A REVIEW OF IOS MOBILE DEVICES FORENSIC AND INVESTIGATION FRAMEWORK INTEGRATED WITH MACHINE LEARNING

Ishaq Ahmed[1], Norjihan Abdul Ghani[1*], and Ainuddin Wahid Abdul Wahab[2]

[1]Department of Information Systems, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia

[2]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia

Emails: s2192167@siswa.um.edu.my, norjihan@um.edu.my*, ainuddin@um.edu.my

ABSTRACT

The review covers key components of iOS forensics, including data acquisition, data analysis, and evidence interpretation, highlighting how machine learning algorithms can automate and optimize these processes. The paper also discusses the ethical and legal implications of deploying machine learning in forensic contexts, emphasizing the need for transparency, accountability, and privacy preservation. In recent years, the exponential growth of mobile devices, particularly iOS devices, has posed significant challenges to digital forensic investigators. The sheer volume of data and complexity of data stored on these devices require innovative approaches to efficiently extract, analyze, and interpret digital evidence. This review aims to provide a comprehensive overview of the integration of ML approaches with iOS mobile devices' forensic and investigation framework. As mobile devices continue to play an increasingly central role in our daily lives, they have become a critical source of evidence in digital forensic investigations. Among these devices iOS-based mobile devices pose unique challenges due to their closed ecosystem and strong security measures.

KEYWORDS: iOS Mobile Forensic; Digital investigation framework; Machine learning; Integrated framework.

1. INTRODUCTION

In the ever-evolving landscape of digital technology, mobile devices have become an integral part of our daily lives. iOS devices, produced by Apple, have gained immense popularity, and are used by millions of individuals across the globe [1], [2]. as these devices store an abundance of sensitive information, they have also become an attractive target for cybercriminals, and as a result, digital forensics has become an indispensable tool in law-enforcement and cybersecurity. Mobile device forensics and investigation is a branch of digital forensics that focuses on the acquisition, analysis, and preservation of digital evidence from mobile portable devices. Digital evidence, ranging from text messages and call logs into images, videos, and application data, plays a pivotal role in modern investigative procedures devices such as smartphone, tablets, and Other mobile devices, including smartphones and tablets, are particularly rich sources of such evidence due to their pervasive use and capacity to store a vast array of personal and sensitive information [3]-[5]. Digital forensic investigation on iOS mobile devices involves the systematic collection, and preservation of electronic evidence in a manner that ensures its admissibility in a court of law [6]. These investigations have relied on manual processes and well-established forensic techniques to uncover critical data such as text messages, call logs, email correspondence, and more. As the volume and complexity of data on iOS devices continue to grow, there is an urgent need for innovative

approaches that can cope with this escalating challenge [7]. The review paper explores the integration of machine learning within the forensic framework of iOS mobile devices. It aims to provide a comprehensive overview of the current methodology, tools, and framework, examining how ML can enhance each stage of the forensic process for data acquisition to analysis and interpretation. Key applications of machine learning in this context include automated data classification, anomaly detection, and predictive analytics. In Figure 1. Discuss an investigation process of mobile devices forensic, preparation and planning, evidence extraction, evidence preservation, the chain of custody, data analysis, artifact examination, metadata analysis, and expert testimony. archiving and storage, and report generation [8], [9].

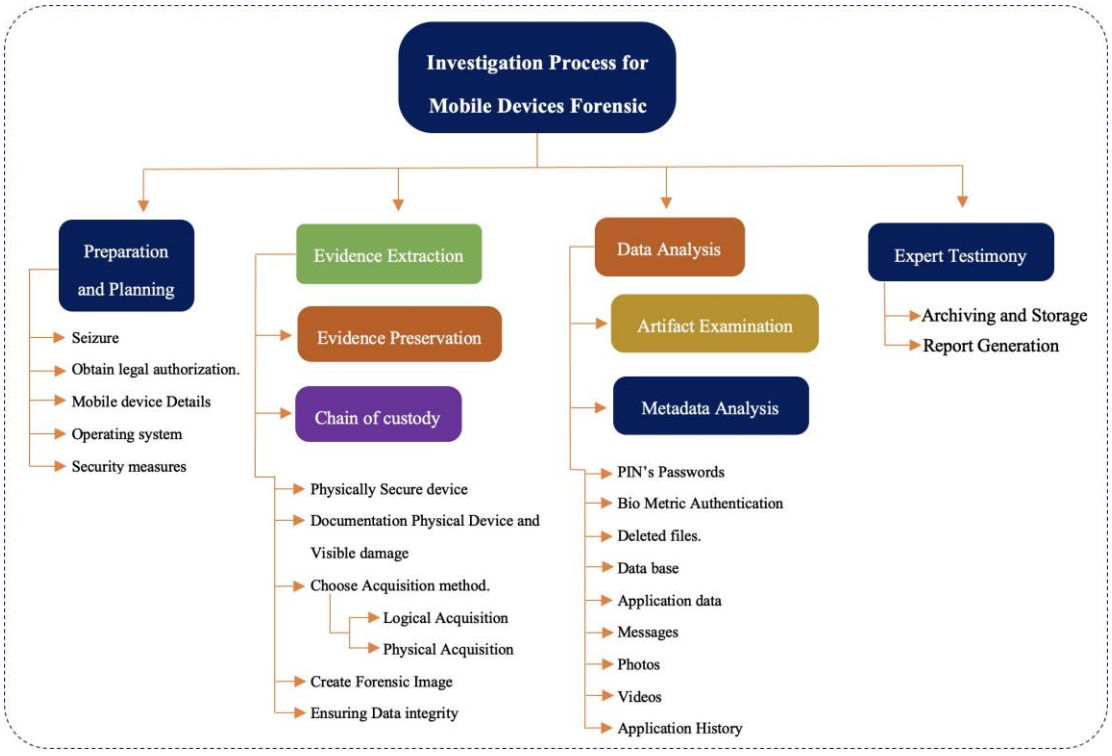


FIG.1: Investigation process for Mobile devices forensic

1.1 CONTRIBUTION OF RESEARCH

The main contribution of this work is to produce a comprehensive idea for the researcher and law enforcement agencies about iOS mobile devices' forensic and investigation framework integrated with machine learning models. It offers a detailed overview of existing forensic methodologies and tools specific to iOS, including their capabilities, limitations, and applications, and explores the unique challenges posed by iOS architecture and security features. The integration of machine learning into the forensic investigation framework for iOS mobile devices represents a significant advancement in addressing the complexities of digital investigation. While existing studies demonstrate the efficiency of ML techniques, ongoing research and development are essential to overcome remaining challenges and enhance the reliability of forensic examinations. Future directions may include the development of specialized ML models tailored to iOS devices forensic and the exploration of emerging techniques of data privacy preservation and ethical AI deployment. In section II discusses (LR) review and background. Furthermore, the paper identifies key research gaps and- proposes future directions, emphasizing the need for robust machine learning models tailored to forensic needs, improved data acquisition techniques, and better methods for handling encrypted and deleted data.

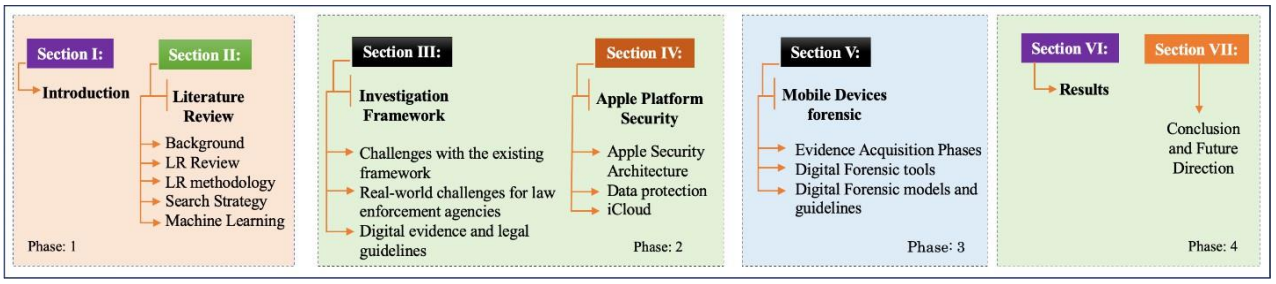


FIG.2: Index of document

2. BACKGROUND

In 2007 Apple introduced the most powerful smartphone called the iPhone. Apple operating system (iOS) devices have begun to gain popularity in the world. The latest smartphones and tablets can perform any task that a laptop or personal computer can. Furthermore, because of the high quality of functionality in their central processing, they can perform tasks faster than computers, resulting in a significant amount of data and evidence [10]. Mobile forensics is a subfield of digital forensics that focuses on mobile devices by utilizing logical strategies to retrieve information from mobile phones. Which are becoming increasingly popular. iOS mobile forensics has grown in lockstep with the explosive growth of Apple's iPhones and iPads. From the forensic perspective, such devices could provide numerous useful artefacts during the investigation. However, the golden rule for the forensic examination of digital evidence is that original evidence should not be altered [11]. iOS devices provide larger storage space that could store emails, browsing histories, chat histories, Wi-Fi data, GPS data and more, if a forensic examiner understands the APFS file system will become more convenient. Such devices could present lots of useful artefacts during the investigation [12]. Machine learning, a subset of artificial intelligence, has emerged as a game-changing technology in the digital forensic field. It has the potential to enhance the efficiency and accuracy of evidence acquisition and analysis, enabling investigation to navigate the intricate world of iOS mobile devices more effectively [13]-[16]. This review paper presents a comprehensive iOS mobile device forensic and investigation approach that harnesses the power of machine learning to facilitate evidence acquisition on iOS devices. The paper also addresses the ethical and legal considerations associated with using machine learning in forensic investigation. Issues such as data privacy, algorithmic transparency, and the potential for bias must be carefully Ethical and legal considerations, such as data privacy algorithms bias, and the admissibility of machine learning-derived evidence in legal proceedings, are also discussed to provide a balanced perspective on the integration of these in digital forensics. Managed to ensure the responsible application of these technologies. By reviewing existing literature and case- studies, this paper highlights the current state of the field and areas of future research and development.

