

Comparative Analysis of 4X Smartphone Forensic Toolkits on iOS 13.4 Extracted Artifacts



By

Haq Nawaz

Fall-2019-MS(IS)-00000319766

Supervisor

Dr. Hasan Tahir

Department of Information Security

A thesis submitted for partial fulfillment of the requirements for the degree of

Master of Science in Information Security (MSIS)

In

School of Electrical Engineering and Computer Science,


National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(2022)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by Mr. Haq Nawaz, (Registration No 00000319766), of SEECs has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: 

Name of Supervisor: Dr Hasan Tahir

Date: 08-July-2022

Signature (HOD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

APPROVAL

It is certified that the contents and form of the thesis entitled "Comparative Analysis of 4X Smartphone Forensic Toolkits on iOS 13.4 Extracted Artifacts" submitted by Haq Nawaz have been found satisfactory for the requirement of the degree

Advisor: Dr. Hasan Tahir

Signature:



Date: 08-July-2022

Committee Member 1: Dr. Qaiser Riaz

Signature:



Date: 09-July-2022

Committee Member 2: Dr. Zunera Jalil

Signature:



Date: 13-July-2022

Signature: _____

Date: _____


DEDICATION

I dedicate this dissertation to my parents, colleagues, and honorable teachers
for their love and affection

CERTIFICATE OF ORIGINALITY

I hereby declare that this submission titled "Comparative Analysis of 4X Smartphone Forensic Toolkits on iOS 13.4 Extracted Artifacts" is my own work. To the best of my knowledge, it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation, and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Author Name: HAQ NAWAZ

Student Signature: 

ACKNOWLEDGEMENT

I am thankful to my beloved parents, my wife, and my siblings for their moral support. They have always encouraged me to overcome challenge. Utterly indebted to Mr. Faraz Iqbal Memon, without his guidance and support this work would not have been possible. I am profoundly grateful to my supervisor Dr. Hasan Tahir for his continued interest in planning, execution, and successful completion of the project. It is only because of his consistent encouragement, inspiring guidance, dynamic supervision, and sympathetic attitude that enabled me to prepare this manuscript. He will remain a great source of inspiration and kindness for me. Heartiest thanks and gratitude are also extended to respected committee members Dr. Qaiser Riaz and Dr. Zunera Jalil for their scholarly contribution, valuable suggestions, and constructive criticism toward the successful completion of this research. I am obliged to all my respectable teachers for sparing their valuable time and sharing the knowledge. I believe that this work would not have been possible without their cooperation and support.

I will also express my gratitude to my colleagues, who encouraged and supported me to do MS alongside a job. Despite all the assistance provided by the supervisor, committee members and others, I take the responsibility for any errors and omissions which may unwittingly remain.

TABLE OF CONTENTS

CHAPTER 1	1
INTRODUCTION	1
1.1 Overview	1
1.2 Research Problem	3
1.3 Research Motivation	4
1.4 Problem Statement	4
1.5 Thesis Contribution	5
1.6 Thesis Organization	6
CHAPTER 2	7
LITERATURE REVIEW	7
2.1 Background	7
2.2 Timeline of Related Studies	7
2.3 Existing Research	8
2.4 Artefacts Recovery	8
2.5 Application Specific iOS Forensic Analysis	9
2.6 Analysis Limitations Due to Specific Apps	11
2.7 Facing Challenges and Limitations in DF	12
2.8 Tabular Representation of Literature Review	14
2.9 Identified Limitations	18
CHAPTER 3	19
RESEARCH METHODOLOGY	19
3.1 Arrangement of iOS V13.4 Smartphone	20
3.2 Preparation of Forensic Workstation	20
3.3 Selection of 4x Smartphone Forensic Tool Kits	21
3.3.1 Belkasoft Evidence Center X	22
3.3.2 Oxygen Forensic Detective	22
3.3.3 Magnet AXIOM	23
3.3.4 Smartphone Forensic System Professional	23
3.4 Acquisition of Device (Image Creation)	24
3.5 Comparison with State of the Art	25
3.6 Total Artefacts Extracted Against Each Smartphone Forensic Tool Kits	27

CHAPTER 4	29
COMPARATIVE ANALYSIS	29
4.1 Time Duration	30
4.2 Artefacts Extractions	30
4.3 Timeline and Number of Categories	30
4.4 Category Wise Artefacts	31
CHAPTER 5	33
RESULTS	33
5.1 Most Artefacts	34
5.2 Time Constraints	34
5.3 Dashboard Representation	34
5.4 Timeline Provision in Tool	34
CHAPTER 6	36
DISCUSSION AND FUTURE RECOMMENDATIONS	36
6.1 Conclusion	36
6.2 Limitations	36
6.3 Future Recommendations	37
REFERENCES	38
ANNEXURE.....	43

TABLE OF FIGURES

Figure 1: Insights of Research Methodologies	20
Figure 2: Acquisition of Device.....	25
Figure 3: Insert Case Details.....	43
Figure 4: Select Mobile as Evidence Source	44
Figure 5: Select iOS as Evidence Source.....	44
Figure 6: Load the Evidence	45
Figure 7: Load the Image.....	45
Figure 8: Browse to Select the Image	46
Figure 9: Image Selected as Evidence Source	46
Figure 10: Select Mobile Artifact as Artifact Details	47
Figure 11: Analyze Evidence.....	47
Figure 12: Case Dashboard Displayed.....	48
Figure 13: Add Details of New Case	49
Figure 14: Browse and Select the Mobile Image.....	49
Figure 15: Select the Options to Search.....	50
Figure 16: Details of Selected image	50
Figure 17: OXYGEN Dashboard.....	51
Figure 18: Importing Backup.....	51
Figure 19: Select Import Apple File System.....	52
Figure 20: File Extraction	52
Figure 21: Extracted Files Dashboard.....	52
Figure 22: Extracted Results	53

LIST OF TABLES

Table 1: Existing Literature Review	18
Table 2: Smartphone Specifications and Details	20
Table 3: Workstation Hardware Specification.....	21
Table 4: Software Configuration of Workstation	21
Table 5: Tools and Their Versions Used	22
Table 6: Comparison with State of The Art.....	27
Table 7: Artefacts Extracted by Each Tool.....	27
Table 8: Time Taken by Each Tool for Analysis.....	30
Table 9: Number of Artefacts Extracted	30
Table 10: Categories and Timeline Support	31
Table 11: Artefacts Distribution	32
Table 12: Timeline Support and Categories by Toolkits	35

ABSTRACT

The emergence of technology has put humans into the very different realm of reality of life. Ubiquitous technology now plays a central part in everyday activities. Smartphones are a major advancement that has had a profound effect on human life. The concept of smartphones was once an imaginary concept which is now a reality. With time, its functionality is also increasing with endless customizability. But there is another side of the story, actors that can turn such positive innovation into a disaster. The very same smartphone can be utilized to perform terror activities, online frauds, identity thefts, intellectual property breaches and many more. However, to compete with adversaries, positive actor's also forged ways through which they can identify, detect, examine, and verify the intent of a malicious entity. Digital Forensic Investigators (DFIs) often lack time thus are unable to engage in activities like research for the creation of better and efficient forensic tools. This study focuses the comparative analysis of smartphone forensics toolkits that are design and build to counter adversaries. Thus a comparative analysis of four benchmark toolkits after extracting the artifacts from iOS device version 13.4 has been presented in this research.

A comprehensive study has been presented to show a comparative analysis of 4 x smartphone forensic toolkits. Thus, ranking them according to the artefacts that were extracted by each toolkit during the examination and analysis. To serve this purpose, initially images were taken for iOS 13.4 version and then after confirming the integrity of the image (taken); the same has been examined, analyzed and finally compared by applying the developed methodology. Selection of adequate toolkit is a real issue faced by the study considering international practice toolkits. Firstly, considering the total number of artefacts, Magnet AXIOM presents the most artefacts while Oxygen Forensics and Belkasoft Evidence Center X have been close runner ups. Considering time constraints, Oxygen was the fastest among the 4x forensic toolkits with the shortest time taken to extract artefacts, while Belkasoft and AXIOM are close third and fourth. Considering the dashboard representation for extracted artefacts, Belkasoft and AXIOM were better as compared to Oxygen. To complete the 4x toolkits, MOBILedit was also incorporated but failed to process the image. This study provides in-depth comparative study of toolkits and how those can be used to identify criminal activities. Thus, this research finds the best smartphone toolkits as per the respective category in the numbering mentioned earlier.

CHAPTER 1

INTRODUCTION

To build a fundamental understanding, this opening chapter encompasses essential principles pertaining to the research effort undertaken in this thesis. The technicalities and procedures are explained to assist both novice and expert audiences in developing an in-depth understand. The purpose of this research is to contribute in a constantly developing science of digital forensics and help Law Enforcement Agencies (LEAs) in conducting their daily operations in a more efficient manner. The problem statement, research topic, and rationale for this study are also detailed in this chapter.

1.1 Overview

Diversified applications have become one of the main reasons for the rapid increase in the popularity of smartphones in recent years. According to a report, smartphone users have increased in bulk recently and this range has come to a total of 6.4 billion [1]. An estimate shows that the penetration rate of smartphones has reached more than 80% in comparison to the total population of the world that has come to 7.9 billion. A study has also shown that smartphone users are also increasing speedily with passing time, if compared factually, back in 2016 there were only 3.7 billion smartphone users that are doubled now. However, if calculated in percentage this has grown to 73.9% only in five years. Research conducted in 2019 showed that a typical American adult spends 3 hours and 43 minutes on average in a complete day. This research highlighted that this electronic device usage has broken the previous record of watching television which was 3 hours 35 minutes. At the start of the year 2015 when the online traffic was observed smartphone devices were only reported for less than one third (31.16%) of the worldwide traffic and this figure has grown up to 54.8% only in a course of 6 years and its rise again in 2021 to 75.9% [1]. Keeping these facts in view experts has also predicted that by the year 2026, data usage of smartphones that

was 10 GB at the end of the year 2020 will increase up to 35 GB. This was also reported that smartphones account for 70% of all digital media time in the United States (ComScore, 2019), however, this usage was only 57% when reported in 2017.

On the other hand, a comparison study can also be started between UK and United States considering all the facts and figures reported by several experts. Reports show that back in January 2021, the UK had 65.32 million internet users that increase rapidly in the time of only a year between 2020-2021 with a count of 325 thousand users. Keeping in view this information the internet penetration rate in January 2021, was 96.0% [2]. In January 2021, the United Kingdom had 67.61 million smartphone connections. Drastic changes in m smartphone connections were witnessed where the number of connections fell by 2.5 million between January 2020 and January 2021. But in January 2021, the number of smartphone connections in the United Kingdom was equal to 99.4 percent of the entire population [2].

The magnanimous rise in the use of smartphone devices triggered the intensity of cybercrime likewise, and involvement of phones in it also increased because phones are now replacing laptops and desktops to some extent. One can do everything on a smartphone device that was previously dependent only on laptops or desktops. So, incorporating phones in a digital investigation is vital. Investigations on a worldwide level have taken smartphones into account very seriously depending upon their use and record tracing importance. They are also revealed as a piece of evidence at a crime scene and later on sent for a forensic investigation. Having read all this information there is a dire need for working with the latest iOS version forensic being the lead market player.

Android and iOS now are considered as one of the competitive OS for the smartphone industry. A report that was published in June 2021 has also revealed that Android and iOS are the leading market shareholder in the smartphone OS market with a share percentage of 73% [1]. These figures show that the Android and iOS Operating Systems are ubiquitous on smartphones.

In addition, the biometric API allows apps to leverage fingerprint and facial identification features securely and reliably. Cloud computing is accelerating the development of these applications. The new smartphone cloud computing architecture introduces a novel approach to offloading smartphone apps and employing cloud computing to fulfill resource demands.

Cloud-based computing's growing popularity raises the risk of abuse and criminal conduct. When it comes to the utilization of smartphone technology, there is still a significant gap between policy enforcement and organized crime. In the early 1980s, criminal groups used smartphones

and pagers to avoid capture and facilitate day-to-day operations. While it took decades for law companies and forensic investigators to persuade and understand such difficulties and enhance their operations, it took decades for legal firms and forensic investigators to do so.

Dealing with such issues is a challenge, which was established by employing various tactics and ways. These procedures comprised a wide range of instruments, subject-matter experts, image capturing of digital evidence, extraction, analysis, testing, and verification. Documentation and reporting, as well as sufficient rationale, are all part of the process. Many aspects of people's lives are now transferred to cyberspace, particularly through online social networks or social media sites. Unfortunately, gathering data to rebuild and identify an attack could endanger users' privacy and lead to serious consequences when using cloud services. Defensive tactics include encryption, obfuscation, and cloaking mechanisms, as well as information concealment.

The main goal of this research is to demonstrate and investigate the fact that nothing is destroyed or concealed even when iOS's security is tightened, and new technologies are used. Our research provides a complete review of how contemporary iOS file systems (v14 and later) have been made secure. As a result, file systems have gotten more efficient in storing data and, as a result, at keeping track of all data that has been destroyed.

However, the amount of information that can be recovered from such versions is limited by time and effort. It's also worth noting that each toolkit has distinct advantages and disadvantages over others, necessitating the use of several tool kits and a sufficient skillset to extract relevant data. Even though the privacy and security features in iOS have made it difficult for traditional tool kits to recover lost data, there is always a way and a toolkit. Our research work is a step toward accomplishing the same objectives.

1.2 Research Problem

The main issue with doing forensic analysis on smartphone is that evidence is now scattered over a range of physical and virtual locations, including online social networks, cloud resources, and personal network-attached storage units. As a result, to reconstruct evidence completely and properly, extra knowledge, specific tool kits, and incident correlation skill sets are necessary. Adding to the challenges, there are a plethora of smartphone makers who are always releasing new models. China's cellphone production capacity reached around 127 million units in July 2021 [1]. Because each model has its configurations, access mechanisms, and cable interface for

connectivity, each model is unique. Furthermore, not every smartphone forensic toolkit (software/hardware) recovers and examines all evidence from the most recent iOS versions.

