Digital Forensic Investigation of an iOS Mobile Phone Using iTunes and iCloud Backup

Robinson Tombari Sibe[1,*], Adewale Alayegun[2]
[1]Rivers State University, Nigeria, Digital Footprints Ltd, Nigeria
[2]Digital Footprints Ltd, Nigeria
Emails: robinson.sibe@ust.edu.ng; adewale.alayegun@digitalfootprints.ng

Abstract

The growing popularity of iOS devices and the increasing complexities of forensic investigation of these devices requires more research attention. Due to the complex encryption and closed nature of iPhones, it is inherently complicated to perform digital forensic investigations. While there are many extraction and analysis methods for iphone, the most comprehensive (but most complex) is the full physical acquisition. However, the likelihood of acquiring physical extraction of an iPhone is becoming more challenging as Apple improves on its mobile technology, with more emphasis on privacy and security. Factors such as the adoption of full file and disk encryption, and secure enclave technology poses serious challenge to forensic investigators. This paper explored alternatives, by extracting and analyzing valuable evidential artifacts using iTunes and iCloud, unique to the iOS environment. This research involved the forensic examination of an iPhone XR running on iOS 17.5, using Oxygen Forensic Device Extractor v2.13.1, with each step documented. The study uncovered several artifact locations and provided a brief description of each, and their usefulness in a forensics analysis. Some of these include user-generated content, system artifacts, application data, and cloud interactions, such as contacts, SMS data, call history, media files, database, browser data, application data and others, that could prove vital in solving a case. This study made valuable contribution to the body of knowledge by highlighting specific challenges faced in iOS forensics and recommending a methodical approach to examining and analyzing evidential artifacts using iTunes and iCloud. The paper also addressed the gap in available literature in iOS forensics.

Keywords: Digital Forensics; Mobile Forensics; iOS Forensics; iOS; Forensic Acquisition; Cybersecurity; Digital Investigation; iTunes; iCloud

1. Introduction

Globally, mobile phone adoption has surged over the last decade. In 2016, there were about 3.7 billion smart phone mobile network subscriptions in the world. By 2023, this figure had risen to almost 7 billion [1]. Statistics by the International Telecommunication Union [2] show that globally, about 5.228 billion persons (representing 78.1% of world population) own a mobile phone. In terms of brand dominance, the top three smart phone brands (in terms of number of shipments) are Samsung at number one, Apple at number two, and Xiaomi at number three. Specifically, in Q3 of 2024, Samsung accounted for 19% of Global Smartphone Shipments Market Share, Apple accounted for 17%, while Xiaomi accounted for 14%. In terms of numbers, Samsung shipped 55 million smart phones globally, with Apple shipping 45.5 million, and Xiaomi shipping 42.3 million smartphones, respectively [3]. From an Operating System (OS) perspective, as at Q2 2024, Android was the dominant mobile OS, with a market share of 71.65%. The closest to this was iOS, with a market share of 27.62% [4]. It is noteworthy that while Android runs on most smart phones, iOS only runs on Apple devices, and this is a major reason behind the market dominance of Android.

As indicated by the market share statistics above, Apple devices continued to gain market dominance, following closely behind Samsung. This makes iOS the second most popular mobile Operating System, and therefore of interest in digital forensics. The ubiquity of iOS devices in contemporary society has brought about an unprecedented surge in digital interactions, underscoring the need for a sophisticated understanding of forensic

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

methodologies tailored to Apple's ecosystem. As these devices become increasingly popular, the demand for robust digital forensic investigation techniques intensifies. Apple iOS is renowned for its complex design and closed features, with emphasis on privacy and security. While these features are desirable from an information governance and security standpoint, however, it poses complex challenges from a mobile forensic perspective [5]. This research interrogates these complexities and challenges inherent in the digital forensic investigation of iOS devices, highlighting methodologies crucial for extracting and interpreting digital evidence within this distinct ecosystem.

The inherent complexity of iOS devices is underscored by Apple's adoption of security-by-design. With emphasis on safeguarding user data, iOS employs intricate security mechanisms, including encrypted file systems and the incorporation of a secure enclave within the device architecture [5,6]. These features, while pivotal for user protection, present formidable challenges for digital forensic investigators aiming to access and analyze device data. This research investigated the complexities surrounding iOS digital forensics, offering a comprehensive guide for practitioners and scholars alike.

To comprehend the complexities of iOS digital forensics, it is imperative to consider the unique characteristics of Apple's ecosystem. The closed nature of iOS and the stringent security measures implemented by Apple necessitates a complex and tactical approach to digital investigations. As Apple's devices are designed to prioritize user privacy, forensic investigators encounter obstacles such as encrypted backups, encrypted communication channels, and secure enclave protection [5,7]. The most comprehensive method of acquisition for iOS is the physical acquisition. However, due to the complexities mentioned, it is becoming extremely difficult for mobile forensic tools to perform full physical acquisition on modern apple devices, which frustrates the investigative process. These challenges form the crux of the investigation undertaken in this paper, as the researchers delved into methodologies capable of overcoming these barriers and extracting valuable digital evidence.