2.1 LITERATURE REVIEW

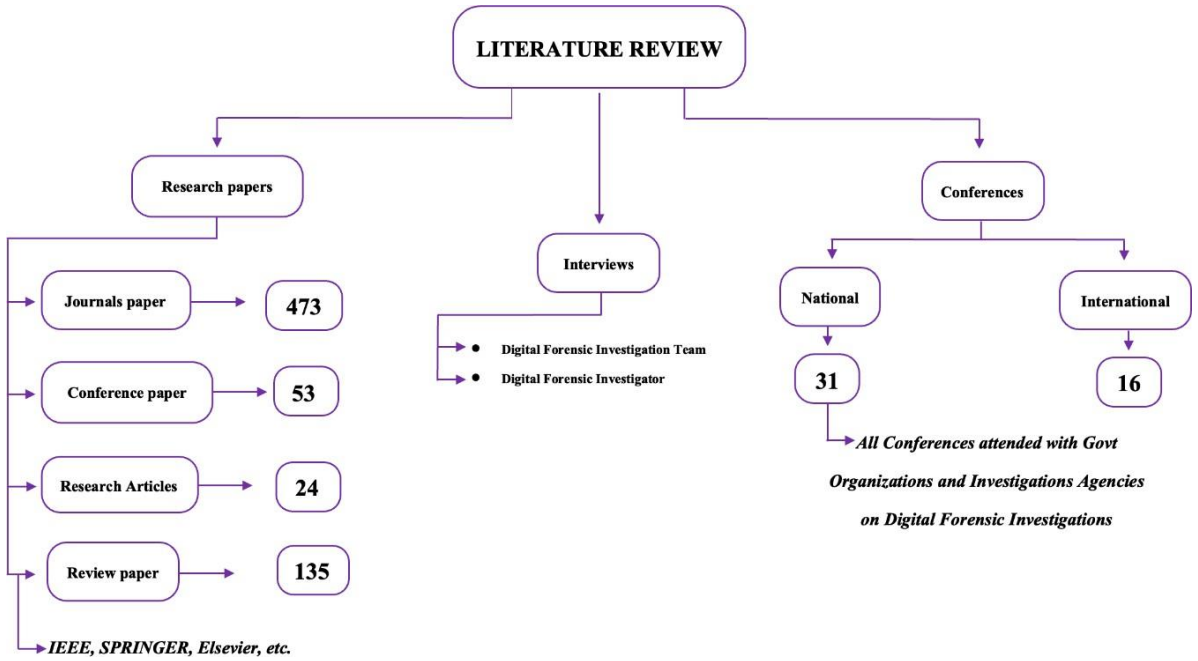


FIG. 3: Literature review

The objective of this literature review (LR) is to provide a comprehensive overview of the integration of ML approaches with iOS mobile devices forensic and investigation framework. By synthesizing existing research literature, this review aims to identify key trends, methodology, challenges, and future directions in this emerging field.

2.2 SELECTION OF TOPIC

Selection of the studies based on research questions and objectives.

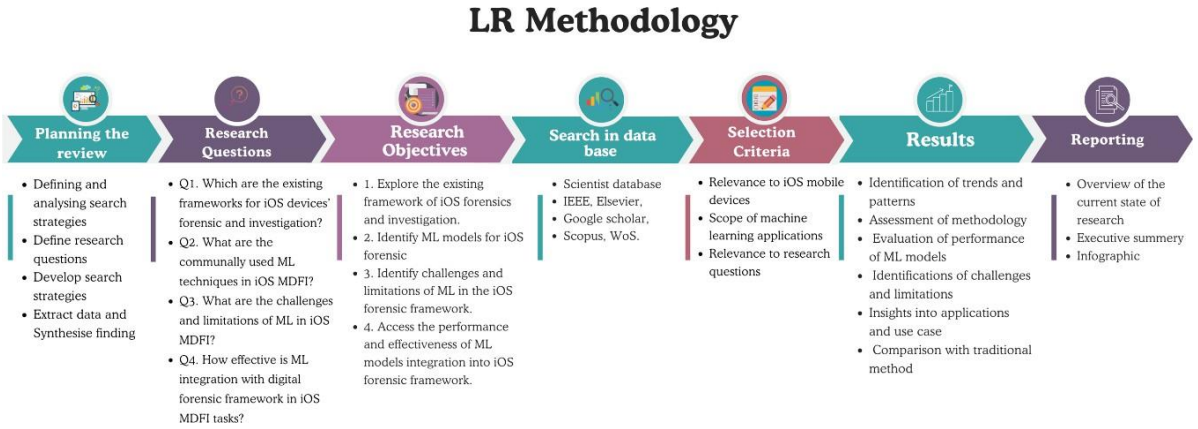
2.3 Questions

Q1. What are the existing frameworks for iOS devices' forensics and investigation?
Q2. What are the communally used ML techniques in iOS MDFI?
Q3. What are the challenges and limitations of ML in iOS MDFI?
Q4. How effective is ML integration with the digital forensic framework in iOS MDFI tasks?

2.3 Objective

1. Explore the existing framework of iOS forensics and investigation.
2. Identify ML models for iOS forensic
3. Identify the challenges and limitations of ML in the iOS forensic framework.
4. Access the performance and effectiveness of ML models in the iOS forensic framework.

3. LR METHODOLOGY



3.1 INTEGRATION OF MACHINE LEARNING IN iOS MOBILE FORENSICS

In conducting a literature review on the integration of iOS mobile devices forensic and investigation framework with machine learning (ML), it is essential to adopt a structured and rigorous approach to identify, evaluate, and synthesize relevant research. The integration of ML approaches with iOS mobile devices' forensic investigation framework represents a burgeoning area of research and development within the digital forensic community. These approaches hold promise for improving the efficiency, accuracy, and depth of forensic investigation involving iOS devices, ultimately enhancing the capabilities of forensic examiners to uncover valuable insights from digital evidence. ML algorithms enable forensic examiners to automate tasks, classify data detect patterns, and make predictions based on large datasets extracted from iOS devices [17],[18]. Machine learning offers promising solutions to address the challenges encountered in iOS forensic investigation. Implementing machine learning in mobile device forensics, outlining key applications such as automated data classification and anomaly detection. ML algorithms can automate data analysis tasks, reduce manual effort, and enhance the accuracy of forensic examinations. Anomaly detection using machine learning has garnered significant attention in iOS forensics [19]. Integration of machine learning (ML) techniques within the digital forensic investigation framework provides an opportunity to enhance the efficacy and effectiveness of data analysis and evidence extraction [20]. Automated data analysis is one of the significant advantages of (ML) is its ability to handle large datasets. Algorithms such as clustering and classification can automatically categorize data, identify patterns, and highlight anomalies. Nature language processing (NLP) can be used to analyze text messages and emails, while image recognition algorithms can help in identifying relevant photos or videos [21]. Machine learning models can predict potential data locations and types of evidence based on previous cases, thereby streamlining the investigation process. The predictive capability can significantly reduce the time required to find crucial evidence [22], [23].

Machine learning (ML) has emerged as a powerful tool that can significantly enhance forensic investigation. By leveraging its capabilities in pattern recognition and data analysis, machine learning can address many of the limitations faced by traditional forensic methods. ML algorithms can automate the process of data extraction and analysis, improving both the efficiency and accuracy of investigation [24]- [26].

3.2 SEARCH STRATEGY

The search strategy involves querying multiple academic databases, including IEEE Explore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar, keywords and search terms are carefully chosen to capture the breadth of relevant research. These include a combination of terms such as "iOS forensic," "mobile device investigation," "machine learning," "digital investigation," and "data analysis." Period between 2019 to 2024 but focus on the most related and latest research.

Search	Mobile forensic	iOS forensic	ML Integrated Framework with MDFI
Google Scholar	1710	443	57
IEEE Explore	97	31	16
Web of Science	149	48	7
Others	118	63	20
Total	**2074**	**585**	**100**

TABLE 1: Search strategy

3.3 Challenges with machine learning integration

3.3.1 Framework integration challenge. The absence of a comprehensive digital forensic framework especially attuned to iOS devices impedes the seamless amalgamation of traditional forensic methods with machine learning techniques. This gap restricts the holistic examination and extraction of digital evidence, hindering the development of comprehensive investigative protocols crucial for iOS device forensic proceedings [27].