For smartphone forensics investigations, a variety of forensic tool kits for smartphones are available, each with its own set of capabilities and efficiency. One of the most significant obstacles confronting digital forensic investigators (DFIs) is a lack of in-depth understanding about an appropriate instrument in relation to the occurrence and the evidence discovered. Another issue that DFIs frequently confront is gaining access to a certain instrument, since regional borders (LAW) may allow or prohibit the buying of such a toolkit. In comparison to our study benchmark 4 x smartphone forensics tool kits, there is a dearth of research on Apple iOS v13.4. The 4x tool kits are best practices international forensics tool kits in terms of acquisition and examination.

1.3 Research Motivation

In terms of acquisition and examination using best practices international forensics tool kits, there is a limitation of study on iOS versions specially the later versions such as 13.4 and so on. There's also the question of which forensic toolkit is best for which iOS version.

The study's major goal is to identify forensic tool kits that are widely acknowledged as best practices, as well as to evaluate them in terms of artifact acquisition and inspection on iOS 14 v. This study will bring new ideas to the table by comparing the findings of various forensics tool kits on the various iOS versions. To investigate the artifacts from photographs captured with various technologies, all one needs is the correct toolkit. The main objective of this research is to see if the correct toolkit for the job can get you the right type and amount of data.

1.4 Problem Statement

The problem forensic investigators face these days is the variety of device in the market and an ever increasing number of tools that may or may not assist them in their tasks. The problems which exist are:

- Poorly trained forensic investigators tasked with investigating an incident
- Little to no professional help provided by relevant departments/ Law Enforcement Agencies (LEAs)
- Limited credible research on tool kits that are efficient and appropriate under certain circumstances while keeping time constraints and type of digital evidence in mind

As a result, to reconstruct evidence systematically, extra knowledge, specific tool kits, and incident correlation skill sets are necessary. For mobile forensics investigations, a variety of forensic tools for smartphones are available, each with its own set of capabilities and features. One of the most significant obstacles confronting forensic investigators is a lack of in-depth understanding in relation to the occurrence and the evidence discovered. Moreover, many tools are prohibited by LEAs or simply not made available to certain countries. This project will benchmark four forensic analysis tools and their effectiveness in conducting forensic investigations in the iOS environment.

1.5 Thesis Contribution

A wide collection of smartphone forensic tool kits (both open source and proprietary) are accessible on the market. However, there isn't a comparison between those tool kits and Apple iOS 13.4 yet. Furthermore, one of the most important aspects of our study is that it is both proprietary and lawful. For smartphone Forensics Investigators, understanding of the availability and suitability of smartphone forensics toolbox is a problem. According to studies, one set of forensics kit appears to be effective during forensic inquiry, while another set of forensics toolkit appears to be ineffective for the same version. Similarly, the vendor's point of view or self-provided statistics are insufficient to respond completely. Thus this research makes the following contributions.

- The quantitative values for analyses the objects are covered in a comparative analysis report on various smartphone forensics tool kits.
- Quickly learn about the finest forensics' tool kits for Apple iOS v13.4 for artefact capture, analysis, and inspection.
- During the configuration and testing phases, a full report on artefacts, as well as any problems that were encountered and their remedies.

This study will be unique in that it will employ a variety of forensics techniques on the iOS version in question. To investigate the artefacts from photographs acquired with various instruments, all that is required is the correct toolkit. The main objective of this study is to see if the correct instrument for the right job can bring you the proper type and amount of information (evidence). That evidence will eventually provide a positive percentage in the inquiry procedure.

1.6 Thesis Organization

This thesis aims to provide the best possible comparison on iOS 13.4 using benchmark 4x smartphone forensic tool kits. The thesis is divided into six chapters for clarity and understanding.

To be more specific:

- **CHAPTER 1** - offers a brief introduction containing the overview, research problem, its motivation, problem statement, thesis contribution and outline.
- **CHAPTER 2** - provides literature review and limitation in that research.
- **CHAPTER 3** - presents research methodology that was followed.
- **CHAPTER 4** - refers to the core research of this paper that is comparative analysis.
- **CHAPTER 5** – presents the results and outcomes of the thesis.
- **CHAPTER 6** – contains a brief discussion on the work done, the limitations to our research and future recommendation for the research.

LITERATURE REVIEW

This chapter presents a comprehensive literature review carried out to form the basis of the research. Here the focus is on presenting the latest research that is both related and can also update the reader about the state of art.

2.1 Background

Analysis has shown that smartphones are substituting standard computer infrastructure since last decade [3]. People are getting addicted due to spending many on smartphones regardless of age and gender. This is because mobile devices are becoming more user oriented, and most of the human needs can be fulfilled while using mobile phones. Smartphones now enable users to perform professional functions, financial transaction, shop online, establish social connection, and many more all under one compact platform. Similarly, in many aspects, smartphones and computers are almost identical. For example, in contrast to past, newer smartphones can allow an individual to perform multiple tasks simultaneously, such as office suite (excel sheets, word docs, powerpoint presentations, outlook), online presence on social networks (SN's), browsing the web, video chat, and gaming, to name a few. This can be attributed to the fast growth in usage and continual availability of services via the cloud. Excessive reliance on the internet and various digital services has raised the importance of forensically examining and comparing evidence commonly through hash values, stream hash values, metadata, and audio samples [4].

2.2 Timeline of Related Studies

It is pertinent to mention that all the studies considered for the literature review are from the year 2018 and on-wards. All the articles, journal articles, and research papers are taken from recently done work. None are from ten years prior or more. This is so because the researcher wanted to keep the originality and authenticity and realness of the current study intact. Reason

keeping the most recent studies done in the said field for consideration of the following research work is to collaborate in a positive manner to find suitable results.

2.3 Existing Research

In the coming paragraphs, the literature regarding comparative analysis of tools and forensic analysis of iOS is reviewed and discussed.

2.4 Artefacts Recovery

The iOS devices keep their information secure through a strong protection by encrypting the device's passcode, this would prevent accessing the information by a third party. The closed and secure environment of the Apple system makes it difficult to handle some applications during a mobile forensic examination. Therefore, resetting the smart device and after than recovering the artefacts is one of the provisioning exists. When running in a configuration control enabled undertaking wherein in which there are a couple of configurations, records inconsistencies can arise if there are conflicts whilst turning in adjustments. To keep away from such conflicts, you ought to hold alternate units pretty small and supply them as quickly as possible. However, if a records inconsistency does arise, you could manually get better lacking artifacts on your configuration. The software program structures evolve and new modules and dependencies are introduced to aid new features, whilst out of date capability is removed.

Consequently, the layout step by step diverges from its authentic layout. Different layout artifacts grow to be inconsistent with the contemporary implementations, making software program evolution and servicing obligations tough and blunders prone. The adjustments provoke the gadget's evolution because of quite a few reasons; through including the brand-new capability within-side the gadget at the customer's request, adapting the brand-new hardware and software program generation and enterprise choices to enhance the maintainability, reusability and high-satisfactory of supply code. In evolution stage, improvement attempt cognizance on extending gadget abilities to fulfill the consumer desires and the layout step by step diverges from its authentic layout. Different layout artifacts grow to be inconsistent with the contemporary implementation, making alternate obligations tough and blunders prone. Software evolution and servicing phase (maintenance) relies upon on numerous elements inclusive of the lifestyles of correct documentation of the gadget layout.

2.5 Application Specific iOS Forensic Analysis

There is also work completed on non-ephemeral applications, such as [9] conducted a forensic analysis on Kik Messenger on iOS. While there have been similar studies in a wide range of apps, the focus of this review is to highlight the findings in extraction of artefacts from the apps which are specifically ephemeral. In research [6], a new framework was introduced by authors in order to validate the digital forensics software data particularly to apply to smartphones. The framework is mainly centered upon iOS apps; the process of gathering data is performed on iOS devices, then the collected data is transferred onto a laptop to do the validation processes. Consequently, the changes that have occurred on Android and iOS over the last decade has meant that more research is needed to stay up to date with the changing forensic techniques of these Operating Systems (OS), given that they currently are widely used [8].

Researchers [7] also analyzed iPhone Backup Analyzer and Cellebrite Universal Forensic Extraction Device (UFED) that worked on iOS platforms. iPhone Backup Analyze is one of the free source tool kits that enables you to restore unencrypted backups, but you will encounter some problems. In the backup file, all files are logically arranged. The user can access the files and there is a feature to export all the binary files in the backup files forensic review. Backup contents of an iPhone system or other device using an iOS system can be viewed through the frontend provided by the toolkit. Archives and databases can be viewed, and configuration files read. For many illegal acts there are always some clues hidden. Forensic experts have lately placed a high priority on smartphone forensics, that can help investigators in finding evidence by identifying and recovering digital information. Even erased evidence can be discovered with right tool kits and methods. This research aims to dive into the mostly used application and tool kits for forensic investigation, most of them are open source and are Android Debug Bridge (ADB) [35].

Creating a single source specialized to verified tool kits is one option for reforming the forensic investigation. For this we have shortlisted few open-source tool kits after precise research on different digital forensics. Rather than focusing on standalone tool kits, we need to focus on coding methods and plugins [36]. Studies show that a new modern technology is launched every 10 minutes. This rises some critical problems for Android Operating system by the third part interference such as data uncertainty, data exploitation etc. This can be solved by storing data on cloud which makes it inaccessible by unauthorized user [29]. finding the correct toolkit might be tough as market is flooded with both open-source and corporate mobile phone OS. Investigators

use a range of physical and logical acquisition tactics. The study analyses the two methods to see which is the most successful at gathering evidence for forensic investigation. [30].

Although forensic experts can unlock Smartphones and extract essential data, user information integrity is a major issue when collecting evidence from them. In a nutshell, the images of a phone that has been cloned in order to obtain access to the system are the subject of this study. The main issue in investigation is the huge number of Android/ iOS devices on the market, as well as the frequent change in OS versions and the lack of a new tool kits that are applicable to forensic investigation of all Versions of Android and iOS. Logic and physical analysis are required for data extraction and inspection from smartphones. ‘Autopsy’ and ‘Belkasoft Evidence Center’ are two popular data analysis programs that can be used to evaluate collected data in forensically manner [23]. The capability of smartphones to isolate application program is one of its security features. On either hand, the Android user-based permission method violates that privacy characteristic. In view of these facts, surveys were performed to gather information on customers' knowledge of Android and iPhone permissions. People lack critical knowledge about Android and iPhone permissions, as per the conclusions of this poll, which included 380 respondents, which directly results to hasty decisions when downloading apps on Android mobile device [24].

With a market share of over 73%, the Android operating system is widely installed by smartphone makers [25]. Every day, tens of thousands of applications are added to the Android repository by major vendors and given available free by Android phones. Most created apps are designed by third parties, resulting in significant loopholes that may subject user privacy to numerous risks. Data is available on the cloud storage and is accessible to authorized third parties. Cloud computing on Android smartphones is in risky due to this unlawful access to information. The evaluated study provides a method for safeguarding information and data when utilizing an iOS and Android cloud application from unauthorized access [26]. It is critical to emphasize that the research effort is varied. Many existing Mobile malware detection approaches were thoroughly evaluated and classified based on their detecting methodologies for first stage.

They were also evaluated in terms of their benefits and limitations. For Android, a research team developed a novel malware detection methodology this is a hybrid technique for excellent accuracy rate known as SAMADroid. It delivers great malware detection accuracy by optimizing power and storage use [27]. In this open-ended 3 level algorithm malwares are detected using a 3 layered method which included static as well as dynamic analysis, physical and virtual hosts, and

machine learning understanding. Results are way higher than Drebin's methodology [28]. The proposed model does not require admin privileges, boosting interoperability for Android devices and ignoring spyware categorization. These evaluations have been effective in extracting personal details, images, video files, contact records, and SMS.

Study has helped to establish that MOBILedit has been able to outperform Magnet AXIOM on more data extraction and recovery aspects [38]. Because of the massive commercial exploitation of wide range of digital devices, forensic investigation, a process in which digital information stored in digital devices is precisely recognized, gathered, maintained, and evaluated, as well as the data is tabled to the court evidence, is receiving wide acceptance. This report analyzes electronic forensic tool kits and contrasts them in terms of convenience of use, supporting investigators in integrating them into inquiries by offering an assessment of their aspects, tool kits, and capabilities [37].

According to research [39] both freeware and profitable forensic software are contentious fields, with opposing concerns about accessibility and security. By comparing the analysis of forensics tool kits on the same collection of images against subsequent versions 8 and 9 of Android devices, our research aims to uncover the most promising prospects for aiding Law Enforcement Agencies (LEAs). Various sets of the most recent and popular forensic tool kits used for analysis on various versions of Android give a proper orientation for investigation process that fully utilizes a beneficial path with LEAs throughout the investigation process

2.6 Analysis Limitations Due to Specific Apps

In another research [10], author forensically investigated a mobile device, an iPhone 4 running iOS 5.0.1 previously jail broken by the mobile phone owner, as a part of a real legal case. The case was from the Sultanate of Oman, and the aim of the investigation was to forensically examine the iPhone to determine if the device had been hacked and sent messages over the application 'WhatsApp' out to the owner's contact list. In the investigation, the ISP report of the device was observed and examined, and two forensic tool kits were used to extract and examine mobile data, one toolkit being the Universal Forensic Extraction Device's (UFED) physical analyzer Cellebrite, and the other being the Oxygen Forensic Suite. The credibility of both tool kits is highly regarded by computer forensic experts. Results showed that Cellebrite recovered more forensic evidence than Oxygen, including call log artefacts, SMS messages, web history, etc.

A comparative study can serve as the basis for several Android/ iOS users, forensic investigators. The study discovered, for example, that just a handful of articles regarding Android forensic tool kits are available [19]. Research depicts the architecture of Android, along with thorough information on its security protocols and the main dangers it faces, as well as important components. It also shows data recovery by providing a simple comparison of forensics methodologies. In addition, the research article develops research on the architecture of Android and data recovery that might lead for a future research project. In this research work commercially available toolkit Paraben E3: DS and open-source forensic toolkit Autopsy are compared. Results show that commercially available toolkit outperform the open-source toolkit for Android smartphone versions. [20]. Another research looked into a technique that did not allow forensic tools to collect encryption key from Android devices. The key is kept in ROM of the smartphone thus making the key inaccessible [21].

