reiner Creutzburg "*iPhone forensics: a practical overview with certain commercial software*", Proc. SPIE 8063, Mobile Multimedia/Image Processing, Security, and Applications 2011, 80630M (31 May 2011); https://doi.org/10.1117/12.884589. link: https://www.researchgate.net/publication/258726589_iPhone_forensics_a_practical_overview_with_certain_commercial_software
7. Blog, *Phone Security and more*, Link: https://preyproject.com/blog/en/phone-security-20-ways-to-secure-your-mobile-phone/
8. Michael Goad, Mobile *Computing*, link: https://www.techtarget.com/searchmobilecomputing/definition/mobile-operating-system#:~:text=A%20mobile%20operating%20system%20(OS,information%20and%20provide%20application%20access.
9. Sean Morrissey *IOS Forensic Analysis for iPhone, iPad and iPod touch*",SPRINGER 2010