The forensic toolkit includes both hardware and software-based analysis tools. Hardware tools, such as those that facilitate the extraction of physical images from iOS devices, are instrumental in circumventing encryption barriers and gaining access to raw data [8]. Complementing this, software-based analysis tools play a pivotal role in interpreting the acquired data, deciphering application artifacts, and reconstructing user activities. By synthesizing these methodologies, this research aims to offer a holistic approach to iOS digital forensics.

Digital forensic investigation is not confined to the examination of device-resident data alone; it also encompasses the intricate interplay between iOS devices and evidential artifacts stored in the cloud. In an era where cloud storage and synchronization have become ubiquitous, understanding the footprint left by iOS devices in cloud environments is quite important. Apple’s iCloud serves as a repository for a myriad of user data, ranging from photos to app backups. Navigating this dynamic landscape requires an adaptive forensic strategy capable of traversing the boundaries between device and cloud [9]. Specifically, this study explores the alternative to the challenging full physical acquisition, by presenting a methodical alternative of acquiring and analysing forensic artifacts from iTunes backup and iCloud.

Finally, despite the growing popularity of iOS, there are only a handful of scholarly research on iOS forensics. For instance, the researchers in this study did a quick Google Scholar search for Peer review articles on iOS forensics published since 2018 and got only a few directly relevant articles. Therefore, this research is a valuable contribution to the scanty scholarly publications on iOS forensics. As digital forensic investigations evolve with technological advancements, this research contributes not only to the understanding of iOS digital forensics but also to the broader field of digital investigation methodologies. By bridging theoretical foundations with practical insights, the ensuing sections of this paper will provide a detailed exploration of methodologies, challenges, and solutions pertinent to the digital forensic investigation of iOS Mobile Phone, ensuring that practitioners and researchers are equipped with the knowledge needed to navigate the intricacies of this distinct ecosystem.

2. Literature Review

A. Overview of Digital Forensics

Digital forensics is a branch of forensic science that deals with the identification, preservation, examination, and analysis of digital evidence in investigations. The ubiquity of smartphones and their role as repositories of critical information has heightened the importance of mobile forensic investigations within the broader field of digital forensics [8]. It encompasses a systematic approach to collecting and analyzing electronic evidence to uncover facts related to cybercrime, fraud, or other digital incidents [9]. It involves the application of forensic techniques to collect, preserve, and examine data stored on various digital devices. Digital Forensics is a methodical discipline requiring defined steps and procedure for evidence acquisition, preservation, analysis, and reporting [10,11]. For instance, one such rule is to ensure original evidence is not tampered with - this is the golden rule for the forensic analysis of digital evidence [12].

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

Within the realm of digital forensics, mobile forensic investigations focus specifically on extracting and analyzing data from mobile devices through the application of logical techniques to obtain information from mobile phones [13]. From the forensics perspective, mobile devices such as iPhone could be a treasure trove of evidence, containing valuable artefacts that could be vital in solving a case. However, the dynamic nature of mobile technology, coupled with the diverse range of devices and operating systems, poses unique challenges for investigators. Among the various mobile operating systems, iOS, developed by Apple Inc., presents distinct challenges due to its closed ecosystem and robust security features [5]. The forensic analysis of iOS devices requires specialized methodologies and tools to navigate Apple's security measures and extract relevant data [14].

Efficient iOS forensic investigations rely on the knowledge and expertise of the forensic examiner who performs forensics on an iPhone. Avancha [15] submitted that the examiner must be knowledgeable enough about every aspect of the device, including the different models that have been introduced over time, as well as the internal workings of the iPhone, operating system, file system structure, location of common artifacts, and so on. Moreso, the utilization of specialized tools designed to overcome the unique challenges posed by Apple's ecosystem is essential. Proprietary solutions such as Cellebrite, Oxygen Forensics, Belkasoft, and Magnet AXIOM have gained prominence for their ability to acquire and analyze data from iOS devices [16]. Open-source tools, including libimobiledevice and iLEAPP, offer alternative avenues for forensic professionals to extract valuable artifacts from iPhones and iPads [17].

The closed nature of the iOS ecosystem and Apple's commitment to user privacy present formidable challenges for digital investigators. Features like end-to-end encryption and restricted access to certain data types necessitate innovative approaches, including the analysis of iCloud backups and the exploitation of known vulnerabilities [18]. Recent developments in the field highlight the increasing significance of cloud-based forensics in iOS investigations. As users store more data in the cloud, accessing information from services like iCloud becomes paramount for a comprehensive digital forensic examination [19]. Additionally, the integration of machine learning and artificial intelligence in iOS forensic analysis is gaining traction, offering potential breakthroughs in automating the identification of patterns in large datasets [20].