2.7 Facing Challenges and Limitations in DF

This smartphone regime has made technology more susceptible to attack when considering user data privacy. At the same time in many cases the smartphones serve as powerful toolkit for committing crime owing to which forensics of smartphones is a key field for this purpose. Since all cyber-crimes typically include smart technology, the examination of this kind of storage media with reference to any crime activity can yield critical information about just the actions that have occurred frequently [11]. The use of mobile forensics is an important part of obtaining clues against any crime [12]. Traces of erased data is stored in cellphones' internal memory. Due to the absence of relevant significant tool kits and understanding of such tool kits for the newest Android/ iOS versions, thus massive amount of data is not retrieved, and cannot be traced fruitfully.

Smartphone forensics is gradually stretching research to include the presentation of systematic and complex information as well as aggressive behavior analysis. Research illustrates the extraction of data via smart devices in addition to its core. Despite this, data collection remains the primary emphasis of research. Innovations, such as the role of cloud computing in the smartphone investigative environment and the development of mobility applications in the industry, such as mobility management and bring your own device (BYOD), present new potential and problems in this area [13]. As the mobile device industry grows, the probability of cellphones being utilized for illicit activities will also grow. As a result of the vast number of manufacturers and versions available, the smartphone industry is becoming diverse. Professional analysts may struggle to

identify the suitable forensic tool kits to capture material from your smartphone's internal storage [14]. One approach is to set up a forensic farm, where the toolkit captures images of the file of Symbian and Windows Mobile devices, delivers them to the forensic operator's mobile device, and the programmed automatically transmits them. This gives a quick and reliable answer. The goal of this rapid response is to get key investigation information to crime scene operators as soon as possible so that more evidence about smartphone content is focused [15].

Information gathering is an integral part of every research. Data must be extracted (in a forensically legitimate order) before it can be analyzed [16]. Phones are replicas of a person's personality and hold considerable data of personal nature. Thus, main goal is to do forensic analysis on 13.4 iOS version w.r.t significant comparison of extracted Artefacts by means of 4 x Smartphone forensic tool kits. smartphones are manufactured each year with a variety of hardware and operating system which presents huge challenges for Digital Forensic investigators (DFI). Majority of current mobile forensics investigation is possible only by unlocking devices to retrieve information [17]. Unlocking smart device offers a real challenge for forensic investigators, as numerous papers in this research will demonstrate user data integrity. Rooting is a disadvantage in itself, when at all feasible, it should be avoided. The method usually takes advantage of a security hole in a specific device or operating system, and it might lead to more security flaws. Rooting also modifies some aspects of a device (an action contradictory to forensic practices). Rooting a device for forensic access is a risky proposition.

Rooting a device for forensic access is a risky proposition. On the other hand, skilled examiners can use easily available tool kits to analyze digital devices [18]. Justice system is increasingly fighting with cybercriminals, requiring the creation of technologies to scan smartphones for evidence in this case in a systematic manner.

Data encryption makes it harder for investigators to evaluate data clearly as many applications are data encrypted to ensure the privacy of personal data. Volatile memory is a critical for both OS and application thus it holds major interest of analysis in digital forensics. Number of researches have been proposed for gathering volatile memory form mobile devices. Confidential data is retrieved from volatile memory using a technique called PASM, introduced by a researcher for android memory. It uses intermediate devices to migrate personal data, this action is doable by Androids OEMs. Experiments are conducted on 30 different data sensitive applications with 7 optimal experimental conditions. Resulting in leakage of private data from memory using PASM

method [31]. The 'EaseUS Data Recovery Wizard is an open-source application, used to retrieve files from the LOST.DIR on external memory [32]. In the respective study [33], some data can be retrieved from digital device without any authorization required.

Nowadays mobile devices are used by a large population of users. These devices carry some of the most personal and important information about an individual. Research [34] on this issue is considered very useful for educational reasons. The research merely focused on the Android architecture, memory design and data flows. The research also proposed a technique for designing a better application for control resources and retrieve important data. It also proposed some data retrieving method that assist in forensic analysis of a given system.

There is a need to ensure that devices can be securely wiped when they are misplaced, stolen or disposed. In [40] studied that data can be recovered, from the three categories of wiping, using Mobile Phone Examiner Plus, and MOBILedit.

It is important to authenticate the record before consideration as legal evidence. Study [41] aims to develop a method to authenticate audio recordings generated using the iPhone.

2.8 Tabular Representation of Literature Review

The literature review in the previous section is represented here in tabular form to give more clarity.

S no	Paper Title	Tools	Versions	Limitations
1	A Comparison Analysis of Saved Snapchat Video Files on Android Vs iPhone		iPhone 6	Only focused on snapchat video files
2	Mobile Device Forensics	MOBILedit iPhone backup analyzer Extraction device (UFED)	Android iPhone 6s	Missing comparison of different datasets w.r.t to forensic tool kits

3	A Method of Forensic Authentication of Audio Recordings Generated Using the Voice Memos Application in the iPhone	Magnet forensics sleuth kit (Autopsy) prodiscover Oxygen Forensic suite	iPhone (11 Pro max, 11 pro, xr, 12 pro max) galaxy (a12, a72, a31) blackberry evolve (x, key2)	Application specific
4	Effectiveness of Mobile Wiping Applications	Mobile phone examiner plus (MPE+) from ACCESSDATA, and MOBILedit	iOS 13.2.2 Android 6.0.1	
5	Comparative Analysis of Android Forensic Tools [42]	MOBILedit Cellebrite's UFED The sleuth kit Sans sift including other 24 tools	Android (2,4,5)	Missing comparison of different datasets w.r.t to forensic tool kits. No physical extraction
6	Comparative Analysis & Study of Android/ iOS Mobile Forensics Tools [38]	Magnet AXIOM MOBILedit	Android 8,5.1/ iOS 13.5, 14.4	Only two forensic kits were used. Missing detailed sn's data extraction and comparison No subcategory comparison
7	Analyzing Data from An Android Smartphone While Comparing Between Two Forensic Tools	Autopsy and paraben e3:ds	Android	Only focus on WhatsApp, twitter and fb sn's apps with no quantitative values.
8	Comparative Evaluation of Mobile Forensic Tools [43]	ACCESSDATA FTK imager, paraben device seizure, encase, and MOBILedit	Android	Data (photos, videos, audio, documents, music, Text, links, username)
9	Mobile Forensic Tools Validation and Evaluation for Instant Messaging [44]	Wa key/ db extractor, Oxygen Forensics, and magnet AXIOM, NIST forensic tool	Android	WhatsApp artifact, application specific

10	An Improved Framework for Cyberbullying Investigation Process On WhatsApp Application [45]	MOBILedit and Belkasoft evidence center x trial	iOS v14.4	Acquisition, data extraction and analysis of WhatsApp, application specific
11	Analysis of a Third-Party Application for Mobile Forensic Investigation [46]	Editplus3 Plist editor for windows Apple iTunes Ibackupbot iPhone backup extractor Ibackup viewer iPhone tracker Db browser for SQLite	iOS v10.3.0	Only focus on third-party applications
12	Mobile Forensic Tools Evaluation for Digital Crime Investigation [47]	WhatsApp key/ db extractor, Belkasoft Evidence Center (ver trial), SQLiteStudio	Android	Application specific and it is on Android
13	Forensic Analysis of Social Networking Applications on An Android Smartphone [48]	Magnet AXIOM, XRY, Autopsy	Android	
14	Forensic Analysis of Android-Based WhatsApp Messenger Against Fraud Crime Using the National Institute of Standard and Technology Framework [49]	Ftk, Oxygen	Android	Only focus on WhatsApp. Only two forensic tool kits were used

15	Forensic Tools Performance Analysis on Android-Based Blackberry Messenger Using NIST Measurements [50]	Andriller, Oxygen Forensic suite and Autopsy	Android	Only focus on bb messenger. Only three forensic tool kits were used
16	Comparative Study on Data Extraction and Acquisition Tools for Facebook Messages [51]	Cellebrite, encase, ofs, ftk, tfd, adel, fmf, caine	Android	Only focus on Facebook
17	Comparative Study of Mobile Forensic Tools [52]	UFED, paraben, XRY and MOBILedit	Android	
18	Physical Data Acquisition from Virtual Android Phone Using Genymotion [53]	Autopsy, foremost	Android	
19	Comparative Study of Various Digital Forensics Logical Acquisition Tools For Android Smartphone's Internal Memory [54]	Encase, mobile Device seizure, Mobile Oxygen Forensics, MOBILedit, mpe+, secure view, UFED, XRY	Android	Android based
20	Digital Forensic Tools Used in Analyzing Cyber Crime [55]	Encase, digital forensics framework (dff), cofee, prodiscover, recuva, caine, FTK, bulk extractor, Autopsy, sift, redline, hxd, magnet ram capture, nigliant32, memoryze, MOBILedit,	Android/ iOS	Only introduced the tools. Not included the working of tools. Categorized the tool but not compared. Only two liner about the tools used. Lacks practical demonstration. Nothing about extraction

		Andriller, Belkasoft evidence		
21	Forensics Analysis of WhatsApp in Android Mobile Phone [56]	WhatsApp db/ extractor and Belkasoft evidence center	Android	Focuses on WhatsApp only. Only two tools used.
22	Forensic Analysis of “WhatsApp” Artifacts in Android Without Root [57]	WhatsApp forensics, Autopsy 4.4, Andriller, db extractor, finalmobile forensics4	Android	Focuses on WhatsApp only.
23	Assess of Forensic Tools on Android Based Facebook Lite with The NIST Method [58]	MOBILedit forensic express pro, Magnet AXIOM forensics	Android	Focuses on WhatsApp only. Used only two tools

Table 1: Existing Literature Review

2.9 Identified Limitations

Considering the literature review regarding this study, it was evident that majority of studies lacked following key points, which this study addresses:

- Studies are application specific
- Mostly research is performed in controlled environment with no real existing scenarios (data sets)
- Working on application specific evidence
- Missing in comparison of tool kits in terms of efficiency in time, artefact extractions and dashboard for results
- Missing artefacts for entire user profile data set

RESEARCH METHODOLOGY

This research is focused on analyzing data set of iOS 13.4 mobile device while conducting the examination, analysis on 4 x smartphone forensic tool kits. Comparison of extracted data against each toolkit is the core of our research. This is necessary to know which amongst the forensics tools performs the best under the same data set. Sub-categorization is also the part of our research. Keeping the real-world scenarios and actual investigation of iOS devices, a forensically sound methodology on data extraction, generating a hash value and time stamps are required to prove evidence in the court of law. Therefore, all the experiments in this research will be performed using forensically accepted tools under the required condition by the National Institute of Standards and Technology (NIST). This will preserve the integrity of data on the Android phone so that evidence can be accepted in the court of law. Both quantitative and qualitative methods are adopted to conduct this research study.

Following figure highlights the insights of our research methodology.

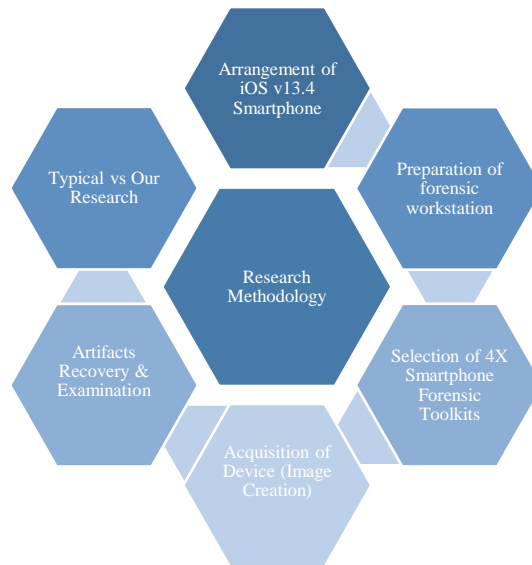


Figure 1: Insights of Research Methodologies

3.1 Arrangement of iOS V13.4 Smartphone

The test phone for this research was iPhone SE with iOS version of 13.4.1. The rationale behind it was that research on 13.4.1 was not available. In addition, for fruitful results we acquire the acquisition of mentioned set with the capacity of user data around 9GB. We aimed towards finding user level artifacts. Following are the smartphone specifications details that was used in our research:

Category	Description
Make	iPhone SE
Model	A1662
RAM	2 GB
Storage	64 GB
Serial	DX3T126VH2XV
iOS version	13.4.1
Build	17E262

Table 2: Smartphone Specifications and Details

3.2 Preparation of Forensic Workstation

It is recommended to decide things ahead of the forensic analysis. In order to truly test the efficiency of the tools, it is very important to test the tools under same conditions. For that purpose, we kept the following specifications for the system on which all tools be tested. It is pertinent to mention that we have kept specifications that provides the optimal results. Before diving deep into

the comparative analysis of the tools, we need to know about the machine specifications used to install and run selected 4x smartphone forensic tool kits for comparative analysis of iOS version 13.4. The target system has been built so each selected Forensic Toolkit requires minimum resources while delivering maximum efficiency of the tool. Hardware specifications for this scenario are:

Hardware Specifications	
RAM	64-128 GB DDR4
Processor	Intel(R) Xeon(R) Gold 6238 CPU @ 2.10GHz
Generation	10 th
SSD	2 TB
OS	Windows 11

Table 3: Workstation Hardware Specification

Note: It has been noted that as one increases the device specifications, time to generate the results decreases.

We have kept the specifications optimal, so we used 64 GB RAM for the image processing of iOS 13.4.1 onto the tools. Every tool is tested on the same machines to produce best results. Xeon processors are more suitable for round the clock performance, so we chose that for the image processing. The software utilized for the forensic analysis are as follows:

Software Specifications	
Image Creation Tool	Magnet Acquire
OS	Windows 11
Benchmark Tools for Extraction of Artefacts	Belkasoft Evidence Center X
	Magnet AXIOM
	Oxygen Forensics
	Smartphone Forensic Professional

Table 4: Software Configuration of Workstation

Magnet Acquire was used for image creation. Other 4 x Benchmark Forensic toolkits are for the extraction of artefacts on which comparison analysis was carried out.