3.3.2 Optimizing evidence acquisition. Efforts to enhance acquisition efficiency on iOS devices necessitate a focused exploration of machine learning models, including natural language processing and image recognition. Current literature emphasizes the potential of these models yet highlights the lack of tailored implementation for iOS evidence acquisition, hindering the advancement of optimized methodologies specific to this platform [28], [29].

3.3.3 Validation and dependability of machine learning models. The reliability, accuracy, and robustness of machine learning models utilized in digital forensic approaches for iOS devices remain an area of concern. Recent studies by Garcia and Chen (2023) emphasize the necessity for a standardized evaluation framework to comprehensively assess these models' efficacy in real-world forensic scenarios, indicating a critical gap in ensuring their dependability and accuracy [30].

3.3.4. Lack of integrated machine learning (ML) solutions for iOS forensics. while machine learning algorithms hold promise for improving forensic investigations by recognizing patterns, anomalies, and encrypted content, their integration into iOS devices' forensic framework remains limited. The distinct security features of iOS devices, such as end-to-end encrypted and secure boot processes, pose hurdles for accessing and extracting data without compromising its integrity. The diversity among iOS applications with varied data structures and encrypted methods necessitates a nuanced approach to implementing machine learning effectively [31], [32].

3.4 EXISTING INVESTIGATION FRAMEWORK

Phases	Digital Investigation Frameworks		
	Integrated Digital Forensic process model	Framework for a Digital Forensic investigation	Examination of Digital Forensic Models
Identification state	✓	✓	✓
Collection stage	✓	✓	✓
Authentication stage	✓	✗	✗
Preservation stage	✓	✓	✓
Evidence Reduction stage	✗	✗	✗
Analysis Stage	✓	✓	✓
Examination Stage	✓	✓	✗
Presentation Stage	✗	✓	✓

TABLE 2: Existing investigation frameworks

Based on (studies of Horsman 2023) complexity is another challenge. As the data collected increases, developing tools that can analyze the data collected quickly becomes more challenging. Furthermore, the lack of standardization in the formatting and storage of digital evidence is also a significant issue. It is challenging to share digital proof. This issue could affect the efficiency of investigations by having a standardized set of procedures; law enforcers could exchange information more effectively. According to (Quick 2022) correlation and consistency are the biggest challenges when developing digital analysis tools. Since the evidence is collected from different sources, the data must be analyzed and correlated correctly. This can be time-consuming and drain an investigation's resources.

3.4.1 Strong Encryption and security protocols

iOS devices use advanced encryption to protect user data, including hardware-based encryption and secure enclave. This makes it extremely difficult for law enforcement to access data without the correct passcode or decryption keys, even if they have physical access to the devices. Investigators struggle to unlock iPhones and the difficulty of bypassing iOS encryption. In 2021, FBI Director Christopher Wray highlighted the challenges posed by encryption, referring to it as a major public safety issue (FBI, 2021).

3.4.2 Data privacy laws and regulations

Regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) impose strict rules on accessing and handling personal data. These laws complicate the process of obtaining legal authorization to access and use data from iPhones, delaying investigations and limiting the scope of data that can be accessed. Compliance with these regulations is critical to ensure that evidence is admissible in court (European Commission, 2021).

3.4.3 Advanced Device-looking mechanisms.

iPhones feature advanced locking mechanisms, such as alphanumeric passcodes, Touch ID, and Face ID. If these mechanisms are engaged, accessing the devices without the user's cooperation is extremely challenging. Forensic techniques that attempt to bypass these locks often face limitations due to the continuous enhancements in Apple's security infrastructure (Symantec, 2021).

3.4.4 Cloud data

Many iOS users back up their data on iCloud, which is encrypted and stored on Apple's servers. Accessing iCloud data typically requires cooperation from Apple, which may not always be granted, especially without proper legal authorization. This dependency on Apple can delay investigation significantly (ZDNet. 2022).

3.4.5 App data and end-to-encryption

Third-party apps on iOS devices use their encryption method, and many popular messaging apps, like WhatsApp, and Signal, use end-to-end encryption. This makes it difficult to extract and interpret data from these apps, as forensic tools need to decrypt data by different standards and formats. The popularity of such apps has increased the complexity of digital investigations (TechCrunch, 2021).

3.4.6 Anti-forensic measures

User may employ anti-forensic techniques such as data wiping, encryption apps, and secure deletion tools to protect their information. These measures can destroy or obscure critical evidence, making it more challenging for investigators to recover and analyze data. A study by Haggerty and Talyor (2019) discusses the growing sophistication of anti-forensic techniques and their impact on digital investigations.

4. DIGITAL EVIDENCE AND LEGAL GUIDELINE.

Guidelines and procedure of Evidence acquisition and preservation. Supreme Court on the admissibility of electronic evidence under Section **65B** of the **Evidence Act. Under the Indian Evidence Act, of 1872, Section 65B** prescribes a distinct framework that governs the admissibility of electronic evidence. There have been multiple litigations over the scope and ambit of Section 65B

4.1 Legal framework for electronic evidence

Under Section 65A of the Evidence Act, the contents of electronic records have to be proved as evidence by the requirements of **Section 65B**. Both **Sections 65A and 65B** were inserted through the **Indian Evidence (Amendment) Act, 2000,** and form part of Chapter V of the Evidence Act, which deals with documentary evidence. In Anvar v. Basheer, it was clarified that as **Section 65B** begins with a non-obstante clause, it forms a complete code for the admissibility of electronic evidence.

Under Section 65B(1), any information contained in an electronic record, which has been stored, recorded or copied as a computer output, shall also be deemed as a 'document' – and shall be admissible as evidence without further proof or production of the originals, if the conditions mentioned are satisfied. **Section 65B(2)** lays down the criteria that must be satisfied for the information to be categorized as a 'computer output.' divergent views taken by the Apex Court. Digital evidence acquisitions accepted in court typically adhere to accepted forensic standards and legal protocols.

4.2. Forensic Imaging

Creating a bit-by-bit copy (forensic image) of digital media, ensuring the original data remains unchanged during acquisition. This method maintains integrity and is widely accepted in courts. The Scientific Working Group on Digital Evidence (SWGDE) and the National Institute of Standards and Technology (NIST) provide guidelines on forensic imaging.

4.3 Chain of Custody Documentation

Maintaining a clear and documented chain of custody, detailing who handled the evidence, when, and how, to ensure its integrity and prevent tampering. The Federal Rules of Evidence (Rule 901) and various legal jurisdictions emphasize the importance of a proper chain of custody.

4.5 Verified Forensic Tools

Use validated and accepted forensic tools that comply with legal standards and guidelines. Tools like EnCase, FTK (Forensic Toolkit), and open-source options like Autopsy are widely recognized and accepted in the forensic community.

4.6 Proper Documentation and Metadata Preservation

Accurate documentation of the acquisition process, including timestamps, metadata, and any alterations made during the investigation. SWGDE and NIST provide guidelines on proper documentation and metadata preservation.

4.7 Expert Testimony

Having qualified experts who can validate the acquisition process, affirm the integrity of the evidence, and provide testimony on the methods used. Expert testimony can reinforce the admissibility of digital evidence in court. These types of acquisitions align with legal standards, forensic best practices, and guidelines they are provided by organisations like SWGDE, NIST, and legal codes, ensuring the reliability and admissibility of digital evidence in court.