The legal landscape surrounding digital forensics, particularly in iOS investigations, is evolving. Court decisions regarding the admissibility of evidence obtained from mobile devices impact the forensic process. Researchers emphasize the importance of adhering to strict ethical standards, laid down forensic methodology and best practices to ensure the reliability and validity of evidence presented in legal proceedings [10,21]. Paglierani *et al.* [22] outlined four major rules to be followed in any forensic investigation:

1. Authenticity: The evidence can be linked to a specific individual or incident.
2. Admissibility: The evidence was legally obtained and can be admitted in a court.
3. Completeness: The evidence is not partial; it includes all available information.
4. Reliability / Accuracy: The evidence collection procedure is explainable.

B. Forensic Method

Adoption of well-tested and clearly defined forensic procedures can be a great start to conducting a forensically sound mobile device investigation. Digital forensics involve defined protocols and procedures for seizure, evidence acquisition, preservation, and analysis, to ensure integrity and reliability of evidential items. There are several models and guidelines for digital forensic process [10]. For instance, the NIST.SP.800-101r1 - Guidelines on Mobile Device Forensics [23], Forensic process includes:

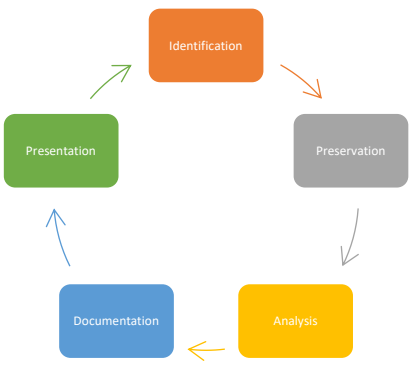

Figure 1. Digital Forensic process

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

1. **Identification:** Identification that includes search and seizure are critical initial steps in the mobile forensic process. From a mobile forensic point of view, this step involves the recognition of the mobile device(s) relevant to the investigation. The forensic investigation must ensure proper documentation and the establishment of chain of custody. Safely seize and secure the device to prevent data alteration or loss.
2. **Preservation:** Evidence preservation is an important step to ensure a forensically sound process for admissibility in court or even for administrative investigations. Preservation involves securing and evaluating the scene, isolation of digital evidence items to maintain integrity, and the collection/acquisition of electronic evidence to create an exact copy in time. Failure to preserve evidence in its original state could jeopardize an entire investigation, potentially losing valuable case-related information [23]. For instance, one safe way to preserve mobile devices is device isolation, away from network connectivity. This can be achieved using a shielding container such as a Faraday bag or enabling the device's airplane mode.
3. **Examination and Analysis:** The examination process uncovers digital evidence, including that which may be hidden or obscured. The conclusions are drawn from the use of accepted scientifically grounded methodologies, and they need to provide a complete description of the data and status, including its source and its importance. In contrast to the examination process, the analysis process considers the examination's findings in terms of their immediate relevance and probative value to the case. The potential evidence that may be relevant and generated in this step during investigation may include the following items:

1) Subscriber and equipment identifiers
2) Date/time, language, and other settings
3) Phonebook/Contact information
4) Calendar information
5) Text messages
6) Outgoing, incoming, and missed call logs
7) Electronic mail
8) Photos
9) Audio and video recordings
10) Multi-media messages
11) Instant messaging
12) Web browsing activities
13) Electronic documents
14) Social media related data
15) Application related data
16) Location information
17) Geolocation data
18) Cloud Storage Data

4. **Documentation:** This is a clear record of actions taken during investigation. It includes information on the tools and procedures used, the date and time of preservation, and any relevant details about the condition of the device. This documentation is crucial for reporting in the later stages of the forensic process and may be required in legal proceedings.
5. **Reporting & Presentation:** The practice of creating a thorough synopsis of all the actions done and judgements made throughout a case investigation is known as reporting. A thorough log of all activities and observations, a description of analysis and examination results, and an explanation of the conclusions derived from the data are all necessary components of reporting. Strong documentation, notes, images, and content produced by tools are essential components of a well-written report [23]. However, presentation involves presenting the collected information and findings in a clear and compelling manner to support the case. In the context of mobile forensics, the presentation of evidence is particularly important because it involves digital information obtained from mobile devices. Presentation of evidence is a crucial aspect of legal proceedings in court, or an administrative panel.

The forensic processes in mobile forensics are a systematic series of steps designed to identify, collect, preserve, analyses, and present digital evidence from mobile devices. These processes are essential for conducting thorough, repeatable, and legally sound forensic investigations.

3. Materials and Methods

The adopted methodology for this study aligns with the NIST forensic process to ensure the repeatability and reliability of the procedures. This study employs a methodical approach of acquisition, preservation and analysis of a newly acquired Apple iPhone XR (iOS 17.5) which was populated with relevant user data using the NIST SP 800-202 Quick Start Guide for Populating Mobile Test Devices [24].

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

The adopted approach for evidence extraction of the device focuses on the iTunes backup acquisition and iCloud data acquisition. These acquisition methods are creative approaches used in acquiring iOS device data where Physical or Full File System (FFS) device extraction are not feasible. Similarly, the approach causes the least amount of alterations to the device being tested, ensuring a more forensically sound acquisition. By exploiting the backup data, the forensic examiner can avoid modifying the device to extract data [25].

iTunes backup and iCloud backup are both methods provided by Apple for users to safeguard their iOS device data, but they differ in terms of where the backup is stored and how it is created. Backups from iCloud and iTunes are designed to preserve a wide range of data, including messages, pictures, device settings, app data, and more, which makes them a goldmine for forensic analysis. In the event of a device loss, damage, or during the setup process, customers can restore their iOS devices to a prior state using either of the backup options.