3.3 Selection of 4x Smartphone Forensic Tool Kits

Four best practice international standard mobile forensic tool kits were used for acquisition, analysis, examination, and comparison of extracted artefacts from iOS device. Keeping in view the metrics against each selected toolkit during acquisition, and analysis phase. These values are:

- How tools vary in terms of artifacts extractions
- Total no. of artifacts and sub-categories extracted
- Metadata details
- Support for images acquisition formats
- How much time to be consumed during image acquisition and analysis

Smartphone Forensics Toolkit	Versions Used in Study
Belkasoft Evidence Center X	2020v9.98
Smartphone Forensic Pro	6.120.2111.1013
Magnet AXIOM Forensics	4.10.0.23663
Oxygen Forensic Detective	12.0.0.151

Table 5: Tools and Their Versions Used

Following are the introduction of the tool kits that were selected for this study:

3.3.1 Belkasoft Evidence Center X

In a forensically sound way, Belkasoft Evidence Center X obtains, investigates, analyses, and presents digital evidence from key sources—computers, smartphone devices, RAM, and cloud services [59].

Belkasoft Evidence Center X is a comprehensive product used for various types of investigation tasks. Besides the following one can utilize it for tasks where a digital device is involved, and it is needed to recover and analyze its contents:

- Conducting digital investigations in a criminal or civil case
- Incident response
- Low level analysis for various types of files such as SQLite databases, registries and so on
- Search for illicit pictures and videos
- Data recovery
- Surveillance

3.3.2 Oxygen Forensic Detective

The Oxygen Forensics is the world's premier provider of digital forensics software, providing important data and insights to law enforcement, government agencies, and businesses faster than ever before. Oxygen Forensic Detective is a multi-source forensic software platform that extracts, decodes, and analyses data from smartphone and IoT devices, device backups, UICC and media

cards, drones, and cloud services. From Windows, macOS, and Linux PCs, Oxygen Forensic Detective can locate and extract a wide range of artefacts, system files, and credentials [60].

The cutting edge and innovative technologies deployed in Oxygen Forensic Detective include, but are not limited to:

- Bypassing screen locks
- Locating passwords to encrypted backups
- Extracting and parsing data from secure applications
- And uncovering deleted data.

3.3.3 Magnet AXIOM

The Magnet AXIOM automates the digital forensic process for lawfully obtained evidence such as cellphones, the cloud, third-party apps, laptops, hard drives, and IoT devices, and consolidates the data into a single solution for improved analysis [61]. Magnet AXIOM is comprised of two parts: AXIOM Process and AXIOM Examine. Using AXIOM Process, you may gather forensic photos, import existing images, and execute scans on those images all from the same interface, depending on your licensing. After processing is complete, you may evaluate the evidence in AXIOM Examine.

Standout features of Magnet AXIOM are:

- The artifacts-first method employed by AXIOM brings the most relevant data and artefacts to the foreground, saving you time and effort.
- From 1000+ artefacts, advanced parsing and carving procedures obtain the most detailed artefact data.
- Industry-leading conversation, image, browser history, and location data discovery.
- Use AXIOM to find other macOS artefacts including AirDrop, Live Photos, KTX files, and iCloud Tabs.
- Use Volatility in AXIOM to improve investigations by recovering and analyzing memory artefacts

3.3.4 Smartphone Forensic System Professional

The SPF Pro (Smartphone Forensic System Professional) is a forensically sound system for extracting, retrieving, analyzing, and triaging data from smartphone devices such as Android phones and tablets, as well as iPhones and iPads. It is the next version of the SalvationDATA

smartphone forensics toolkit, as well as a robust and comprehensive platform for digital investigations [62]. It enables investigators to examine and ascertain relevant information from Smartphone devices both in the field and in the lab, and it assists them in recovering and collecting critical forensic evidence from massive backlogs of even locked smartphones using multi-tasking and intelligent analysis functions and extract more evidentiary data in less time than ever before easily and efficiently.

With the rapid advancement of technology, Digital Forensics among law enforcement agencies now demands more authorization to access Smartphone phones for criminal investigations. Now, using SalvationData SPF Pro (Smartphone Forensic System Professional), you may deeply access a variety of Smartphone phones running Android, iOS, Symbian etc. SPF Pro can simply complete the suspects' analysis with data extraction and imaging for the inspected phones. Additionally, collaborating with the Big Data Forensics System would provide investigators with a comprehensive and visually appealing analytical report.

3.4 Acquisition of Device (Image Creation)

Acquisition of artefacts in every tool follows specific patterns. But if one observes keenly, they all follow the same flow to get the DFI into the detailed interface of their respective artefacts window. This flow is shown in the below figure to provide the basic understanding of how this process works.

Some information related to image creation is following:

1. The phone was in open state with no pin lock.
2. Data inside phone was missing. It was either wiped out or never used. This experiment was to find the same statement.
3. After smartphone was selected, its image was to be taken.
4. For that phone was connected with the specified cable before connecting to the phone.
5. Magnet Acquire was used for a second extraction

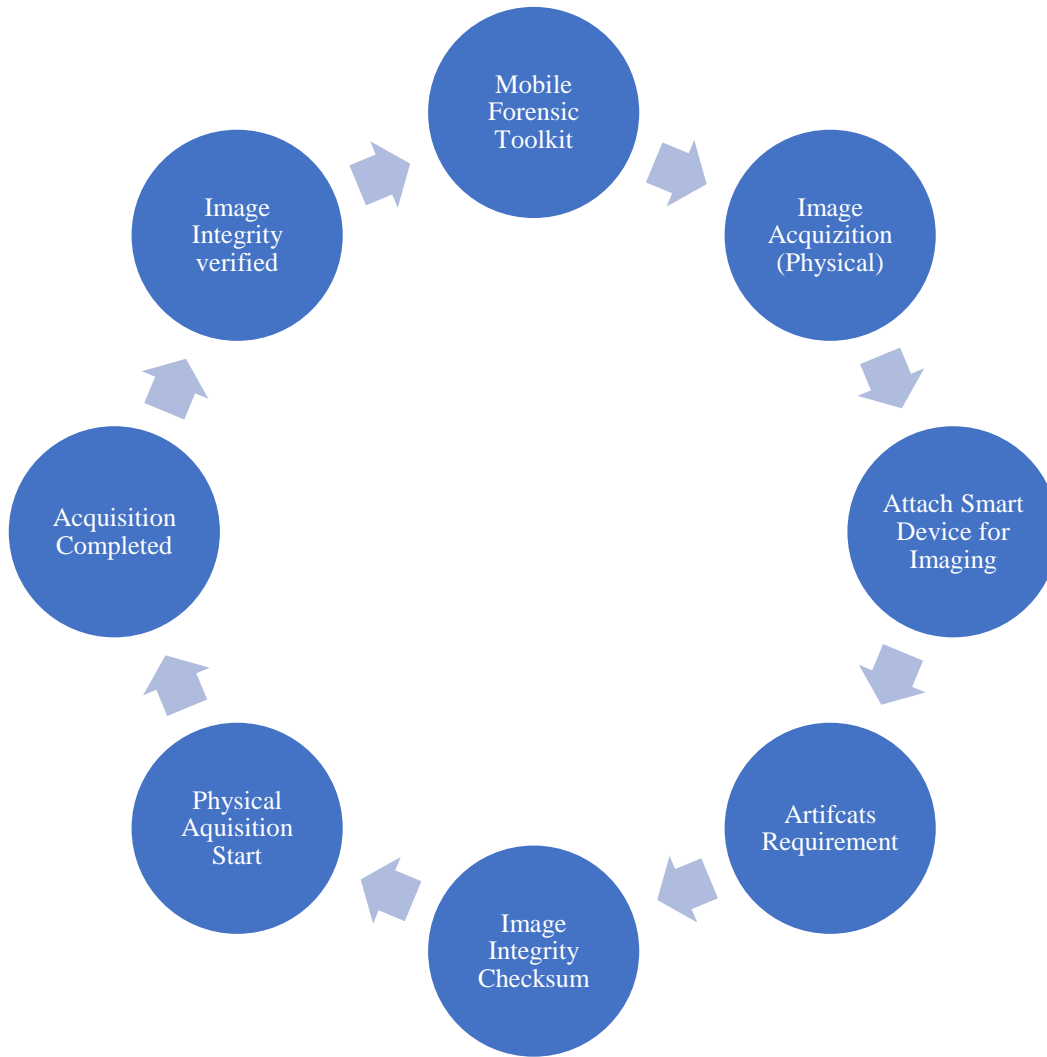


Figure 2: Acquisition of Device

The above figure explains all the steps that were taken to perform forensic analysis of the iOS 13.4 on 4x smartphone forensic tool kits. Firstly, toolkit is invoked, while all other irrelevant processes are closed. Purpose of closing other processes is to keep resources open for the toolkit to utilize. Secondly, image acquisition process is performed using the standard hardware. Moreover, device is attached for imaging; artefacts requirements are fed to the tool for swift results. After compiling image, its integrity is checked using hash; and physical acquisition is pushed in the tool. When acquisition is completed, its time is noted. Lastly, image is verified again.

3.5 Comparison with State of the Art

Detailed comparison of existing research and research presented here is in tabular form below:

Traditional	Our Research
-------------	--------------

Case creation	Case creation
<p>Acquisition & Selection of tool kits</p> <ul style="list-style-type: none"> • Arrangement of a mobile device or a hard disc • Taking image of that potential forensic evidence • Performing a RAM dump if requires • Analysing results produced by the tool kits 	<p>Acquisition & Selection of toolkits & Installation of Dedicated Forensic Workstation</p> <ul style="list-style-type: none"> • Arrangement of a smartphone • Image creation, verification of a mobile device. This is how the Smartphone Images are arranged. • As a study benchmark, we'll use 4 x smartphone forensic tool kits. Arrange high specification machine to get installation of 4 x smartphone forensics tool kits.
<p>Adding Data Source to the Case</p> <ul style="list-style-type: none"> • Using any smartphone forensic toolkit to add one or more dumps • Using a third-party programme to make an image or dump 	<p>Adding Data Source to the Case</p> <ul style="list-style-type: none"> • After Image acquisition, load the image as a source for further examination and analysis
<p>Artefact Extraction and Review</p> <ul style="list-style-type: none"> • Artefact recovery and extraction for over a thousand different applications and formats straight out of the box • Carving deleted data from allocated or unallocated space, RAM, slack space, and other locations, including carving. 	<p>Artefact Extraction and Review</p> <ul style="list-style-type: none"> • Each image is processed, and artefacts are extracted out of the box for over a thousand different apps and formats using four smartphone forensic tool kits.
<p>Analysis and Events Correlation Building</p> <p>Event correlation w.r.t to conducted crime is the decisive factor for digital forensic investigation</p> <ul style="list-style-type: none"> • In this step the DFI's normally conduct the analysis of extracted artefacts, explore the facts and draw a line to co-relate the artefacts in a manner such that eventually the extracted data can become the strong evidence against conducted crime. 	<p>Category Analysis</p> <ul style="list-style-type: none"> • As our study is not based on to investigate the extracted artefacts rather than our study is focused on the artefacts categorization that eventually becomes useful in comparison examination, based on our benchmark of 4 X smartphone forensic tool kits.
<p>Reporting</p> <ul style="list-style-type: none"> • Creating reports in a variety of formats, including HTML, PDF, Word, Excel, and others 	<p>Reporting</p> <p>Reports based on four smartphone forensic tool kits are accessible in a variety of forms, including PDF, Excel, and others, and are appended to help with the artefact inspection.</p>

	<p>Comparative Analysis</p> <p>In this stage of our research, we comparatively analyse the extracted artefacts by using four smartphone forensics tools against each artefact including picture, audio, video, social networks accounts, web related data, contacts, documents etc.</p>
--	--

Table 6: Comparison with State of The Art

3.6 Total Artefacts Extracted Against Each Smartphone Forensic Tool Kits

Table below represents the total number artefacts extracted against each category by the selected 4x smartphone forensic tool kits.

		Tools			
		Oxygen	AXIOM	Belkasoft	SPF Pro
Artefacts	Accounts/ Emails		782	108	-
	Installed Applications		93	192	-
	Contacts		4	18	-
	Media (Audio)		678		-
	Media (Video)		1681	131	-
	Documents	3311	4808	959	-
	Pictures	31101	26220	16841	-
	Social Media		961	446	-
	Web Related		23258	1166	-
	FR (Facial Recognitions)/ Owner Information		5		-
	SSIDs (Network)		5	1	-
	GPS	6	4	1203	-
	Encrypted Files/ Achieves	3137		61	-

Table 7: Artefacts Extracted by Each Tool

Above table distributes the artefacts as per major categories. These categories are defined by tool kits that are considered as benchmarks in smartphone forensics. Most number of artefacts are extracted by the Magnet AXIOM.

Note: The key point worth mentioning here is that the SPF Pro does not support .tar format. MOBILedit was also run to check the additional tool to meet 4x smartphone forensic toolkit. This tool also does not support .tar formats.

COMPARATIVE ANALYSIS

Comparative analysis entails comparing one object or piece of data with others to find similarities and contrasts, such as a statement, an interview, or a theme. It is thus feasible to create a conceptual model of the possible relationships between distinct things by isolating these elements [63]. Comparative analysis helps in creating a better understanding of why and how one thing is better than other, or what are the factors that decide which thing has advantages over other. Comparative analysis plays important role in providing guidance to relative professionals in deciding which thing to use under what circumstances.

The comparative analysis is dependent on number of keys, depending on the type and domain of comparative analysis. This research aims to produce comparative analysis of forensic tool kits. For that purpose, numbers of quantitative and qualitative parameters have been identified. Following are the key parameters that will play decisive role in the comparative analysis of forensic tool kits:

- This research provides comparative analysis of tool kits based on their ability to create user profile that is missing in the previous research
- In addition, this comparative analysis is not application specific i.e., results produced on specific application like WhatsApp etc.
- This comparative analysis also caters timeline of the artefacts produced and captured by the toolkit
- Lastly, this research will also focus on time taken by the tools to generate those results.