5. REAL-WORLD CHALLENGES FOR LAW ENFORCEMENT AGENCY'S ROLE OF AI AND ML IN DIGITAL FORENSIC INVESTIGATION.

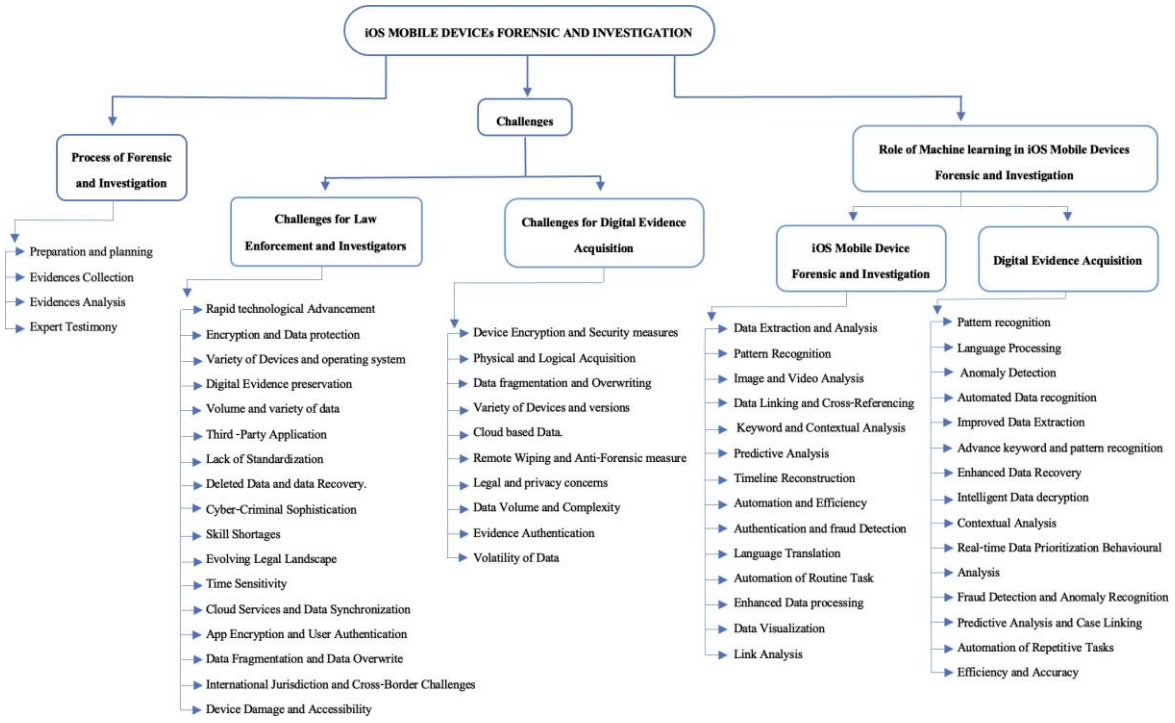


FIG. 4: Challenges and role of ML in Digital Forensics

The following figure 4 highlights the real-world challenges law enforcement agencies face while investigating iOS devices. These challenges primarily revolve around maintaining the chain of custody, preserving evidence, and navigating the complexities of the evidence acquisition process. Integrating AI and machine learning (ML) into digital forensics can significantly streamline and expedite investigations by automating repetitive tasks, such as data sorting and pattern recognition, thereby enhancing the accuracy and reliability of evidence acquisition. Furthermore, these technologies enable the analysis of large and diverse datasets, which is critical when dealing with complex cybercrime cases. Since cybercriminals often use multiple devices and platforms to conceal their activities, ML can improve the detection of hidden relationships between different data points and support multi-stage analysis to efficiently gather evidence. This integration not only reduces the time and effort required for investigations but also improves the ability to predict, detect, and mitigate potential cyber threats more proactively [33], [37].

6. APPLE PLATFORM SECURITY

Secure Enclave

The secure Enclave is a dedicated subsystem in the latest versions of iPhones and iPads.

Overview

The Secure Enclave is a dedicated secure subsystem integrated into the Apple system on chip (SoC). The Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even when the Application Processor kernel becomes compromised. It follows the

same design principles as the SoC- a Boot ROM to establish a hardware root of trust, an AES engine for efficient and secure cryptographic operations, and protected memory. Although the Secure Enclave doesn't include storage, it has a mechanism to store information security on attached storage separate from the NAND flash storage that is used by the Application processor and operating system.

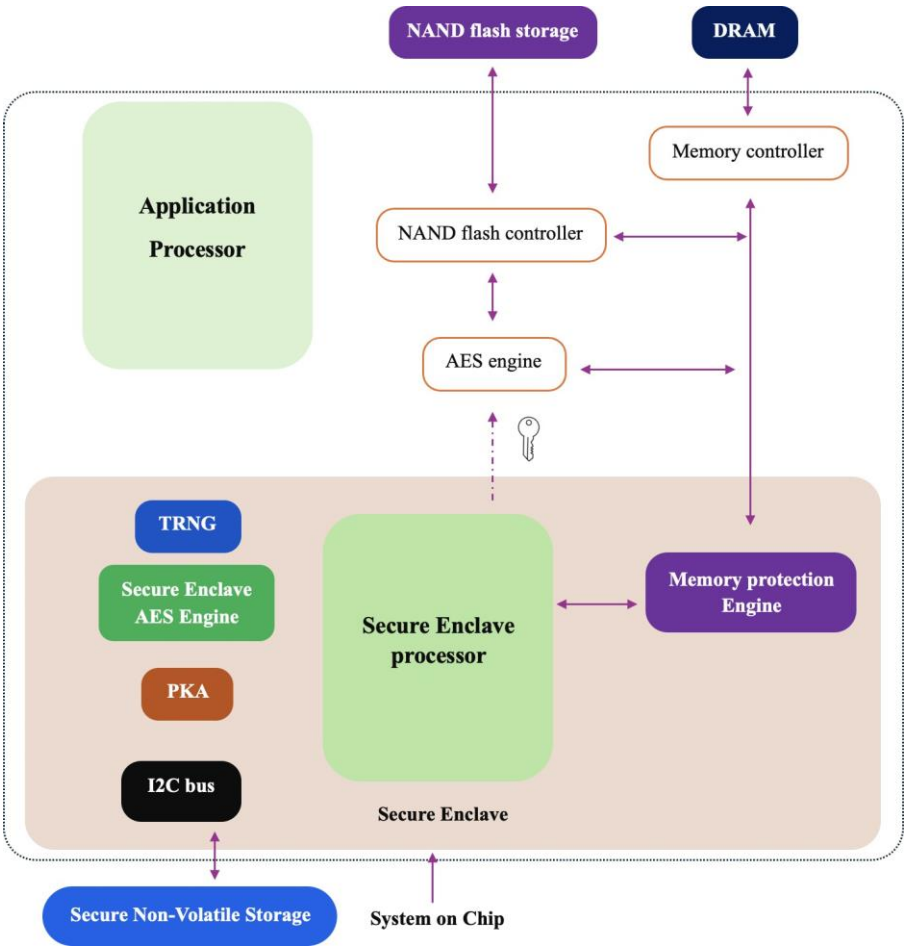


FIGURE. 5 Secure conclaves of iOS security

6.1 AES Engine

Every Apple device with a Secure Enclave also has a dedicated AES256 crypto engine (the "AES Engine") built into the direct memory access (DMA) path between the NAND (non-volatile) flash storage and main system memory, making file encryption highly efficient. On A9 or later A-series processors, the flash storage subsystem is on an isolated bus that's granted access only to memory-containing user data through the DMA crypto engine. At boot time, sepOS generates an ephemeral wrapping key using the TRNG. The Secure Enclave transmits this key to the AES Engine using dedicated wires, designed to prevent it from being accessed by any software outside the Secure Enclave. sepOS can then use the ephemeral wrapping key to wrap file keys for use by the Application Processor file-system driver. When the file-system driver reads or writes a file, it sends the wrapped key to the AES Engine, which unwraps the key. The AES Engine never exposes the unwrapped key to Software.

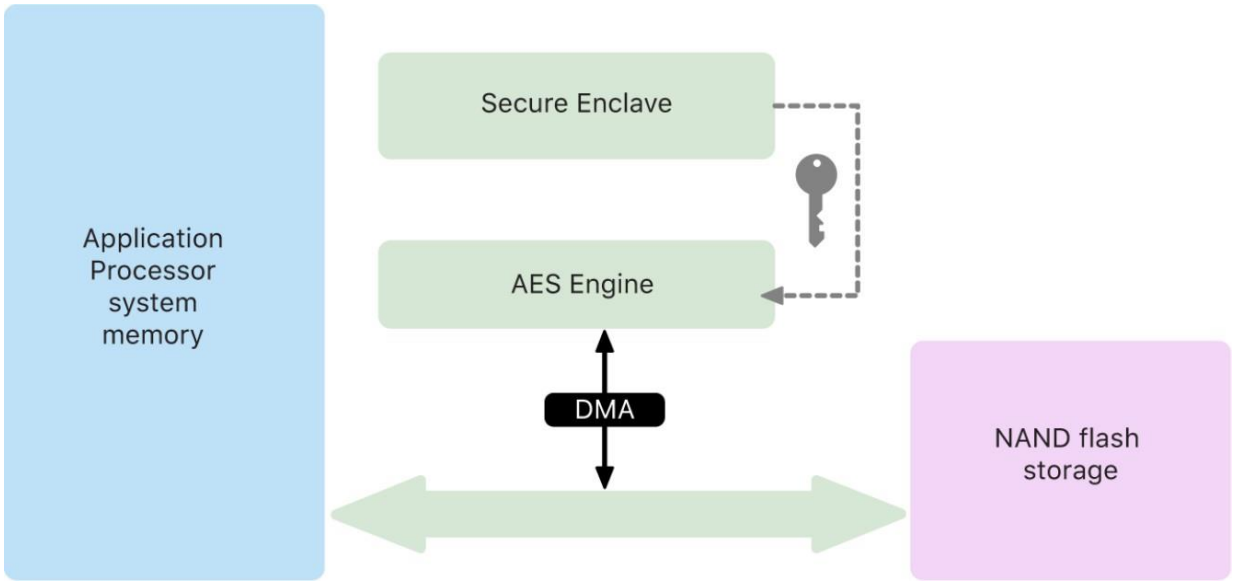


FIG. 6: AES Engine

6.2 iCloud SECURITY

iCloud stores a user's contacts, calendars, photos, documents, and more and keeps the information up to date across all their devices automatically. iCloud can also be used by third-party apps to store and sync documents as well as key values for app data as defined by the developer. Users set up iCloud by signing in with an Apple ID and choosing which services they would like to use. Certain iCloud features, such as iCloud Drive, and iCloud Backup can be disabled by IT administrators using mobile device management (MDM) configuration profiles. iCloud uses strong security methods and employs strict policies to protect user data. Most iCloud data is first encrypted on the user's device, using device-generated iCloud keys, before being uploaded to iCloud servers. For data that isn't end-to-end encrypted, the user's device securely uploads these iCloud keys to iCloud Hardware Security Modules in Apple data centres. This allows Apple to help the user with data recovery and decrypt the data on the user's behalf whenever they need it, (for example, when they sign in on a new device, restore from a backup, or access their iCloud data on the web). Data moving between the user's devices and iCloud servers is separately encrypted in transit with TLS, and iCloud servers store user data with an additional layer of encryption at rest.