A. iTunes Backup Acquisition

iTunes backups are a standard procedure that allows iOS users to create a device backup image on a computer to restore their data and settings if they lose or damage the device. Such backups typically include configuration files, installed applications, their data and settings, media files, messages, contacts, calendars, and other important artifacts such as the keychain file where users can store credentials for websites and apps. iOS device users can secure their iTunes backups with a password. This serves as a defense layer for the protection of the backup from access by a third party.

The forensic iTunes backup acquisition mimics the standard iOS device backup procedure. When performing it, researchers at Belkasoft [26] suggests turning backup encryption on to obtain more data. Investigators can acquire the iTunes backup by acquiring a copy of the device Lockdown file. When a user connects an iOS device to a computer for the first time or initiates an iTunes backup, the device usually displays a prompt asking whether it should trust the computer. If the user confirms the request, the device pairs with the computer and creates a lockdown, file to auto-approve further connections to it.

Forensic investigators can look for iOS device lockdown files on the computers they have connected to at the following listed path:

a. Mac OS X: /private/var/db/Lockdown/ (may require additional access permissions)

b. Windows 7, Windows 8, Windows 10: C:\ProgramData\Apple\Lockdown

Most data can be gotten using a lockdown file for iTunes backup acquisition if the device has been unlocked with a passcode at least once after being restarted or powered on. It is worthy to note that the lockdown file can expire after an unspecified time, and it expires if the device is factory reset.

This iOS forensic investigation was carried out at the digital forensic laboratory of Digital Footprints Nigeria Limited. The investigation adopted the the NIST.SP.800-101r1 - Guidelines on Mobile Device Forensics [23] – Identification, Preservation, Analysis, Documentation, and Presentation. Figure 2 shows the adapted Mobile Forensic Investigation Process used for this study. The identification phase started with initial physical examination and documentation to ascertain that the researchers had the legal right to perform analysis on the phone. Necessary chain of custody entries was performed to ensure accountability for evidence item. During the preservation stage, the researchers ensured the phone was isolated to protect evidence integrity and avoid remote wiping or other tampering. The phone was put on flight mode and securely kept in a Faraday bag to keep it isolated.

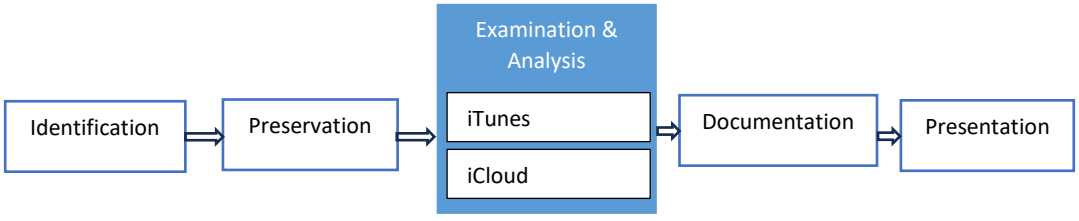

Figure 2. Mobile Forensic Investigation Process used for this study.

The research focused on examination and analysis of iTunes and iCloud backup as alternatives to the increasingly complex full physical acquisition. This study acquired iTunes backup using Oxygen Forensic Detective Extractor v2.13.1. The forensic tools used at the Digital Footprints laboratory are routinely validated as prescribed in the laboratory's Standard Operating Procedure, with the last of such validation exercise happening 3 weeks before the commencement of this study. In addition, Oxygen Forensic have undergone reliability checks through the National Institute of Standards and Technology Computer Forensics Tool Testing Program (CFTT) [27]. All procedures were documented, and a Digital Forensic Report prepared for Presentation.

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

B. iCloud Data Acquisition

iCloud is the cloud platform provided by Apple for users of their iOS devices. Particularly, it is a storage platform for various contents like photos and videos, and application data such as email, calendar, reminders, contacts, notes, etc. [13]. Additionally, a user may opt to store their device backups in iCloud rather than on a local computer. Data from iCloud can be complementary to what was extracted from an iPhone. In some cases, it might be the only data accessible, for example, if the device in question is not available or if it is locked and the passcode is unknown. Moreover, since iCloud can store more than one of a user's most recent backups, previous data which may not be accessible now of investigation could be accessed. This is why it is important to have the ability to download iCloud data in the course of a digital forensic investigation.

The data in cloud backups is identical to the offline backups created with iTunes. If the user's Apple ID, password, and computer's binary authentication token are known, forensic tools can be used to extract iCloud backups [29]. Oxygen Forensic Cloud Extractor supports the downloading of iCloud backups to include accounts protected with two-factor authentication, where no email notification will be sent to an account holder.