4.1 Time Duration

First parameter of comparison is to check the time taken by the application to fetch the results. In the given table below, the forensic tool kits and the total time taken by the tool is shown.

4 X Smart Forensic Toolkits	Total Time Taken by Tool
Magnet AXIOM	1 hour and 13 minutes
Smartphone Forensic Professional	-
Belkasoft Evidence center X	32 mins and 24 sec
Oxygen Forensic Detective	12 min and 21 sec

Table 8: Time Taken by Each Tool for Analysis

Considering time constraints, Oxygen Forensic Detective happened to be the more effective with 12 mins and 21 seconds. In addition, with short time, Oxygen also produced significant number of artefacts from the digital evidence.

4.2 Artefacts Extractions

Another parameter to judge the toolkit is the number of artefacts it extracted from the evidence. Table below shows the number of artefacts extracted by each toolkit.

4 X Smart Forensic Toolkits	Total Number of Artefacts
Magnet AXIOM	280748
Smartphone Forensic Professional	-
Belkasoft Evidence center X	30892
Oxygen Forensic Detective	263316

Table 9: Number of Artefacts Extracted

Magnet AXIOM and Oxygen Forensic toolkit clearly dominated in this perspective of comparison. Magnet AXIOM produced the most artefacts with Oxygen in the second place.

4.3 Timeline and Number of Categories

This table represents the number of categories each toolkit has produced to present artefacts e.g., social media, accounts, media etc. In addition, this table also represent that which tool provide timeline support.

4 X Smart Forensic Toolkits	Number of Categories	Timeline
Magnet AXIOM	10	No
Smartphone Forensic Professional	-	-
Belkasoft Evidence center X	11	Yes
Oxygen Forensic Detective	10	Yes

Table 10: Categories and Timeline Support

4.4 Category Wise Artefacts

Producing the exact number of artefacts generated by the toolkit in each category.

Artifacts/ Tools		OXYGEN	AXIOM	BELKASOFT	SPF Pro
Artifacts	Sub-Category				
Social Networking	Instagram		260		-
	TikTok		13	9	-
	Twitter		681		-
Chats	WhatsApp		20	12	-
	Telegram		26	225	-
	IMO		0		-
	Facebook Messenger		42		-
	LINE		45	107	-
	SKYPE		31	23	-
	Viber		10	10	-
	Discord		12		-
	iMessage/ SMS/ MMS		65	198	-
	Kik		19		-
Media	Pictures	31101	26783	16841	-

	Videos	279	1681	131	-
	Audios	1955	678		-
Email	Gmail				-
	Apple Mail		239	307	-
	Others				-
Documents	PDFs	81	2846	68	-
	Text	212	1679	667	-
	CSVs	1131	220	0	-
	Others	1887	63		-
Mobile	Call logs		83	1188	-
	Contacts		4	18	-
	Installed apps		93	192	-
	Device info		1		-
	Wi-Fi Profiles		5	1	-
Web Related	Safari		124	1166	-
	Google Maps		7		-
	Browsing history		2481	1166	-
OS			196262	8098	-
Custom	Archives		68	61	-
Cloud	Passwords and Tokens				-
Face (Matching) Recognition	Faces				-
Timeline	timeline		-	Y	-

Table 11: Artefacts Distribution

RESULTS

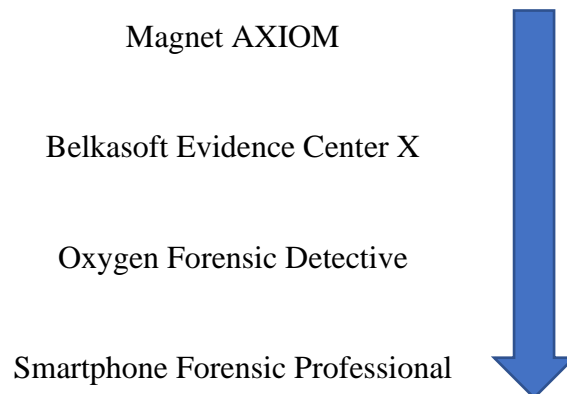
In this study, the researchers have applied four forensic tool kits on iOS13, which after contemporary investigations have shown the following results. The names of these four tools are as follows:

1. Magnet AXIOM
2. Smartphone forensic professional
3. Belkasoft Evidence Center X
4. Oxygen forensic detective

When the results were derived, the findings were concluded as stated below:

1. The maximum time was consumed by Magnet AXIOM.
2. In ranking the next less time consumed was by Oxygen.
3. Belkasoft Evidence Center X consumed 32 minutes and 24 seconds only.
4. While SPF Pro couldn't process the image.

Seeing the results in descending order, it is safe to state that the above-mentioned findings are as follows:

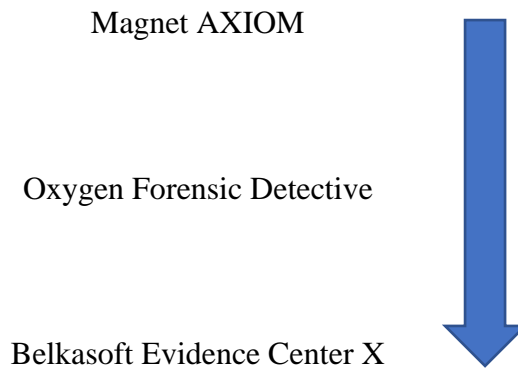


5.1 Most Artefacts

Four X smart forensic tool kits are used whose names are discussed above. Total number of artefacts extracted by Magnet AXIOM are 280748. While Belkasoft evidence center X and Oxygen Forensic Detective, the artefacts are counted as 30892 and 263316 respectively. In contrast to this, SPF Pro was unable to process the image. However, MOBILedit was also run on the iOS v13.4 image and failed to process it.

5.2 Time Constraints

The artefacts-based results relative to time as in, we can use Oxygen Forensic Detective if nothing else is present. Belkasoft Evidence Center X can be used instead of Oxygen Forensic Detective, and vice versa in case Oxygen Forensic Detective is not available.



5.3 Dashboard Representation

The dashboard presents the results of each toolkit. Magnet AXIOM has the comprehensive Dashboard. Similarly, Belkasoft Evidence Center X has well managed dashboard representing the result. Oxygen provided collection of results and one needs to search keyword based to know the actual number of results per sub-category. SPF Pro did not process the image. So, when well categorized results are required, AXIOM and Belkasoft Evidence Center X should be used.

5.4 Timeline Provision in Tool

Timeline is an important belief of virtual forensics. Numerous lasting crimes are basically sequences of movements leaving virtual footprints, that are to be tested little by little of their improvement and interrelation. Even if one offers with a single-factor crime, it usually has a

historical past and its implications constituting a coherent storyline that may be investigated on a temporal basis. That is why it's far frequently now no longer an exaggeration to mention that virtual forensics is all approximately resolving complicated timelines. This significance is the premise of the planned interest Belkasoft can pay to broaden a complicated timeline.

Toolkit	Number of Categories	Timeline
Magnet AXIOM	10	No
Smartphone Forensic Professional	-	-
Belkasoft Evidence Center X	11	Yes
Oxygen Forensic Detective	10	Yes

Table 12: Timeline Support and Categories by Toolkits

Which tool kits perform what function is shown by the graph where it is evident that two of these have performed according to the mark, but one has not. Thus, if a formal timeline is needed, Belkasoft Evidence Center X and Oxygen Forensic Detective may be executed. If we want to examine the tool kits according to categories, we need to see which one is showing more of them, for instance, in the above-mentioned table Belkasoft Evidence Center X shows more categories.

DISCUSSION AND FUTURE RECOMMENDATIONS

6.1 Conclusion

This is the comparative analysis of 4x forensic tool kits on the iOS 13.4. The forensic analysis based on the qualitative and quantitative values. This comparative analysis is for the Law Enforcement Agencies (LEAs) to better understand the use of tool under certain circumstances to produce efficient results.

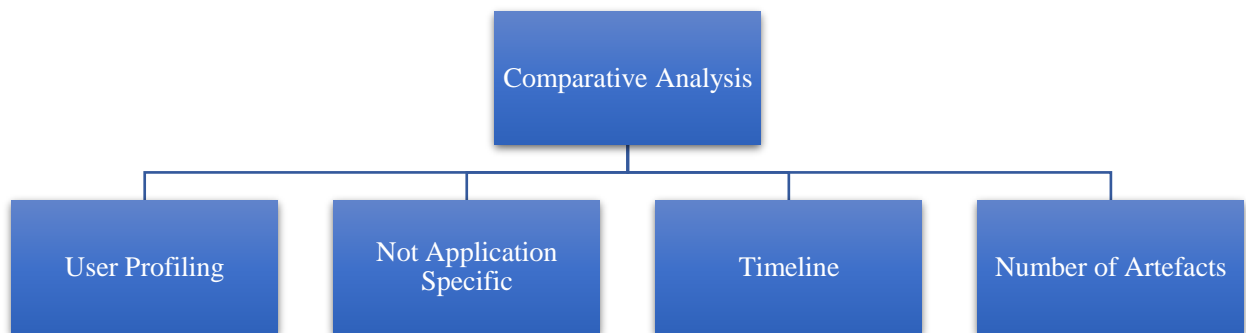


Figure 3: Comparative Analysis

Results are based on the user profiling done by the toolkit. Results are not application specific, and so is the timeline of the artefacts produced in the evidence source. Plus, another comparative parameter is the number of artefacts extracted by the tool from the same evidence resource file.

6.2 Limitations

Limitations as per this research study is concerned are discussed as follows:

- Computation power
- Limited tool kits

- Only one iOS version was used

If these limitations are minimized, a lot can be worked on in much better way. There can be a solution where instead of these some related items can be observed which help in easing the work. These limitations can also be taken as the gaps which can be fulfilled in the future studies.

6.3 Future Recommendations

As the researcher has done the study on 13.4, in future the same work can be done on 15.5. Research on this particularity is missing. It may also be treated as a gap in coming-up research studies. We can use multiple images to extract comprehensive tools. We can take images from different and various extensions to check which extension shows all progressed results. By looking at each tool kits we may look at the time consumption of each of it on each given extensions, we can extract an appropriate extension that the images may come under so and so extension in future work. By using various tools, we may take images of iOS. We have taken one single image by using one tool, in future research study, we may take multiple images by putting in use one single appropriately functioning tool.

REFERENCES

- [1] Statista, 2021. [Online]. Available: <https://www.statista.com>.
- [2] S. KEMP, 2021. [Online]. Available: <https://datareportal.com/reports/digital-2021-united-kingdom>.
- [3] Samsung, "your-phone-is-now-more-powerful-than-your-pc," 2021. [Online]. Available: <https://insights.samsung.com/2021/08/19/your-phone-is-now-more-powerful-than-your-pc-3/>.
- [4] A. R. MALLEY, "A COMPARISON ANALYSIS OF SAVED SNAPCHAT VIDEO FILES ON ANDROIDS VS IPHONES," 2021.
- [5] T.-C. C. L.-M. Min-Hao Wu, "Digital Forensics Security Analysis on iOS Devices," *Journal of Web Engineering*, 2021.
- [6] R. W. a. H. Chi, "A framework for validating aimed mobile digital," 2018.
- [7] N. A. M. A. A. A. T. A. Asia ALJAHDALI, "Mobile device forensics," *Romanian Journal of Information Technology and Automatic Control*, pp. 81-96, 2021.
- [8] J.-U. L. a. W.-Y. Soh, "Comparative analysis on integrated digital," June 2020.
- [9] K. M. O. a. G. Morison, "Forensic analysis of kik messenger on iOS devices.," *Digital Investigation*, pp. 40-52, 2016.
- [10] M. A.-H. a. A. AlShidhani, "smartphone Forensics Analysis: A Case Study," *International Journal of Computer and Electrical Engineering*, pp. 577-579, 2013.
- [11] U. S. Nitesh K. Bharadwaj, "An intelligent approach for examining and detecting target data fragments in suspected large storage drives," 2019.
- [12] B. L. Y. S. Y. Zhang, "Android Encryption Database Forensic Analysis Based on Static Analysisdetecting target data fragments in suspected large storage drives," 2020.

- [13] T. C. E. M. P. S. Konstantia Barmपालou, "Current and Future Trends in Mobile Device Forensics: A Survey," 2018.
- [14] M. Yates, "Practical investigations of digital forensics tools for mobile devices," 2010.
- [15] F. D. A. G. A. L. G. M. V. O. Rosamaria Berte, "Fast smartphones forensic analysis results through mobile internal acquisition tool and forensic farm," 2009.
- [16] X. L. Nathan Scrivens, "Android digital forensics: data, extraction and analysis," 2017.
- [17] O. B. Tahani Almeahadi, "Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics," 2019.
- [18] SANS, "FOR585 | smartphone FORENSIC ANALYSIS IN-DEPTH," 2020.
- [19] N. R. Roy, A. K. Khanna and L. Aneja, "Android phone forensic: Tools and techniques," 2017.
- [20] M. Raji, H. Wimmer and R. J. Haddad, "Analyzing Data from an Android smartphone while Comparing between Two Forensic Tools," 2018.
- [21] J. Zheng, Y.-A. Tan, X. Zhang, C. Liang, C. Zhang and J. Zheng, "An Anti-Forensics Method against Memory Acquiring for Android Devices," 2017.
- [22] I. R. ., B. F. M. Rusydi Umar, "Live forensics of tools on android devices for email forensics," 2019.
- [23] W. P. A. K. K. L. Htar Htar Lwin, "Comparative Analysis of Android Mobile Forensics Tools," 2020.
- [24] S. M. Amukelani Ngobeni, "Towards Enhancing Security in Android Operating Systems – Android Permissions & User Unawareness," 2019.
- [25] Statista, 2021. [Online]. Available: <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>.
- [26] K. A. G. T. M. R. Abdul Wahid, "Anti-theft Cloud Apps for Android Operating System," 2014.
- [27] M. A. S. A. W. A. M. H. S. H. Y. Saba Arshad, "SAMADroid: A Novel 3-Level Hybrid Malware Detection Model for Android Operating System," 2018.