6.3 ENCRYPTION AND DATA PROTECTION OVERVIEW

The secure boot chain, system security and app security capabilities all help to verify that only trusted code and apps run on a device. Apple devices have additional encryption features to safeguard user data even when other parts of the security infrastructure have been compromised (for example, if a device is lost or is running untrusted code). All these features benefit both users and IT administrators, protecting personal and corporate information and providing methods for instant and complete remote wipe in the case of device theft or loss.

6.4 DATA PROTECTION

Apple uses a technology called Data Protection to protect data stored in flash storage on devices that feature an Apple SoC — such as iPhone, iPad, Apple Watch, Apple TV and a Mac with Apple silicon. With Data Protection, a device can respond to common events, such as incoming phone calls, while at the same time providing a high level of encryption for user data. Certain system apps (such as Messages, Mail, Calendars, Contacts, and Photos) and Health data values use Data Protection by default. Third-party apps receive this protection automatically.

6.5 PROTECTING KEYS IN ALTERNATIVE BOOT MODES

Data Protection is designed to provide access to user data only after successful authentication and only to the authorized user. Data protection classes are designed to support a variety of use cases, such as the ability to read and write some data even when a device is locked (but after first unlock). Additional steps are taken to protect access to user data during alternative boot modes such as those used for Device Firmware Update (DFU) mode, Recovery mode, Apple Diagnostics or even during software updates. These capabilities are based on a combination of hardware and software features and have been expanded as Apple-designed silicon has evolved. **Official website Apple.** https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.pdf

6.6 OPERATING SYSTEM INTEGRITY

Apple's operating system software is designed with security at its core. This design includes a hardware root of trust — leveraged to enable secure boot — and a secure software update process that's quick and safe. Apple's operating systems also use their purpose-built silicon-based hardware capabilities to help prevent exploitation as the system runs. These runtime features protect the integrity of trusted code while it is being executed. In short, Apple's operating system software helps mitigate attack and exploit techniques — whether those originate from a malicious app, from the web or through any other channel. Protections listed here are available on devices with supported Apple-designed SoCs, including iOS, iPad OS, and now macOS on a Mac with Apple silicon. Official website Apple.
https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.pdf

6.7 iMessage

Apple iMessage is a messaging service for iOS devices, Apple Watch, and Mac computers. iMessage supports text and attachments such as photos, contacts, and locations. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification service (APNs). Apple doesn't log the contents of messages or attachments, which are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple can't decrypt the data. When a user turns on iMessage on a device, the device generates two pairs of keys for use with the service: an RSA 1280-bit key for encryption and an ECDSA 256-bit key on the NIST P-256 curve for signing. The private keys for both key pairs are saved in the device's Keychain and the public keys are sent to Apple Identity Service (IDS), where they are associated with the user's phone number or email address, along with the device's APNs address. APNs can only relay messages up to 4KB or 16KB in size, depending on the iOS version. If the message text is too long, or if an attachment such as a photo is included, the attachment is encrypted using AES in CTR mode with a randomly generated 256-bit key and uploaded to iCloud. The AES key for the attachment, its URI (Uniform Resource Identifier), and a SHA-1 hash of its encrypted form are then sent to the recipient as the contents of an iMessage, with their confidentiality and integrity protected through normal iMessage encryption, as shown in the following diagram.

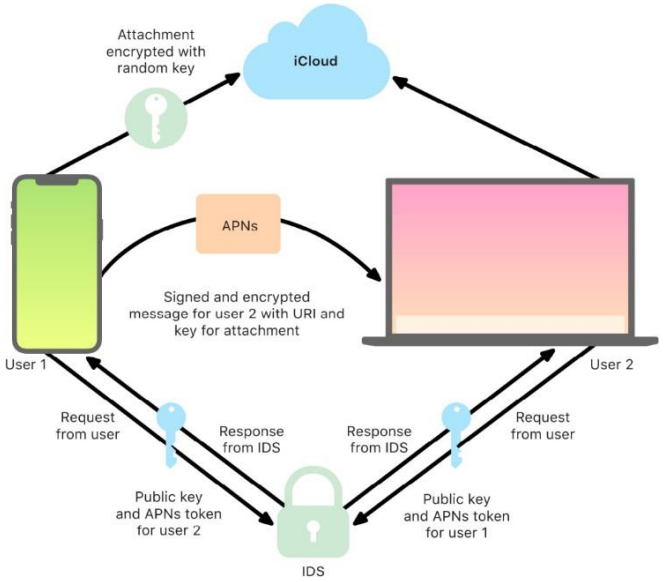


FIG. 7: iMessage

7. Conclusion of iOS security

Apple's robust security architecture, including the Secure Enclave, iCloud security, encryption, and data protection measures, significantly enhances user privacy and data integrity. However, these same features present notable challenges for digital investigators and law enforcement agencies. The Secure Enclave operates as a dedicated secure subsystem within Apple's System on Chip (SoC). By isolating sensitive operations from the main processor, it ensures that critical user data remains protected even if the main operating system is compromised. This architecture employs a secure boot chain, AES encryption, and protected memory, creating a barrier that is challenging for forensic investigators to penetrate. The Data Protection technology further complicates forensic analysis by encrypting data stored on devices, making it accessible only after successful user authentication. Investigators may struggle to retrieve encrypted data without user credentials, rendering traditional forensic techniques less effective. iCloud's strong security protocols, including device-generated encryption keys and end-to-end encryption for certain data, pose challenges for investigators seeking access to user data stored in the cloud. Although Apple implements encryption at rest and in transit, the reliance on user authentication for data recovery complicates investigations, particularly in cases where users are uncooperative or unavailable. Apple's encryption methods, including the AES engine and ephemeral wrapping keys generated during the boot process, further secure data. Investigators face difficulties in decrypting files without the appropriate keys, which are securely managed within the Secure Enclave. Moreover, because the AES engine never exposes unwrapped keys to software outside the enclave, gaining access to user data without consent becomes increasingly complex. Apple's operating system integrity measures, designed to mitigate exploitation risks, reinforce the security of the device. The secure boot process, coupled with hardware-based protections, means that unauthorized modifications to the operating system are difficult to achieve. This integrity makes it challenging for investigators to analyze the system without alerting security features that may wipe or lock the device upon detection of unauthorized access. iMessage employs end-to-end encryption, ensuring that only the sender and recipient can access message contents. This level of security complicates the efforts of law enforcement to access potentially vital communication data during investigations, as Apple cannot decrypt messages, nor does it store their contents. The encryption of attachments and the use of key pairs stored within the device's Keychain present additional hurdles for forensic analysis.

8. DIGITAL FORENSIC MODELS AND LEGAL GUIDELINES

The literature review highlights a wide range of mobile forensic models, yet the number of models specifically designed for iOS devices remains limited, as seen in Table 3. While some digital forensic models focus on collecting evidence from iPhones and iPads such as recovering deleted data and analyzing network traffic the

integration of machine learning frameworks in these models has not been thoroughly explored in existing studies. Recent advancements in digital forensics have been driven largely by the rise of cybercrimes, which have become a significant challenge for law enforcement agencies worldwide. Investigating crimes involving iOS devices adds further complexity due to Apple's robust security features, which are designed to protect user data. Forensic models tailored specifically for iOS are crucial for addressing these challenges, enabling investigators to extract critical evidence such as communication logs, multimedia files, location data, and more. the forensic process is not just about evidence collection but also involves proper analysis, reporting, and ensuring the admissibility of the evidence in court. One of the most critical challenges is maintaining the chain of custody throughout the investigation [38], [42].

S no	iOS Mobile Devices Forensic models and guidelines	years
1	iPhone forensic: recovering evidence, personal data, and corporate assets	2008
2	iPhone forensic	2009
3	iPhone 3Gs forensics: a logical analysis using apple iTunes backup utility	2010
4	Campbell, iOS forensic analysis for iPhone, iPad, and iPod touch	2010
5	iForensic: forensic analysis of instant messaging on smartphone, in digital forensic and cyber crime	2010
6	iPhone and iOS forensic: Investigation analysis and mobile security iOS devices	2011
7	A simple cost-effective framework for the iPhone forensic analysis, in digital forensic cyber crimes	2011
8	Sensitive privacy data acquisition in the iPhone for digital forensic analysis	2011
9	Third- party application forensic on iOS mobile devices	2011
10	Analysis of Smart phone based location information	2012
11	Forensic analysis of social media networking application on iOS mobile devices	2012
12	Forensic analysis techniques for fragmented flash memory pages in iOS devices	2012
13	Versatile iPad forensic acquisition using the Apple camera connection kit	2012
14	A novel method of iOS devices forensic without jailbreaking	2012
15	ACPO guidelines	2012
16	Analysis of the forensic traces left by AirPrint in iOS devices	2013
17	Design and implementation of digital forensic software for iOS devices	2013
18	Forensic analysis of social media networking application on iOS devices	2013
19	Fast data acquisition with a mobile devices in digital crime	2013
20	Analytical Crime Scene investigation model	2013
21	Advance data acquisition model	2013
22	Integrated digital investigation process (IDIP)	2014
23	Scientific working group on digital evidence(SWGDE) guidelines	Regular Update
24	National institute of standard and technology (NIST) guidelines	Regular Update
25	INTERPOL Guidelines for Digital forensic laboratories	2019
26	ENFSI Guidelines	2020-23