An important thing to note is that with iCloud backup acquisition, different backups from different phones can be acquired including access to different snapshots of the device data at different time. These further enable the investigator to correlate data of interest across multiple devices, which has been synced to the iCloud account under investigation at different time. Such correlation with different device back-ups could prove very vital to solving a case. In addition, unlike a regular user, a forensic investigator may benefit from having some knowledge of snapshots. One important detail to note is the date and time of snapshot creation. This information helps to understand when a user was backing up their device.

4. Results

As stated, it is essential to utilize specialized tools, which are designed to analyses the acquired backup. These set of tools parse the content of the backups and decode the data for the analyst to further investigate and determine the presence of the artifacts of interest. Analysis of the acquired data was performed using Oxygen Forensic Detective v 16.1.0.172 – a commercial forensic tool.

A. iCloud Data Analysis

Analysis of iCloud data showed evidential artifacts such as application data, accounts and passwords, contacts, and other categorized files. These important datasets can be crucial to solving cases. For instance, application data shows all installed application on device; contact shows list of saved contacts on phone; accounts and passwords, as the name implies shows the user accounts and passwords on the device. These are all important artifacts that could be very useful in the investigative process.

B. iTunes Backup Analysis

The adopted strategy for the analysis of the iTunes backup involved the analysis of user-generated data and system-generated data to establish how and where data produced by the automated tool originated from on the device.

a) User-generated Data Analysis

User generated data are artifacts which would have not been generated without user input. Such artifacts include call history, photos, videos, contacts, messages, website visited, etc. These artifacts provide verifiable evidence of activities and data stored by a suspect on the device. The following databases were analyzed using Oxygen Forensic SQLite Editor, to ensure retrieval of user-generated artifacts.

1. **AddressBook.sqliteDB:** This file contains information of all contacts stored on the device. Knowing the contacts saved on a device could be useful in an investigation. The investigation shows that the phone has three user entries in the contact information, showing their names, phone number, and other attributes.

The path to the AddressBook.sqliteDB is: /private/var/mobile/Library/AddressBook/

2. ***CallHistory.storedata:*** This file maintains call logs, including missed calls, incoming calls, and received calls. Call logs could prove crucial in an investigation, as a knowledge of calls made by the user with the device could be vital in solving a case. This investigation produced detailed call logs showing contact number, country code, duration, time stamps, and other call metadata. The path information and SQL Query that spooled this is showed below:

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

Path: */private/var/mobile/Library/CallHistory/*

SQL Query: SELECT *ZDATE, ZDURATION, ZISO_COUNTRY_CODE, ZADDRESS*

FROM *ZCALLRECORD;*

3. ***Sms.db****:* This database stores the SMS messages (both sent and received) present on the device. Messages could also be very crucial to solving a case, and this investigation produced all the messages stored on the device. A close review of the messages shows both user generated/personal messages as well as network messages from service provider. The database shows vital information such as the destination phone number, date delivered, and date read. The path information and SQL Query (viewed using Oxygen Forensic SQLite Browser) is shown below:

Path: */private/var/mobile/Library/sms/*

SQL Query*:* ***SELECT*** *text, service, date_read, date_ delivered, destination_caller_id*

FROM *message;*

4. ***Bookmarks.db:*** This file stores bookmarks on Safari Web Browser. Bookmarks could be vital to an investigation as it is indicative of user's browsing activities and preferences. This investigation showed that the user had 12 bookmarks on Safari. The entries show the bookmark title, URL, and other metadata. The path to the Bookmarks.db is showed below:

Path: */private/var/mobile/Library/safari/*

5. ***BrowserState.db****:* This database shows the content of the browser at backup or acquisition time. This could also prove to be useful in an investigation as it shows user's active browser activities as at the time of the backup. The database shows information such as title, URL, last viewed time, etc. The result of this investigation shows three active browser activities. For instance, a review of the result shows that the user had searched for "how to make money online" using Google search at 14:03:06 hours on 16th May 2025. Also, the user visited the website, "www.hackernews.com" and read an article titled, "Alert: New Phishing Attack Delivers Keylogger Disguised as Bank Payment Notice", at 10:26:47 hours on the 20th of May 2024. Such precise information about user browsing activities could make a difference in an investigation. The path information and SQL Query is shown below:

Path*: /Private/var/mobile/Library/safari/*

SQL Query: SELECT *title, url, user_visble_url*

FROM *tabs;*

6. ***History.db:*** This database stores web history. Web history captures all the websites visited, along with date and time stamps. It is an important artifact to look at in investigations, as it shows user's browsing history. The result of this investigation shows 179 browsing activities, time stamps, and other useful metadata. The path information is showed below.

Path*: /private/var/mobile/Library/safari/*

7. ***Voicemail.db:*** This database contains voicemails and the associated metadata. The result of this investigation shows no voicemail data present, indicating no voicemail sent at the time of the backup. The path information is shown below.

Path: */private/var/mobile/Library/voicemail/*

8. ***Photos and Video:*** Images and video taken with device camera can be of value during investigations. In iOS devices, the Digital Camera Images (DCIM) folder contain the 100APPLE folder where videos and images captured with the device camera are stored. This investigation showed 29 photos stored.