- [28] M. A. S. A. S. H. M. A. W. Saba Arshad, "Towards 3-level hybrid security model for Android Operating Systems," 2017.
- [29] T. N. Osama Sohail, "Anti-theft cloud application for android operating system (Nougats)," 2018.
- [30] N. M. D. Sneha C Sathe, "Data acquisition techniques in mobile forensics," 2018.
- [31] Q. L. P. Z. Z. C. Peijun Feng, "Private Data Acquisition Method Based on System-Level Data Migration and Volatile Memory Forensics for Android Applications," 2019.
- [32] E. F. Aiman Al-Sabaawi, "A Comparison Study of Android Mobile Forensics for Retrieving Files System," 2019.
- [33] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," 2013.
- [34] J. H. F. Dian, "Efficient Sensitive Data Gathering with Forensic Analysis of Android Operating System," 2019.
- [35] N. M. Nirneeta Gupchup, "A Systematic Survey on Mobile Forensic Tools Used for Forensic Analysis of Android-Based Social Networking Applications," in *Data, Engineering and Applications*, 2019.
- [36] F. B. S. O. Tina Wu, "Digital forensic tools: Recent advances and enhancing the status quo," 2020.
- [37] W.-Y. S. Jae-Ung Lee, "Comparative analysis on integrated digital forensic tools for digital forensic investigation," 2020.
- [38] A. H. M. K. M. Shakir, "Comparative Analysis & Study of Android/iOS MobileForensics Tools," 2021.
- [39] N. K. B. a. Gyana Ranjana Panigrahi, "A Review on: the Rise in Cyber Forensics &," 2021.
- [40] K. J. B.-K. R. Choo, "Effectiveness of Mobile Wiping Applications," in *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures*, 2021.
- [41] N. I. W.-S. SeokByunOc-YeubJeon, "A method of forensic authentication of audio recordings generated using the Voice Memos application in the iPhone," *Forensic Science International*, 2021.
- [42] U. Yasin, "Comparative Analysis of Andorid Forensic Tools," Islamabad, 2021.

- [43] R. T. O. M. A. R. M. D. J. K. Alhassan, "Comparative Evaluation of Mobile," in *Proceedings of the International Conference on Information 2018*, 2018.
- [44] I. R. Guntur M. Zamroni, "Mobile Forensic Tools Validation and Evaluation," *International Journal on Advanced Science Engineering and Information Technology*, pp. 2088-5334, 2020.
- [45] M. J. Raghad Khweiled, "An Improved Framework for Cyberbullying," *Journal of Xi'an University of Architecture & Technology*, pp. 1006-7930, 2021.
- [46] N. Y. K. B. W. K. S. K. S. Jung Hyun Ryu*, "Analysis of a Third-Party Application for Mobile," *Journal of Information Processing System*, 2018.
- [47] I. R. G. M. Z. Rusydi Umar, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *International Journal on Advanced Science, Engineering and Information Technology*, 2018.
- [48] W. I. ., I. W. B. S. M. a. S. R. Anoshia Menahil, "Forensic Analysis of Social Networking Applications on an," 2021.
- [49] H. T. I. Riadi, "Forensic Analysis of Android-based WhatsApp Messenger Against Fraud Crime," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 8(1): 89-97, 2019.
- [50] R. U. A. F. Imam Riadi, "Forensic Tools Performance Analysis on Android-basedBlackberry Messenger using NIST Measurements," *IJECE*, 2018.
- [51] L. K. S. A. A. C. P. Praneta Anand, "Comparative study on data extraction and acquisition tools for Facebook messages," *International Journal of Scientific Research in Computer Science Applications and Management Studies*, 2019.
- [52] P. K. a. S. R. S. Animesh Kumar Agrawal, "Comparative Study of Mobile Forensic Tools," in *Advances in Data and Information Sciences. Lecture Notes in Networks and Systems*, 2018.
- [53] A. K. A. P. K. Sumit Sah, "Physical Data Acquisition from Virtual Android Phone Using Genymotion," 2019.
- [54] Z. H. M. Azimuddin Khan, "COMPARATIVE STUDY OF VARIOUS DIGITAL FORENSICS LOGICAL ACQUISITION TOOLS FOR ANDROID smartphone'S

INTERNAL MEMORY," *International Journal o Advance Research in Computer Science*, 2018.

- [55] D. E. A. E. Mohammad Dweikat, "Digital Forensic Tools Used in Analyzing cyber crime," *Journal of University of Shanghai for Science and Technology*, 2021.
- [56] S. P. N. D. V. S. Samarjeet Yadav, "Forensics Analysis of WhatsApp in Android Mobile Phone," in *Proceedings of the International Conference on Advances in Electronics, Electrical & Computational Intelligence (ICAEEEC) 2019*, 2020.
- [57] L. A. A. M. O. Mohammad Shadeed, "Forensic Analysis of “WhatsApp” Artifacts in Android without Root," *Advances in Science, Technology and Engineering Systems Journal*, 2021.
- [58] R. U. A. Y. Rauhulloh Ayatulloh Khomeini Noor Bintang, "Assess of Forensic Tools on Android Based Facebook Lite with the," *Scientific Journal of Informatics*, 2021.
- [59] belkasoft, "x," belkasoft, 2022. [Online]. Available: <https://belkasoft.com/x>.
- [60] o. forensic, "home," oxygen forensic, 2022. [Online]. Available: <https://www.oxygen-forensic.com/en/>.
- [61] magnetforensics, "for-law-enforcement," magnetforensics, 2022. [Online]. Available: <https://www.magnetforensics.com/for-law-enforcement/>.
- [62] salvationdata, "smartphone-forensic-system-professional," salvationdata, 2022. [Online]. Available: <https://www.salvationdata.com/business-list-page/smartphone-forensic-system-professional/>.

USER MANUALS

AXIOM

1. Fill Case Details

CASE DETAILS

CASE INFORMATION

Case number: Case-105

Case type: Select case type...

LOCATION FOR CASE FILES

Folder name: AXIOM - May 21 2022 222611

File path: C:\Users\Forensic\Documents\AXIOM [BROWSE](#)

Available space: 77.19 GB

LOCATION FOR ACQUIRED EVIDENCE

Folder name: AXIOM - May 21 2022 222611

File path: C:\Users\Forensic\Documents\AXIOM [BROWSE](#)

Available space: 77.19 GB

SCAN INFORMATION

SCAN 1

Scanned by: Haq Nawaz

Description:

[GO TO EVIDENCE SOURCES](#)

Figure 3: Insert Case Details

As shown in the above figure, Case Details are to be entered here. Case Details include the case information which has.

- I. Case Number
- II. Case Type

Furthermore, information regarding "Location for Case Files" is to be filled. here, File Path can be browsed as well.

Next step will be to add information regarding the "Location For Acquired Evidence". Here also, Folder name and File Path are to be selected.

2. Select "EVIDENCE SOURCES"

After filling in the Case Details, next step is to select the "Evidence Source" i.e. from where the evidence was taken. In this case, "Mobile" is selected as we have worked on mobile device, as shown in the below figure:

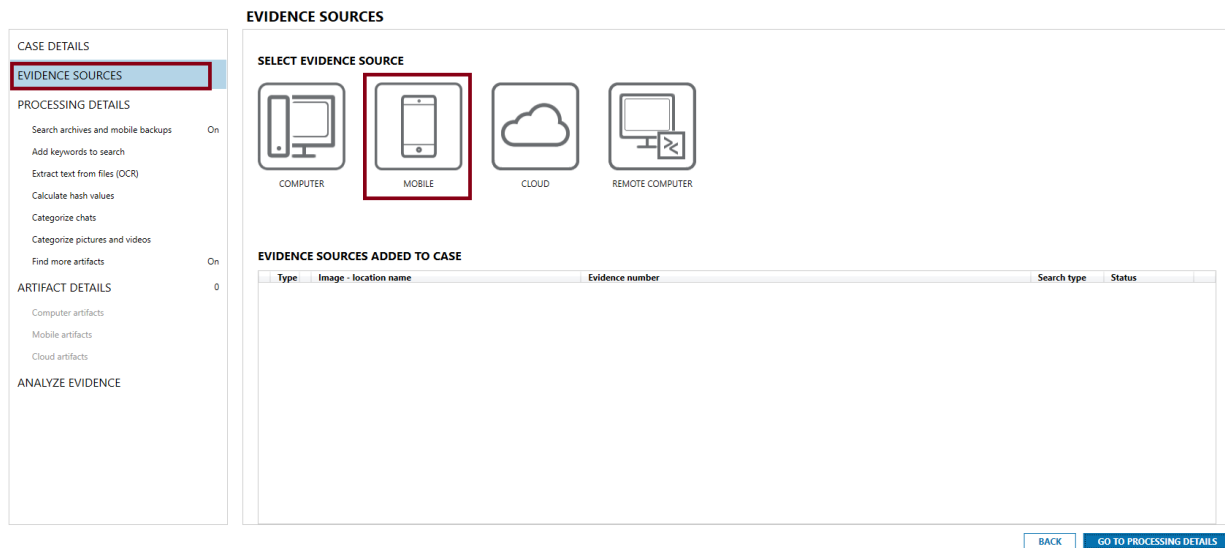


Figure 4: Select Mobile as Evidence Source

3. Select Type of Evidence Sources:

As shown in the following figure, select the type of evidence source. In this case, we will select iOS.