TABLE 3. Digital forensic guidelines and models

9. EVIDENCE ACQUISITION PHASES

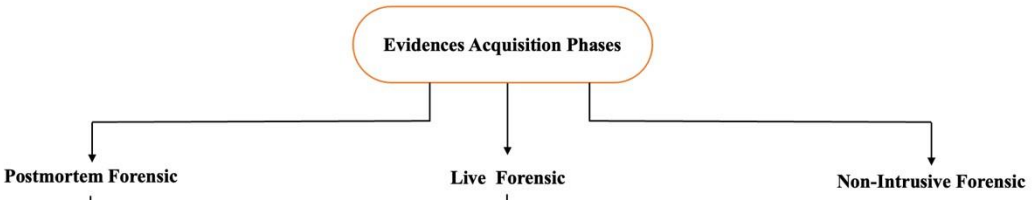


FIG. 8: Evidence acquisition phases

9.1 LOGICAL ACQUISITION ON IOS MOBILE DEVICES

Logical acquisition is a method of extracting data from a mobile device that does not involve creating a physical copy of the entire storage but focuses on the data that is accessible through the device's operating system and interfaces. Here's a general overview of the process of logical acquisition on iOS mobile devices:

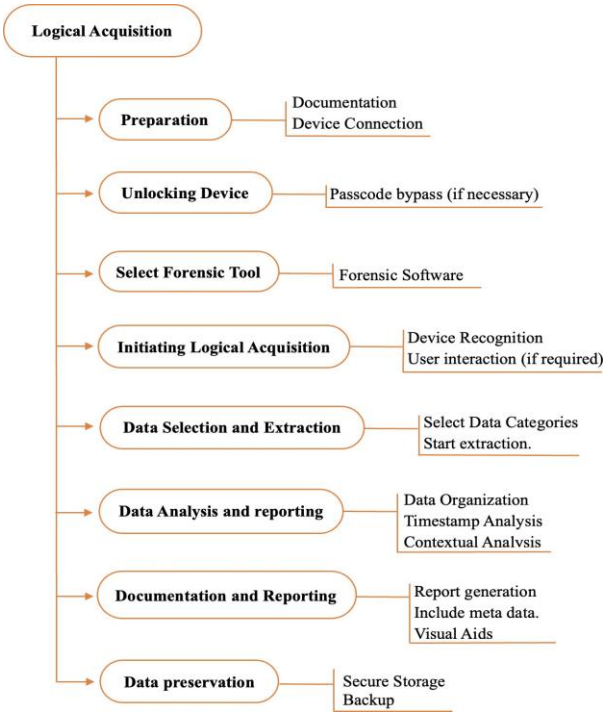


FIG. 9: Logical Acquisition Phases

Preparation

Documentation: Document the device's make, model, iOS version, and any other relevant information.

Device Connection: Connect the iOS device to a forensic computer using a USB cable. Ensure the device is recognized and authorized by the computer.

Unlocking the Device

Passcode Bypass (if necessary): If the device is locked and the passcode is not available, some forensic tools might provide limited access or bypass options. However, the legality and ethics of this process may vary by jurisdiction.

Selecting the Right Tool

Forensic Software: Use a forensic software tool (such as Cellebrite UFED, Oxygen Forensic Detective, or others) capable of logical acquisition from iOS devices. Ensure the software is updated to support the specific iOS version on the device.

Initiating Logical Acquisition

Device Recognition The forensic software will recognize the connected iOS device. Ensure that the software establishes a stable connection with the device.

User Interaction (if required) Some devices might require the user to grant access permissions for data extraction. Prompt the user on the device screen to authorize the data transfer if necessary.

Data Selection and Extraction

Selecting Data Categories: Choose the specific data categories to extract. Common categories include contacts, call logs, messages, photos, videos, and application data.

Start Extraction: Initiate the extraction process through the forensic software. The software will send commands to the iOS device to retrieve the selected data.

Data Analysis and Reporting

Data Organization: Organize the extracted data into relevant categories for analysis. Different types of data (messages, photos, etc.) are often stored separately for easier examination.

Timestamp Analysis: Analyze timestamps to establish timelines of events and activities.

Contextual Analysis: Understand the context of messages, emails, or other communications. Analyze relationships between different types of data.

Documentation and Reporting

Report Generation: Create a detailed forensic report documenting the logical acquisition process, methods used, and the extracted data.

Include Metadata: Document metadata such as timestamps, device information, and any relevant context.

Visual Aids**:** Use visual aids like timelines, charts, and graphs to present complex data relationships.

Data Preservation

Secure Storage: Preserve the extracted data in a secure, tamper-evident storage environment to maintain its integrity until required for legal proceedings.

Backup: Create backup copies of the extracted data to prevent loss due to hardware failures or other unforeseen events [43], [46].

9.2 PHYSICAL ACQUISITION ON IOS MOBILE DEVICES

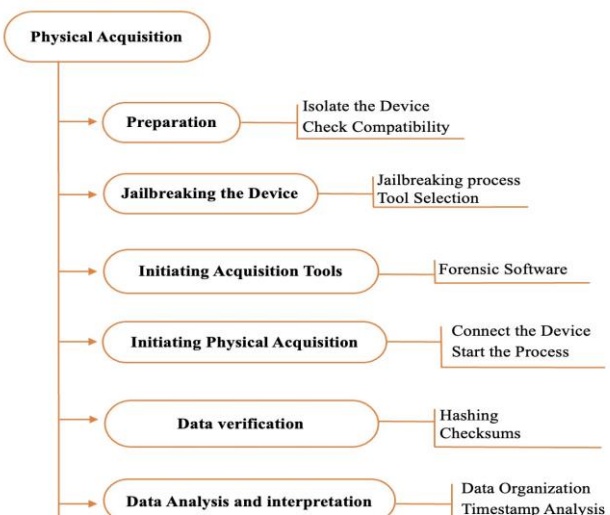


FIG. 10: Physical Acquisition Phases

The physical acquisition involves creating a bit-by-bit copy of the entire storage of an iOS device, capturing not only active data but also deleted, hidden, and system files. Performing a physical acquisition on iOS devices often requires exploiting security vulnerabilities, such as jailbreaking, to bypass device protections. It's essential to note that this process can be complex, time-consuming, and may void the device's warranty. Legal and ethical considerations must be taken into account it's crucial to consult with legal experts and adhere to applicable laws and regulations before attempting physical acquisition. Here's a general overview of the process of physical acquisition on iOS mobile devices.

Device Preparation

Isolate the Device: Place the iOS device in a Faraday bag or shielded container to prevent remote wiping or tampering. Check Compatibility: Verify that the device model and iOS version are compatible with the physical acquisition tool to be used.

Jailbreaking the Device:

Jailbreaking Process: Perform the jailbreaking process, which involves exploiting vulnerabilities in the iOS operating system to gain root access. This step allows the installation of custom software and access to the device's file system. Tool Selection: Use a reputable jailbreaking tool compatible with the device's iOS version. Note that new iOS updates often patch existing jailbreaking methods.

Installing Acquisition Tools Forensic Software**:** Install forensic software (such as Cellebrite UFED, GrayKey, or other specialized tools) capable of physical acquisition on the jailbroken iOS device. Ensure the software supports the iOS version and device model.

Initiating Physical Acquisition

Connect the Device: Connect the jailbroken iOS device to a forensic computer using a USB cable.
Start the Process: Initiate the physical acquisition process through the forensic software. This process will create a forensic image of the device's storage, capturing all data, including deleted information.

Data Verification

Hashing: Generate hash values of the acquired data to verify its integrity. Compare these hash values with the hash values of the original device to ensure data integrity.
Checksums: Check for file and data integrity using checksums. Compare these values with known checksums of the original files.

Data Analysis and Interpretation

Data Organization: Organize the acquired data into categories (contacts, messages, media files, etc.) for easier analysis.
Timestamp Analysis: Examine timestamps to create a timeline of events and activities.

Contextual Analysis: Understand the context of messages, emails, or other communications. Analyze relationships between different types of data.

Documentation and Reporting

Report Generation: Create a detailed forensic report documenting the physical acquisition process, methods used, and the extracted data.

Include Metadata: Document metadata such as timestamps, device information, and any relevant context.

Visual Aids: Use visual aids like timelines, charts, and graphs to present complex data relationships.

Data Preservation

Secure Storage: Preserve the acquired data in a secure, tamper-evident storage environment to maintain its integrity until required for legal proceedings.

Backup: Create backup copies of the acquired data to prevent loss due to hardware failures or other unforeseen events. [47], [51].

10. iOS MOBILE FORENSIC TOOLS AND FEATURES

Digital forensic tools play a pivotal role in the investigation of mobile devices, particularly iOS platforms. These tools can be broadly categorized into commercial and open-source solutions, each offering unique advantages and challenges across various forensic phases, including acquisition, analysis, and reporting. Additionally, legal considerations and emerging challenges significantly impact the effectiveness and reliability of these tools. The use of digital forensic tools is subject to stringent legal standards, including the need for proper chain of custody, adherence to privacy laws, and compliance with local and international regulations. Commercial tools are often designed with these legal frameworks in mind, offering documentation and support to help investigators maintain compliance. However, open-source tools may lack formal legal documentation, which could pose challenges in court regarding their validity and reliability. Forensic practitioners must be mindful of the admissibility of evidence obtained through these tools and ensure that proper procedures are followed throughout the investigation. Both commercial and open-source digital forensic tools have distinct roles in mobile device investigations. Each type has strengths and weaknesses across forensic phases, legal considerations, and challenges [52], [64].