Path on sample device*: /private/var/mobile/media/DCIM/100APPLE/*

b) System-generated Data Analysis

Beyond the user generated data, the system-generated data could be of immense evidential value. Apple devices record and store various user settings and activities, and some of these records could potentially be useful in

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

reconstruction of events being investigated. The following databases and files had several system artifacts useful for gathering additional evidence on iOS devices during investigation.

1. ***Consolidated.db:*** Location information is usually important in Digital Forensic investigation. For instance, in criminal investigation, it could support or refute alibi claims. In iOS devices, the Consolidated.db database keeps track of past Wi-Fi and Cell locations, thus giving a history of where the user have been. This investigation showed three location records, showing the exact latitude and longitude. The path where this can be found, and the SQL query is shown below.

Path: */Private/var/root/Library/cache/Locationd/*

SQL Query: SELECT *Name, Timestamp, Latitude, Longitude, Distance*

FROM *Fences;*

2. ***CellularUsage.db:*** This file contains phone numbers and SIM IDs associated with device being investigated. It also shows phone numbers previously associated with the device. This research shows two subscriber ID's (both Nigerian GSM numbers) associated with the device, with the last update date for the former as 17th April 2024 at 15:27:31, and the latter at 24th June 2024 at 08:32:25. This important evidential item was found following the path below:

Path: */private/var/wireless/Library/Database/*

3. ***Accounts3.sqlite:*** This file stores additional account information of device owner that may be useful in the investigation. It contains important details such as associated email address(es) and other information of evidential value. The path information and SQL query is shown below.

Path: */private/var/mobile/Library/Accounts/*

SQL Query: SELECT *ZDATE, ZACCOUNTDESCRIPTION, ZOWINGBUNDLEID,*

ZUSERNAME

FROM *ZACCOUNT;*

4. ***DataUsage.sqlite****:* This file stores details of mobile network traffic. It also captures important information on installed apps and time stamps (time of first use and time of last use). This could be very important in investigations, as a knowledge of installed applications and associated timestamps could be helpful. This investigation showed the following applications were installed on the iPhone device as shown in Figure 3.

Path*: /private/var/wireless/Library/Database/*

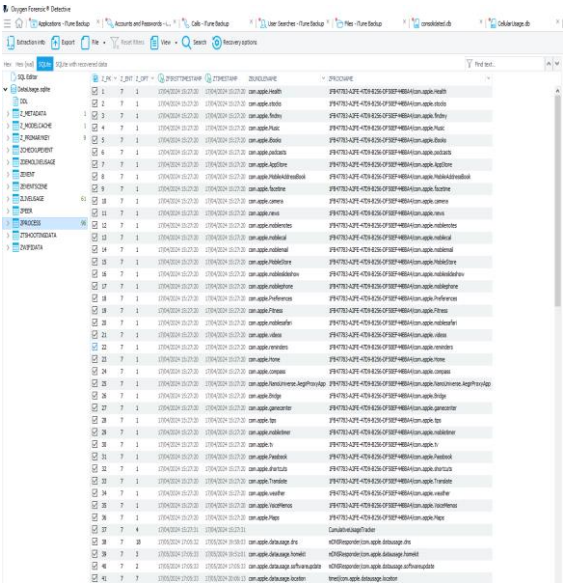

Figure 3. Content of DataUsage.sqlite Showing Device Usage Statistics.

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

5. ***Keychain-2.db:*** Keychain is the password manager Apple builds into its devices to store sensitive information such as passwords, credit card details, Wi-Fi login details, authentication tokens, and a host of other sensitive data. These details could be crucial in investigations. Data stored are encrypted, and the path information is shown below.

Path: */Private/var/Keychain/*

6. ***InteractionC.db:*** The InteractionC.db database could be vital in digital investigations as it tracks the recent interactions of the user. This investigation showed the device had 29 interactions; with the oldest happening on 15th May 2024 at 11:40:35, and the latest on 24th June 2024 at 09:59:26. The path is shown below.

Path: */private/var/mobile/Library/CoreDuet/People/*

7. ***Third party applications****:* Third part applications are those that are offered by vendors other than Apple. The AppStore on iOS allows users to install apps on their devices through secure authentication, which requires either finger or Apple password access. Koganti and Rao [29] noted that the path's application names are dynamic, meaning that when it is linked again for forensic purposes, the names change but the data stays the same.

Path: */private/var/mobile/Containers/Data/Application/*

5. Conclusion

The best chance of recovering evidential artifacts from an iPhone is via a full physical extraction. However, due to the high levels of encryption and security of iPhone, it is becoming increasingly difficult to successfully achieve a full physical extraction. The adoption of full file and disk encryption, and secure enclave technology poses serious challenge to forensic investigators. This study explored the forensic examination of an iPhone device (iPhone XR – iOS 17.5) which was populated with data of interest using the NIST SP 800-202 Quick Start Guide for Populating Mobile Test Devices, by demonstrating alternative approach to the regular investigation approach of sole dependency on the physical extraction method of the evidence device.