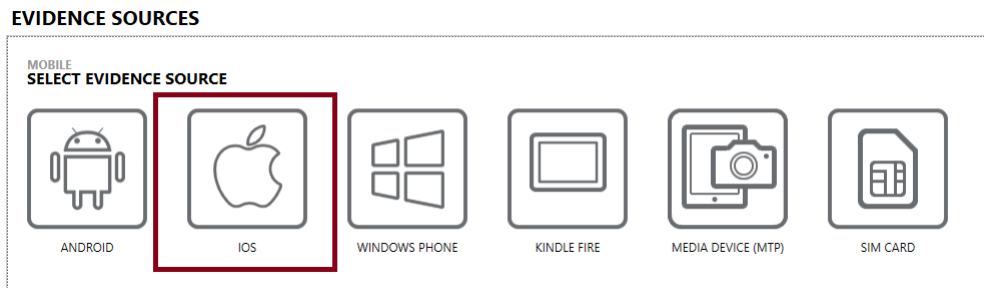


Figure 5: Select iOS as Evidence Source

4. Load the Evidence

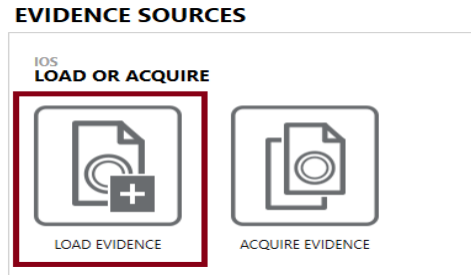


Figure 6: Load the Evidence

5. Next step is to Load the image by selecting the following icon

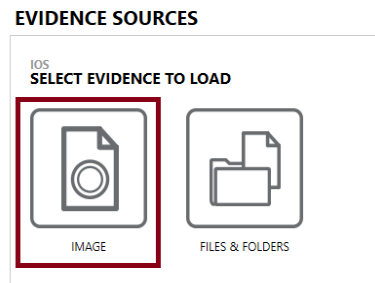


Figure 7: Load the Image

6. Next, a pop-up window will appear as shown in figure to select the image

EVIDENCE SOURCES

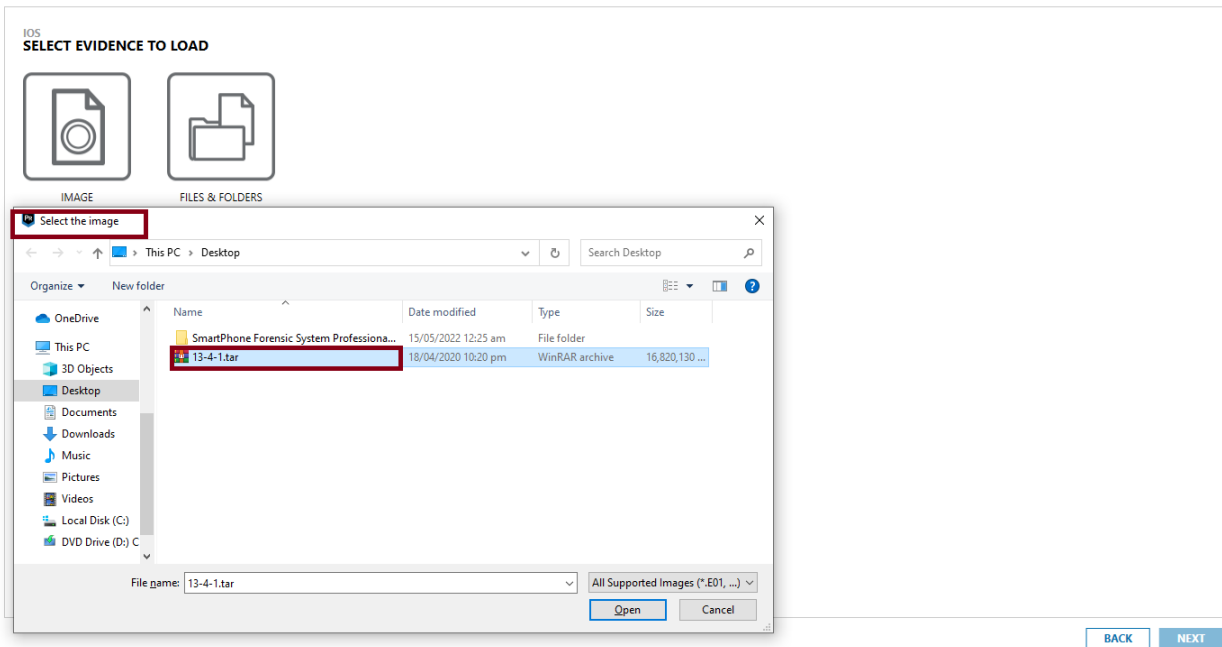


Figure 8: Browse to Select the Image

7. Image is selected as evidence as shown below

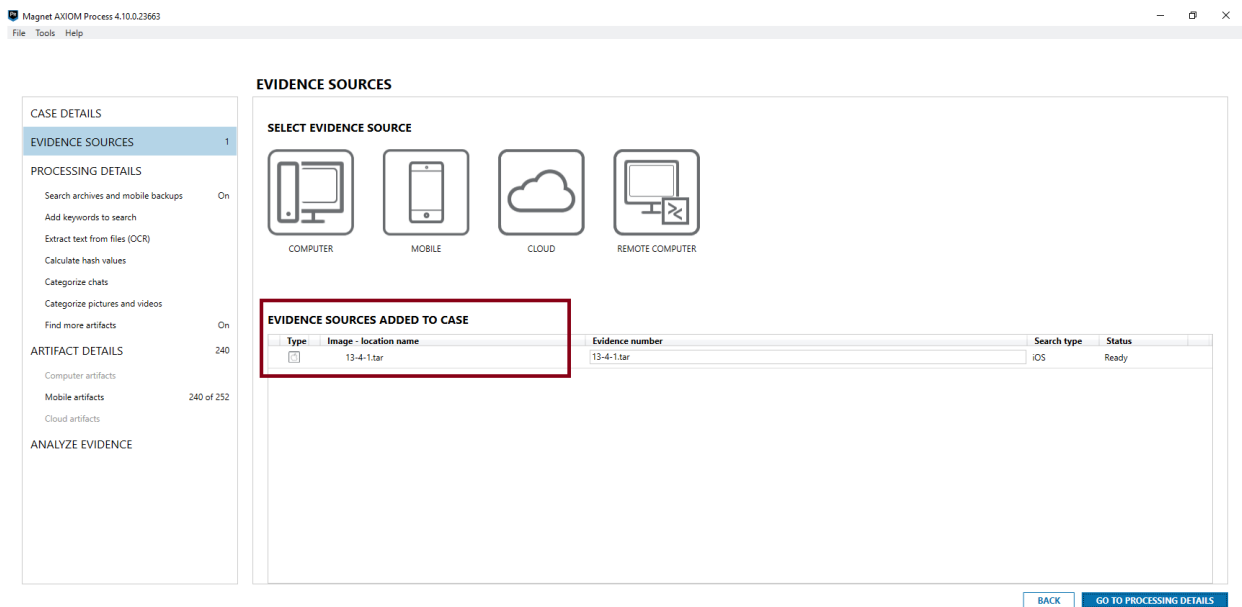


Figure 9: Image Selected as Evidence Source

8. Select Artifact Details, as it is a mobile device so Mobile Artifacts is selected

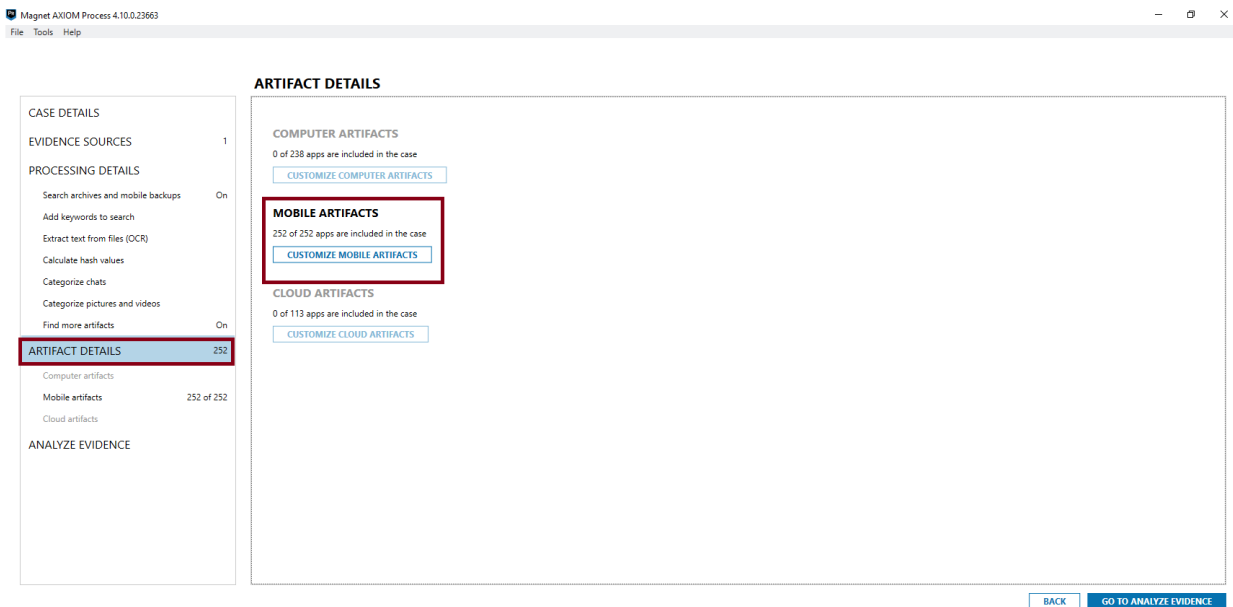


Figure 10: Select Mobile Artifact as Artifact Details

9. After that, Evidence is analyzed by selecting “Analyze Evidence” as shown in figure below.

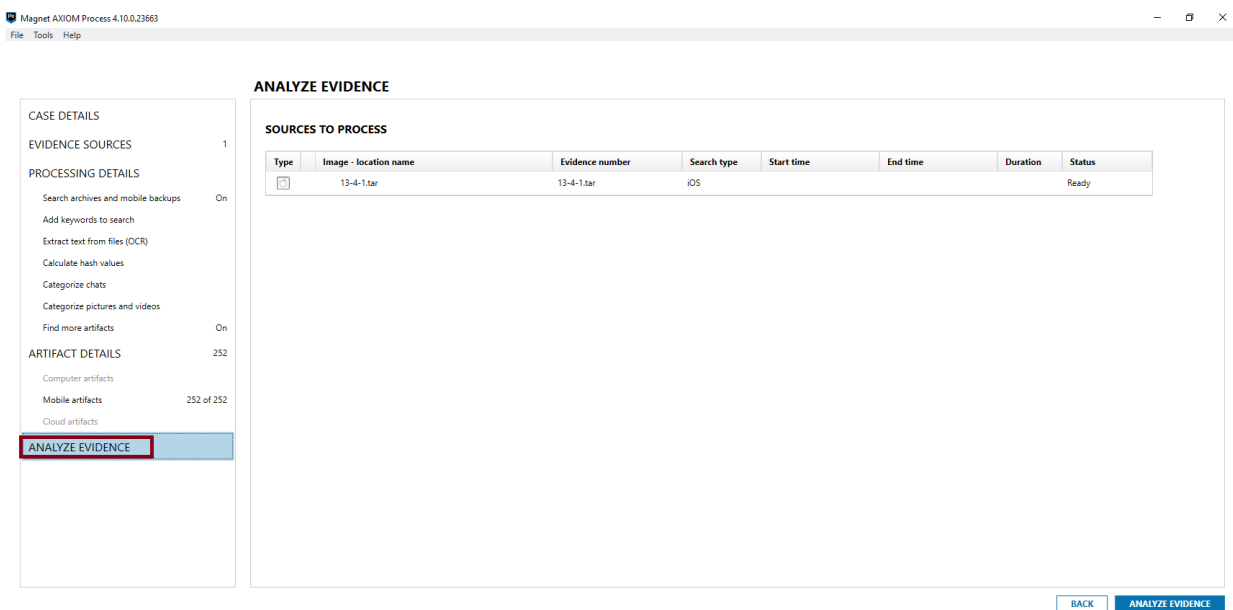


Figure 11: Analyze Evidence



10. Magnet AXOM tool is applied to analyze.

11. Here, information regarding case overview, evidence overview and place to start is present.

We can clearly see each detail in the figure below.