Tools	Source	Features
Cellebrite UFED	Commercial	• Physical extraction of data • Support a wide range of iOS versions and devices models • Advance analysis features including decoding deleted data • Generate report
Magnet AXIOM	Commercial	• Recover deleted data • Support integration with third party -tools for deeper analysis • Generate customizable report
Oxygen forensic Detective	Commercial	• Extract data including iCloud backup • Analysis multiple type of data, Call logs, messages and app data, • Recover deleted data • Advance search and filtering capabilities • Support time line analysis for reconstructing events
Elcomsoft iOS forensic Toolkit	Commercial	• Extract data including locked and disabled devices • Decrypts encrypted backups and extracts keychain data • Recover deleted data and password • Provide comprehensive analysis and reporting tools • Supports physical and logical acquisitions
GrayKey	Commercial	• Provide both physical and logical acquisitions • Supports latest iOS versions • Bypasses device lock screens for data extraction • Recover deleted data • Generate details reports
Xray	Commercial	• Extracted data including locked and damaged devices

Tools	Source	Features
iBackup Viewer	Commercial	• Recovers various type of data, massages, call logs, and app data • Supporting browsing and exporting data in various formats • Provide advanced filtering options • Allow to integrate with other forensic tools
iExplorer	Commercial	• Support various type of data including backups and app data • Recover deleted data and password • Supporting browsing and exporting data in various formats • Provide user friendly interface • Allow to integrate with forensic tools for comprehensive analysis and reporting
EnCase Forensic	Commercial	• Extracts and analyses data including deleted data and file artifacts • Recover passwords and bypasses devices lock for data acquisitions • Supporting comprehensive analysis and reporting features • Allow to integrate with other forensic tools for cross-platform investigations • Provide advanced keyword search and filtering capabilities
Axiom	Commercial	• Extract data including cloud backups and app data • Recovers deleted data and passwords • Support advanced parsing and analysis on iOS artifacts • Allow to integrate with forensic tools for comprehensive investigations
Andriller	Open source	• Extract data including backups and file system images • Recovers various types of data, massages, call logs, and multimedia file • Support SQLite data base analysis • Allow to integrate with forensic tools for cross platform analysis
iPhone backup Analyzer	Open Source	• Analysis iOS devices backups • Extract various types of data including messages, call logs, and app data • Support SQLite database analysis • Allow for custom scripting for advanced analysis
Autopsy	Open source	• Performs automated analysis of iOS devices images • Recover various type of data including, massages, call logs, and media file • Support keyword search and filtering • Generate comprehensive reports • Offer extensibility through modules for additional analysis and processing

TABLE 4. Digital forensic tools and features

11. FUTUI

The future direction of research in iOS mobile device forensic investigation, integrated with machine learning (ML) frameworks, presents several promising directions. One key area is the automation of data extraction and analysis, where ML models can streamline the identification of critical evidence from vast amounts of data, improving efficiency and reducing human error. Cross-platform forensic capabilities are also critical, allowing investigators to analyze data across the Apple ecosystem, including iPhones, iPads, and cloud environments such as iCloud. As iOS security continues to evolve, future research must address challenges posed by encrypted data and cloud-based services. Ethical and legal considerations, including bias in algorithms and the

transparency of ML models, will also be a crucial research area to ensure the reliability and acceptance of ML in forensic investigations.

12. CONCLUSION

In this review, we have explored the intersection of iOS mobile device forensic investigation and machine learning, highlighting the significant advancements and challenges in the field. The integration of machine learning techniques has proven to enhance traditional forensic methodologies by improving data analysis efficiency, pattern recognition, and predictive analytics. This synergy not only facilitates the extraction of relevant evidence but also aids in addressing the evolving complexities of mobile device data. As iOS devices continue to proliferate, the volume and variety of data generated pose unique challenges for forensic investigators. Machine learning offers promising solutions for automating the classification and interpretation of vast datasets, thus accelerating the investigative process. However, the reliance on these advanced techniques necessitates a robust understanding of the underlying algorithms and their implications for data integrity and privacy. Future research should focus on developing standardized frameworks and best practices for the implementation of machine learning in forensic investigations. Additionally, addressing the ethical considerations and ensuring transparency in machine learning applications will be critical to maintaining the integrity of forensic processes. By fostering collaboration between forensic experts, data scientists, and legal professionals, we can pave the way for more effective and accountable forensic investigations in the digital age.

References

[1] Arikan, S. M., & Yurekten, O. (2021, June 28). Development and Maintenance of Mobile Forensic Investigation Software Modules. *9th International Symposium on Digital Forensics and Security, ISDFS 2021*. https://doi.org/10.1109/ISDFS52919.2021.9486353

[2] Chen, H., & Zhao, X. (2023). Machine learning for anomaly detection in digital forensics: A review. Computers & Security, 113, 102587.

[3] Hutchinson, S., Stanković, M., Ho, S., Houshmand, S., & Karabiyik, U. (2023). Investigating the Privacy and Security of the SimpliSafe Security System on Android and iOS. *Journal of Cybersecurity and Privacy*, *3*(2),145–165. https://doi.org/10.3390/jcp3020009

[4] Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys*, *51*(3). https://doi.org/10.1145/3177847

[5] Casey, E. (2020). Handbook of Digital Forensics and Investigation. Academic Press.

[6] Williams, J., Macdermott, A., Stamp, K., & Iqbal, F. (2021). Forensic Analysis of Fitbit Versa: Android vs iOS. *Proceedings - 2021 IEEE Symposium on Security and Privacy Workshops, SPW 2021*, 318–326. https://doi.org/10.1109/SPW53761.2021.00052

[7] Chernyshev, M.,Zeadally, S.,Baig, Z., &Woodward, A.(n.d.). *DIGITAL FORENSICS, PART 1*. www.computer.org/security

[8] Baggili, I., Breitinger, F., Al-Khateeb, H., Marrington, A., & Moore, J. (2020). Implementing machine learning in mobile device forensics: A practical survey. Journal of Digital Forensics, Security and Law, 15(1),1-15.

[9] Jain, N., & Jain, P. (2019). Applications of Machine Learning in Digital Forensics. Journal of Digital Forensic Practice, 11(3), 123-140.

[10] Alomari, M., Alogaiel, R., Alghulayqah, H., & Alsadah, S. (n.d.-b). *Mobile investigation; Forensics analysis of iOS devices*. https://doi.org/10.13140/RG.2.2.16584.60169

[11] Barreto, W., Waghmare, N. P., & Saran, V. (n.d.). Social Media Application Security Extraction and Analysis on Mobile Devices Section A-Research paper 1729 Eur. In *Chem. Bull* (Vol. 2023).

[12] Moreb, M., & Salah, S. (2023). *A Novel Framework for Mobile Forensics Investigation Process*. https://doi.org/10.21203/rs.3.rs-2611927/v1

[13] Alenezi, M., Khan, N., & Ahmed, M. (2020). Machine Learning in Digital Forensics: A Review. International Journal of Computer Applications, 175(7), 30-38.

[14] Conti, M., Dehghantanha, A., & Watson, S. (2021). Machine learning in forensic computing: A review. IEEE Security & Privacy, 19(3), 9-16.

[15] Brkić, J., Pančević, P., & Preneel, B. (2022). Ethical considerations in AI-based digital forensics. Forensic