A viable approach of exploiting iCloud and iTunes backup in a forensically sound manner was demonstrated using Oxygen Forensics Detective, a commercially available tool for acquisition and analysis of data. The examination and analysis process made a comprehensive identification of artifacts with forensic value, which include the user-generated data and system-generated data. With forensic acquisition and analysis of iCloud and iTunes data, investigators are able to overcome certain restriction imposed by Apple during investigation of iDevices.

This research produced valuable data of evidential value, which aligns with the goal of the forensic investigation. Artifacts such as contacts, SMS, call history, media files, database, browser, application data and many others, were extracted and analysed. This study uncovered several artifact locations and provided a brief description of each, along with hints about their usefulness in a forensic analysis. Table 1 itemizes the common forensic artifacts encountered in this investigation, including their locations and description. It is imperative to note that forensic investigators are required to have full understanding of where certain artifacts of interest are located and how to retrieve them without too much dependency on automated tools. Therefore, this study contributed to the scarce resources available on iOS forensics.

The digital forensic investigation of iOS mobile phones is a dynamic and challenging field. Ongoing advancements in tools and methodologies, coupled with the emergence of new trends, contribute to the evolution of the discipline. However, challenges related to privacy, regular iOS updates, and legal considerations necessitate a continual refinement of investigative approaches within the context of mobile and iOS forensic investigations. As technology continues to advance, so too must the methods employed by digital forensic professionals to ensure the integrity of their findings in a rapidly changing landscape.

This study was not without limitations. The result of this forensic investigation was not cross-validated with a second forensic tool. Cross-validation with a different tool is a best practice in digital forensics, to reinforce the validity of the forensic investigation. In addition, since this study focused on Oxygen Forensic Detective, the explanations are limited to this tool. There are other digital forensic tools, each with unique features. While the artifacts will not change, the extraction and analysis approach or methods could change, depending on the tool used. Finally, the iTunes and iCloud backup in this study were encrypted. This required knowledge of user password and decryption keys for successful acquisition. In reality, it is not always the case that a forensic examiner will have user passwords and decryption keys.

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

Table 1: Summary of extracted artifacts showing location and description.

S/N	ARTIFACT	FILE NAME	DESCRIPTION	LOCATION PATH
User-generated Artifacts				
1	Contacts	AddressBook.sqliteDB	Contains information of all contacts stored on the device.	/private/var/mobile/Library/AddressBook/
2	Call Logs	CallHistory.storedata	Maintains call logs, including missed calls, incoming calls, and received calls.	/private/var/mobile/Library/CallHistory/
3	SMS	Sms.db	It contains the default message present on the device.	/private/var/mobile/Library/sms/
4	Browser State	BrowserState.db	Shows content of the browser at backup or acquisition time.	/Private/var/mobile/Library/safari/
5	Bookmarks	Bookmarks.db	Contains bookmarks store on Safari Web Browser.	/private/var/mobile/Library/safari/
6	Browser History	History.db	Stores Safari web history.	/private/var/mobile/Library/safari/
7	Voicemails	Voicemail.db	Contains voicemails and their metadata.	/private/var/mobile/Library/voicemail/
8	Multimedia	-	Images and videos captured with device camera.	/private/var/mobile/media/DCIM/100APPLE/
System-generated Artifacts				
1	Wi-Fi and Cell Locations	Consolidated.db	Keeps track of past Wi-Fi and Cell locations, thus giving a history of where their users have been.	/Private/var/root/Library/cache/Locationd/
2	SIM IDs and Phone Numbers	CellularUsage.db	Contains phone numbers and details of SIM cards that are no longer tied to the device.	/private/var/wireless/Library/Database/
3	Accounts Information	Account3.sqlite	Stores additional accounts information of device owner.	/private/var/mobile/Library/Accounts/
4	Data Usage Statistic	DataUsage.sqlite	Details of mobile network traffic. Helps determine which applications were installed on the device and when they were used for the first and last time.	/private/var/wireless/Library/Database/
5	Authentication data	Keychain-2.db	Stores users' passwords, credit card details, Wi-Fi login details, and a host of other sensitive data.	/Private/var/Keychain/
6	Device Users' Activities	InteractionC.db	Tracks the interactions such as text messages of the user with recent contacts.	/private/var/mobile/Library/CoreDuet/People/
7	Third Party Applications	-	Vendors application data installed from Apple store.	/private/var/mobile/Containers/Data/Application/

Acknowledgments: This research was conducted at the digital forensic laboratory of Digital Footprints Nig. Ltd. We are grateful for the technical support and access to tools used.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] O. W. Samuel and A. Al-Nemrat, "Towards a taxonomy for mobile forensics," in *Proc. 2013 IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining*, Ontario, Canada, Aug. 25, 2013.

[2] Apple Inc., *Apple security releases*. Available: https://support.apple.com/en-us/HT201222 (Accessed: Nov. 8, 2024).

[3] V. Avancha, "Comparison of forensic acquisition and analysis on an iPhone over an android mobile phone through multiple forensic methods." Available: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1125&context=msia_etds (Accessed: Nov. 5, 2024).