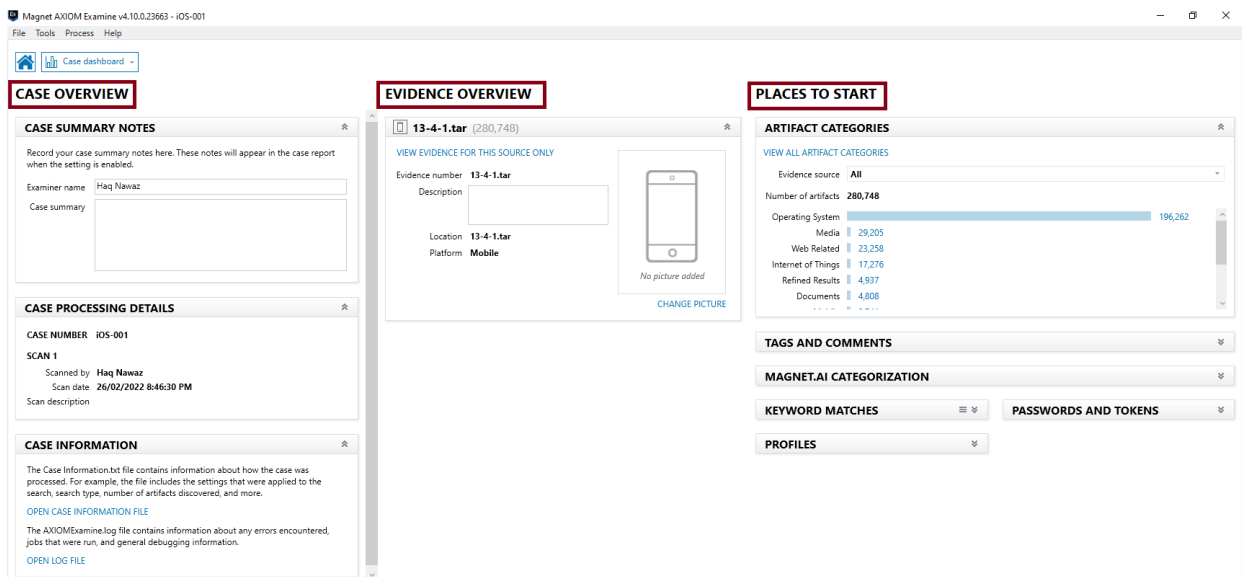


Figure 12: Case Dashboard Displayed

BELKASOFT

1. Insert the details as shown below

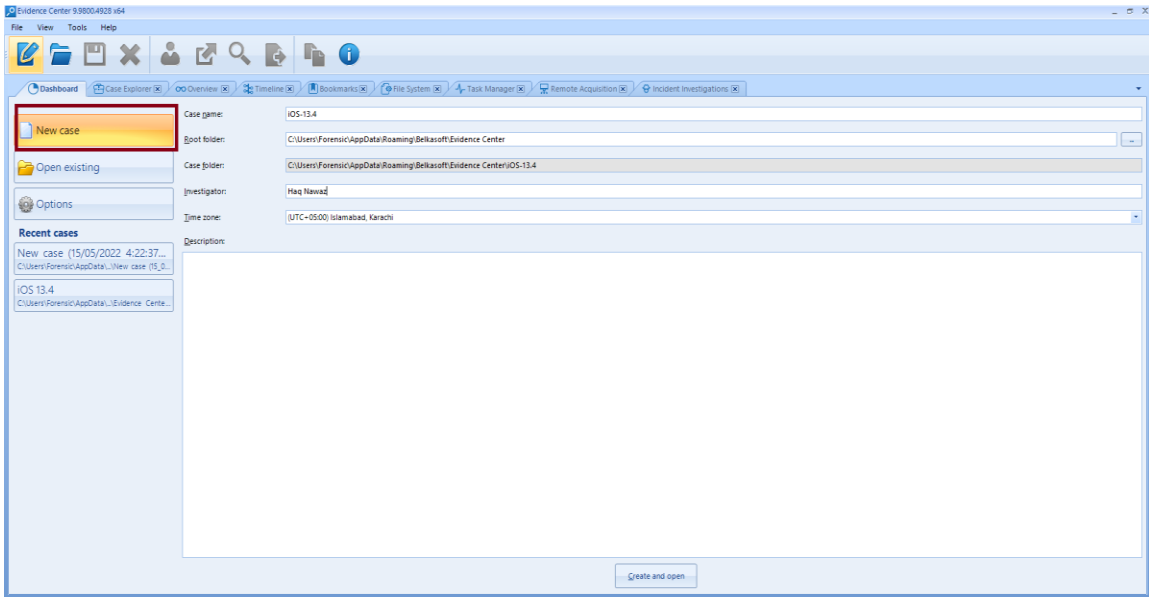


Figure 13: Add Details of New Case

2. Select the mobile image, browse the image as shown

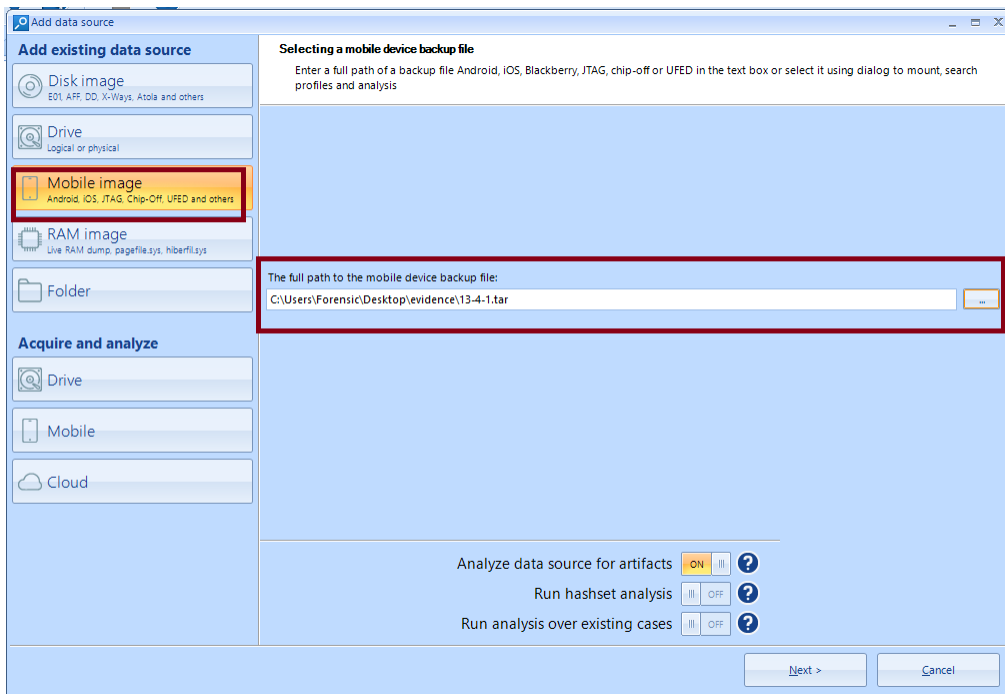


Figure 14: Browse and Select the Mobile Image

3. Here, list of options is given in which select the items that you would like to search for.

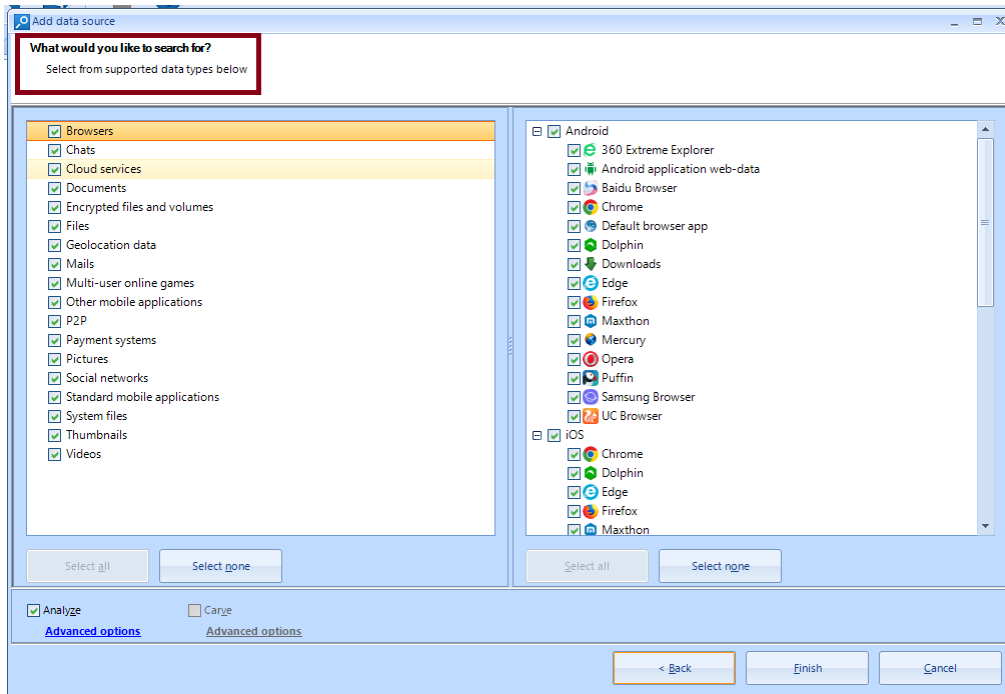


Figure 15: Select the Options to Search

4. Select the image selected and all its details will be shown as below.

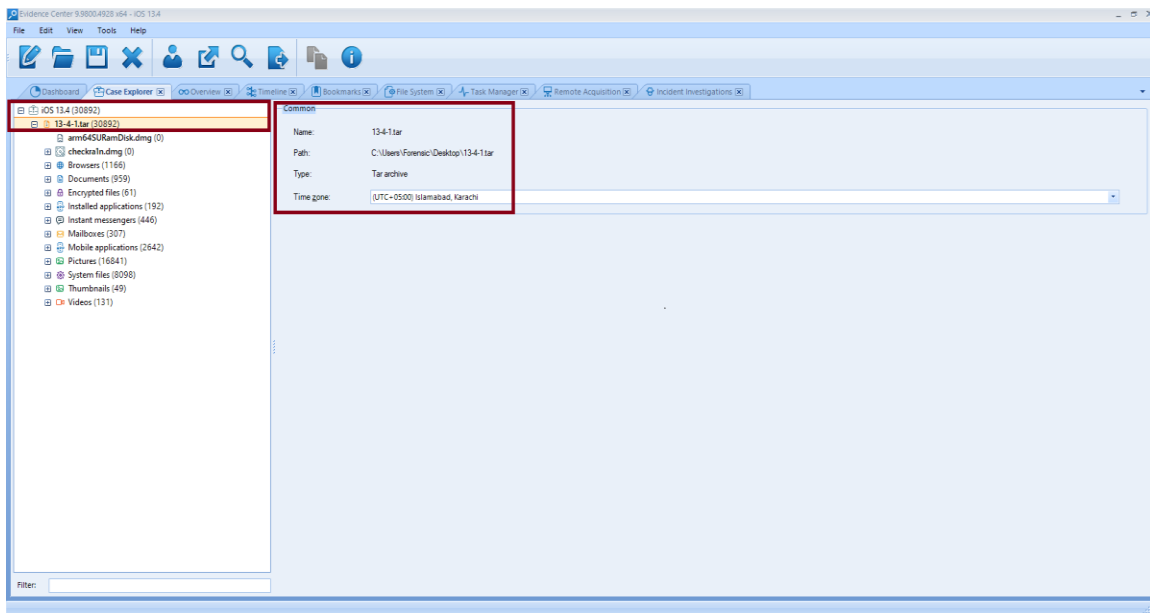


Figure 16: Details of Selected image

OXYGEN

1. Following options are shown on the dashboard as shown

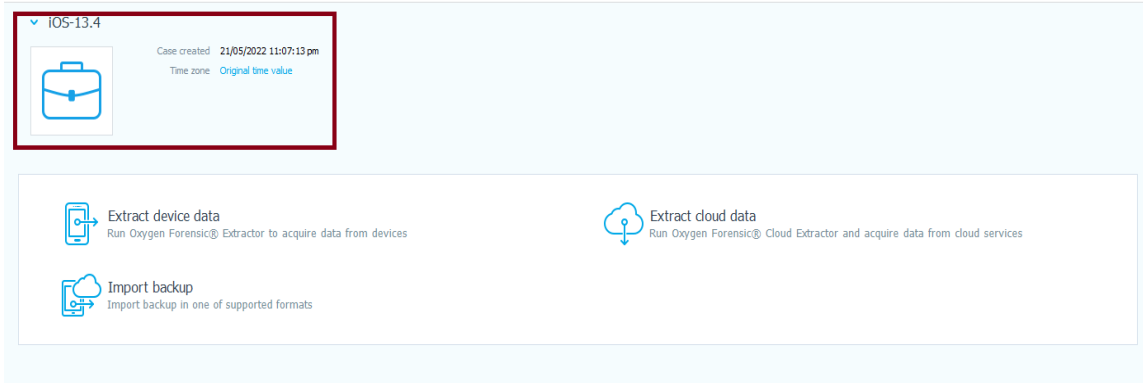


Figure 17: OXYGEN Dashboard

2. After selecting “Import Backup” option, a pop-up window will appear as shown. Select the folder which you want to explore.

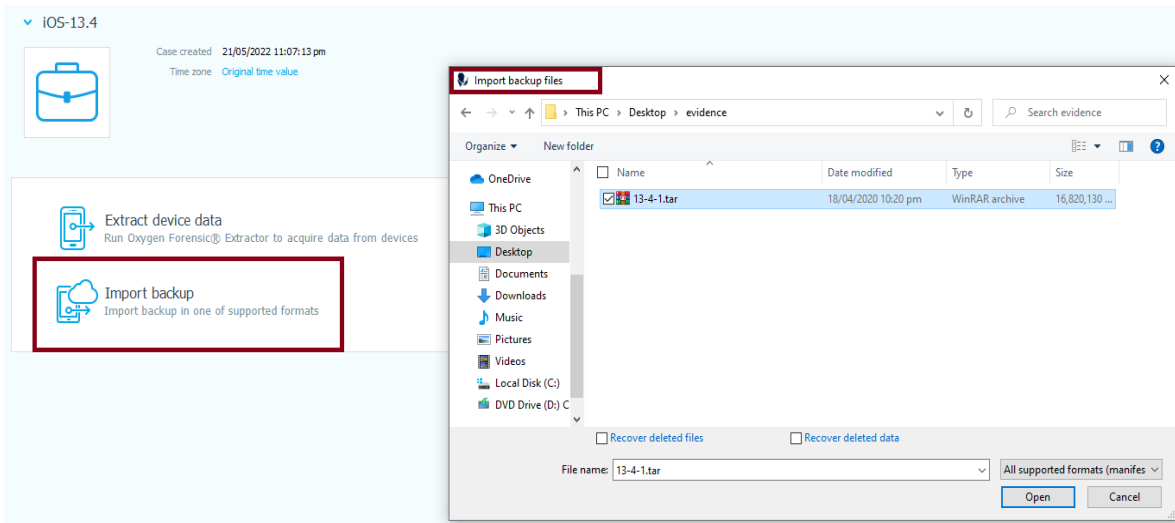


Figure 18: Importing Backup

3. As we are working on iOS so we will select the following option as shown.

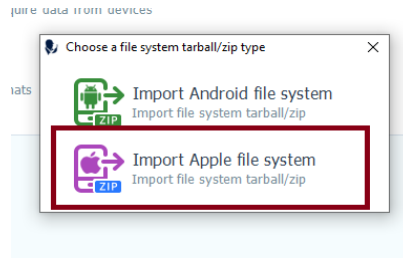


Figure 19: Select Import Apple File System

4. After selecting the “Import Apple filesystem”, it will start extracting files as shown.

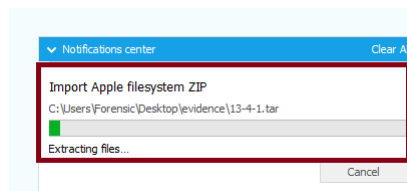


Figure 20: File Extraction

5. Files will be extracted as shown below.

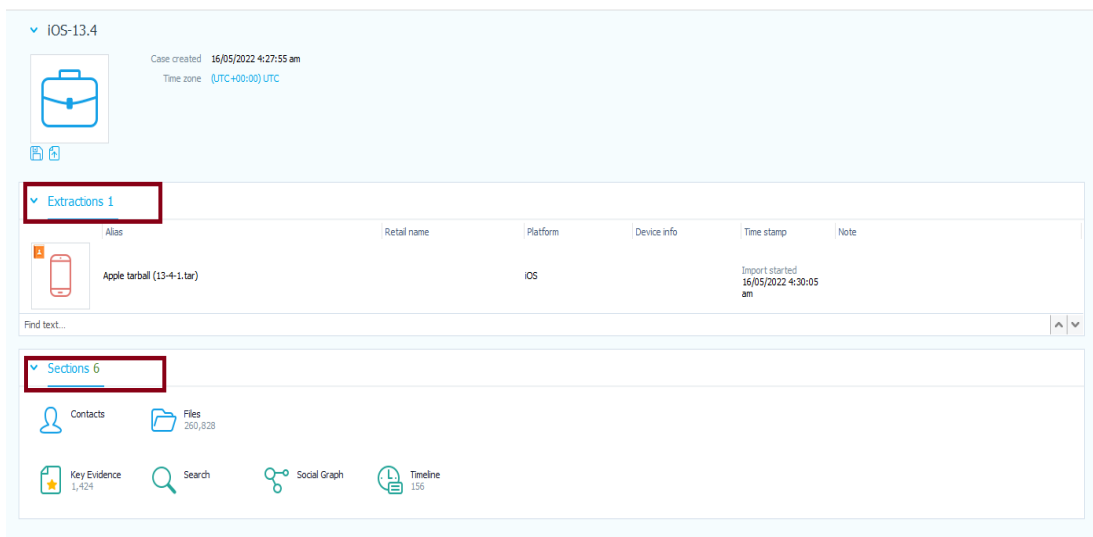


Figure 21: Extracted Files Dashboard

6. Following results are established after applying OXYGEN tool.

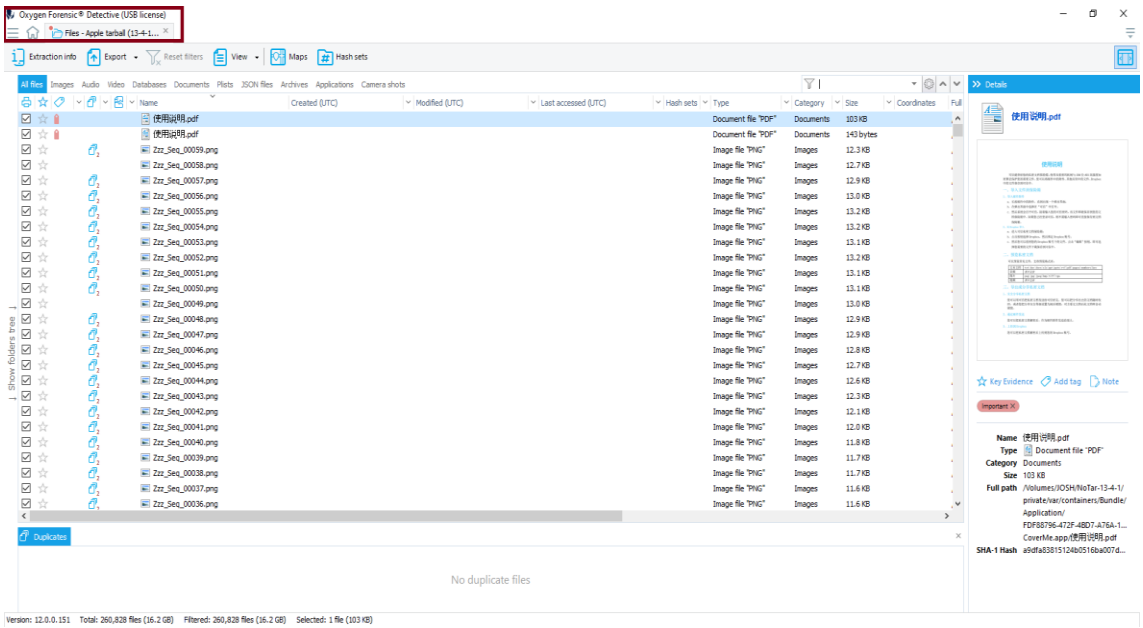


Figure 22: Extracted Results