Science International: Digital Investigation, 41, 301008
[16] Ferguson, A. (2020). The Legal and Ethical Implications of Using AI in Forensic Science. Journal of Law and Technology, 12(2), 145-162.
[17] Ayers, D., Brothers, S., & Jansen, W. (2019). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Revision 1.
[18] Conti, M., Dehghantanha, A., & Watson, S. (2021). Machine learning in forensic computing: A review. IEEE Security & Privacy, 19(3), 9-16.
[19] Li, S., Sun, J., & Zhang, Y. (2022). Leveraging machine learning for advanced mobile forensics. Digital Investigation, 38, 301081.
[20] Casey, E. (2022). Handbook of Digital Forensics and Investigation. Academic Press.
[21] Baggili, I., Breitinger, F., Al-Khateeb, H., Marrington, A., & Moore, J. (2020). Implementing machine learning in mobile device forensics: A practical survey. Journal of Digital Forensics, Security and Law, 15(1), 1-15.
[22] Ahmed, I., & Dharaskar, R. V. (2020). Machine learning techniques for improving data acquisition in iOS forensics. International Journal of Computer Applications, 175(9), 22-28.
[23] Sharma, R., & Mehrotra, H. (2021). Enhanced forensic analysis of iOS applications using machine learning.
Forensic Science International: Digital Investigation, 35, 301093.
[24] Brkić, J., Pančević, P., & Preneel, B. (2022). Ethical considerations in AI-based digital forensics. Forensic Science International: Digital Investigation, 41, 301008.
[25] Chen, H., & Zhao, X. (2023). Machine learning for anomaly detection in digital forensics: A review. Computers & Security, 113, 102587.
[26] Sharma, Y. K., Noval, S. S., Jain, A., Sabitha, B., & Ramya, T. (2022). Forensics-as-a-service: A Review of Mobile Forensics. *Proceedings of 5th International Conference on Contemporary Computing and Informatics, IC3I 2022*, 486–491. https://doi.org/10.1109/IC3I56241.2022.10072726
[27] Van Bussel, J. C., Le-Khac, N.-A., & Kechadi, M.-T. (2020). The challenges of applying machine learning in digital forensic investigations. Digital Investigation, 33, 301093.
[28] Zollner, S., Choo, K. K. R., & Le-Khac, N. A. (2019). An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems. *IEEE Access*, *7*, 158250–158263. https://doi.org/10.1109/ACCESS.2019.2948774
[29] Da Costa, A. M., De Sa, A. O., & Machado, R. C. S. (2022). Data Acquisition and extraction on mobile devices-A Review. *2022 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2022 - Proceedings*, 294–299. https://doi.org/10.1109/MetroInd4.0IoT54413.2022.9831724
[30] Balushi, Y. Al, Shaker, H., & Kumar, B. (2023a). The Use of Machine Learning in Digital Forensics: Review Paper. In *Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)* (pp. 96–113). Atlantis Press International BV. https://doi.org/10.2991/978-94- 6463-110-4_9
[31] Nayerifard, T., Amintoosi, H., Bafghi, A. G., & Dehghantanha, A. (2023). *Machine Learning in Digital Forensics: A Systematic Literature Review*. http://arxiv.org/abs/2306.04965
[32] Al-Dhaqm, A., Razak, S. A., Ikuesan, R. A., Kebande, V. R., & Siddique, K. (2020a). A review of mobile forensic investigation process models. In *IEEE Access* (Vol. 8, pp. 173359–173375). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.3014615
[33] Burrington, I. (2022). "AI and the Future of Mobile Forensics." Digital Investigation Insights.
[34] Vincent, N., & Dragland, Å. (2020). "The Impact of AI and ML on Mobile Forensics." European Journal of Digital Forensics.
[35] Woodward, J. (2021). "Navigating AI in iOS Forensics: Legal and Ethical Challenges." Forensic Science International.
[36] Hutchinson, S., Stanković, M., Ho, S., Houshmand, S., & Karabiyik, U. (2023). Investigating the Privacy and Security of the SimpliSafe Security System on Android and iOS. *Journal of Cybersecurity and Privacy*, *3*(2), 145–165. https://doi.org/10.3390/jcp3020009 .
[37] Bakır, Ç., & Yüzkat, M. (2022). A Review about Forensic Informatics and Tools. In *Journal of Emerging Computer Technologies* (Vol. 2, Issue 2). APA.
[38] Saha, D., Karmakar, S., Nur, F. N., Mariam, A., Moon, N. N., & Ahmed, A. (2021, August 10). Mobile device and social media forensic analysis: Impacts on cyber-crime. *2021 1st International Conference on Emerging Smart Technologies and Applications, ESmarTA 2021*. https://doi.org/10.1109/eSmarTA52612.2021.9515742
[39] Pathak, J., Sankaran, S., & Achuthan, K. (2019). A SMART Goal-based Framework for Privacy Preserving Embedded Forensic Investigations. *Proceedings of the 2019 International Symposium on Embedded Computing and System Design, ISED 2019*, 6–10. https://doi.org/10.1109/ISED48680.2019.9096232
[40] Alashjaee, A. M., & Haney, M. (2021). Forensic Requirements Specification for Mobile Device Malware

Forensic Models. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 930–935. https://doi.org/10.1109/CCWC51732.2021.9376043
[41] Ayers, D., Brothers, S., & Jansen, W. (2019). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101 Revision 1.
[42] Al-Bassam, M., Zamani, M., & Hassan, M. (2019). Advances in iOS Forensics: Current Techniques and Future Directions. Journal of Digital Forensics, Security and Law, 14(2), 89-105.
[43] Bernardo, B., & Santos, V. (2020). *Mobile Device Forensics Investigation Process* (pp. 256–288). https://doi.org/10.4018/978-1-7998-5728-0.ch014
[44] Laayu, M. R., Kurniawan, A., Cahyani, N. D. W., & Satrya, G. B. (2022). Comparison of Acquisition Results on iPhone 7 Plus (iOS 14.8.1) between Jailbreaking vs Non-Jailbreaking Device. *2022 10th International Conference on Information and Communication Technology, ICoICT 2022*, 402–406. https://doi.org/10.1109/ICoICT55009.2022.9914862
[45] Alatawi, H., Alenazi, K., Alshehri, S., Alshamakhi, S., Mustafa, M., & Aljaedi, A. (2020, September 9). Mobile Forensics: A Review. *2020 International Conference on Computing and Information Technology, ICCIT 2020*. https://doi.org/10.1109/ICCIT-144147971.2020.9213739
[46] Bays, J., & Karabiyik, U. (n.d.). *Forensic Analysis of Third Party Location Applications in Android and iOS*.
[47] Freiling, F., Groß, T., Latzo, T., Müller, T., & Palutke, R. (2018). Advances in Forensic Data Acquisition. *IEEE DesignandTest*,*35*(5), 63–74. https://doi.org/10.1109/MDAT.2018.2862366
[48] Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, *38*. https://doi.org/10.1016/j.fsidi.2021.301169
[49] Heath, H., MacDermott, Á., & Akinbi, A. (2023). Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? *Forensic Science International: Digital Investigation*, *46*. https://doi.org/10.1016/j.fsidi.2023.301585
[50] Hutchinson, S., Shantaram, N., & Karabiyik, U. (n.d.). *Forensic Analysis of Dating Applications on Android*
And iOS Devices. https://doi.org/10.1109/TrustCom50675.2020.00113/20/$31.00
Investigation Apple Devices Acquisition & Analysis. (n.d.-a).
[51] Pooters, I. (2010). Full user data acquisition from Symbian smart phones. *Digital Investigation*, *6*(3–4), 125–135. https://doi.org/10.1016/j.diin.2010.01.001
[52] Dragonas, E., Lambrinoudakis, C., & Kotsis, M. (2023b). IoT forensics: Analysis of a HIKVISION's mobile app. *Forensic Science International: Digital Investigation*, *45*. https://doi.org/10.1016/j.fsidi.2023.301560
[53] Joun, J., Lee, S., & Park, J. (2023a). Discovering spoliation of evidence through identifying traces on deleted files in macOS. *Forensic Science International: Digital Investigation*, *44*. https://doi.org/10.1016/j.fsidi.2023.301502
[54] Humphries, G., Nordvik, R., Manifavas, H., Cobley, P., & Sorell, M. (2021a). Law enforcement educational
challenges for mobile forensics. *Forensic Science International: Digital Investigation*, *38*. https://doi.org/10.1016/j.fsidi.2021.301129
[55] Lwin, H. H., Aung, W. P., & Lin, K. K. (n.d.). *Comparative Analysis of Android Mobile Forensics Tools*.
Montasari, R., & Hill, R. (2019). Next-Generation Digital Forensics: Challenges and Future Paradigms; Next-Generation Digital Forensics: Challenges and Future Paradigms. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*.
[56] Murias, J. G., Levick, D., & McKeown, S. (2023a). A forensic analysis of streaming platforms on Android OS. *Forensic Science International: Digital Investigation*, *44*. https://doi.org/10.1016/j.fsidi.2022.301485
[57] Nishshanka, L. C. B., Shepherd, C., Ariyarathna, M. R., Weerakkody, L., & Palihena, J. (2021). An android-
based field investigation tool to estimate the potential trajectories of perforated AK bullets in 1 mm sheet metal, surfaces. *Forensic Science International: Digital Investigation*, *38*. https://doi.org/10.1016/j.fsidi.2021.301267
[58] Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. In *Forensic Science International: Synergy* (Vol. 6). Elsevier B.V. https://doi.org/10.1016/j.fsisyn.2022.100313
[59] Riadi, I., Yudhana, A., & Inngam Fanani, G. P. (2023). Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation. *International Journal of Safety and Security Engineering*, *13*(1), 11–19. https://doi.org/10.18280/ijsse.130102
[60] Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, *45*. https://doi.org/10.1016/j.fsidi.2023.301554

[61] Zhang, X., Liu, C. Z., Choo, K. K. R., & Alvarado, J. A. (2021). A design science approach to developing an integrated mobile app forensic framework. *Computers and Security*, *105*. https://doi.org/10.1016/j.cose.2021.102226
[62] Studiawan, H., Ahmad, T., Santoso, B. J., & Pratomo, B. A. (2022a). Forensic Timeline Analysis of iOS Devices. *8th International Conference on Engineering and Emerging Technologies, ICEET 2022*. https://doi.org/10.1109/ICEET56468.2022.10007150
[63] Sumaila, F., & Bahsi, H. (2022). Digital forensic analysis of mobile automotive maintenance applications. *Forensic Science International: Digital Investigation*, *43*. https://doi.org/10.1016/j.fsidi.2022.301440
[64] Xiao, J., Li, S., & Xu, Q. (2019). Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation. *IEEE Access*, *7*, 55432–55442. https://doi.org/10.1109/ACCESS.2019.2913648