[4] R. Ayers, S. Brothers, and W. Jansen, *NIST.SP.800-101r1 - Guidelines on mobile device forensics*. Available: https://doi.org/10.6028/NIST.SP.800-101r1 (Accessed: Nov. 9, 2024).

[5] R. Ayers, B. Livelsberger, and B. Guttman, *NIST SP 800-202 Quick start guide for populating mobile test devices*. Available: https://doi.org/10.6028/NIST.SP.800-202 (Accessed: Nov. 9, 2019)

[6] V. Baryamureeba and F. Tushabe, "Mobile phone forensics: a challenge to the future of cybercrime investigation," in *Proc. Int. Conf. Adv. Comput., Control, Telecommun. Technol.*, 2010.

[7] Belkasoft, *Acquiring iOS devices*. Available: https://belkasoft.com/iOS. (Accessed: Nov. 14, 2024)

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025

[8] Carrier, *File System Forensic Analysis*. Boston, MA, USA: Addison-Wesley, 2005.

[9] Casey, *Digital evidence and computer crime: Forensic science, computers and the internet*. Massachusetts, MA, USA: Academic Press, 2011.

[10] T. C. Chang and Y. Li-Min, "Digital forensics security analysis on iOS devices," *J. Web Eng.*, vol. 20, pp. 775-794, 2021.

[11] Counterpoint Research, *Global smartphone market share: quarterly*. Available: https://www.counterpointresearch.com/insights/global-smartphone-share/ (Accessed: Nov. 5, 2024)

[12] S. Garfinkel, *iPhone and iOS forensic: Investigation, analysis and mobile security for Apple iPhone, iPad and iOS Devices. J. Digit. Forensics, Security Law*, vol. 8, pp. 65-67, 2013.

[13] Hosmer, *Investigating Digital Crime*. Oxford, United Kingdom: Syngress, 2016.

[14] International Telecommunication Union, *Statistics*. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Accessed: Nov. 4, 2024)

[15] S. Kanarachos, V. Kouliaridis, and G. Kambourakis, "Mobile forensic investigation: A review of malware detection techniques and approaches," *Future Gener. Comput. Syst.*, vol. 78, pp. 1146-1157, 2018.

[16] H. Koganti and G. Rao, "Forensic acquisition of IOS devices," *Int. J. Recent Technol. Eng.*, vol. 8, 2019.

[17] R. Mangalampalli, "The apple of the world: extracting evidential data through iphone," *Culminating Projects Inf. Assurance*, vol. 96, pp. 2-23, 2019.

[18] M. Alomari *et al.*, "Mobile investigation: forensics analysis of iOS devices." Available: 10.13140/RG.2.2.16584.60169 (Accessed: Nov. 5, 2024).

[19] NIST, *Computer forensics tool testing program (CFTT)*. Available: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt (Accessed: Nov. 15, 2024)

[20] J. Paglierani, M. Mabey, and G. J. Ahn, "Towards comprehensive and collaborative forensics on email evidence," in *Proc. 9th IEEE Int. Conf. Collaborative Comput.: Netw., Appl. Worksharing*, Austin, Texas, Oct. 20, 2013.

[21] M. Piccinelli and P. Gubian, "Exploring the iPhone backup made by iTunes," *J. Digit. Forensics, Security Law*, vol. 6, pp. 31-62, 2011.

[22] O. Afonin, "The future of mobile forensics." Available: https://www.proquest.com/trade-journals/future-mobile-forensics/docview/1695022347/se-2. (Accessed: Nov. 9, 2024)

[23] Reilly, *Digital forensics for handheld devices*. Boca Raton, FL, USA: CRC Press, 2015.

[24] R. Sang and K. Yun, "iLEAPP: iOS Logs, Events, and Properties Parser," in *Proc. 2020 ACM Asia Conf. Comput. Commun. Security*, Taipei, Taiwan, Jun. 1, 2020.

[25] R. T. Sibe and C. Kaunert, "Digital evidence, digital forensics, and digital forensic readiness," in *Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria*. Switzerland: Springer Nature, 2024, pp. 57-83.

[26] Statista, *Market share of mobile operating systems worldwide from 2009 to 2025, by quarter*. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/ (Accessed: Nov. 8, 2024)

[27] Statista, *Number of smartphone mobile network subscriptions worldwide from 2016 to 2023, with forecasts from 2023 to 2028*. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (Accessed: Nov. 4, 2024)

[28] Y. Vasserman, M. Ganor, and J. Yen, "iOS forensic research," *Adv. Digit. Forensics XIII*, pp. 137-160, 2017.

[29] S. Zawoad and R. Hasan, "Towards practical cloud forensic investigation," in *Proc. 2015 IEEE/ACM 8th Int. Conf. Utility Cloud Comput.*, Limassol, Cyprus, Dec. 7, 2015.

DOI: https://doi.org/10.54216/JCIM.170212
Received: April 16, 2025 Revised: June 30, 2025 Accepted: August 29, 2025