International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Exploring Mobile Forensic Investigations of Smartphones Using the Cellebrite UFED Tool

Padmawati Soni[1], Dr. Mahesh Pawar[2], Dr. Piyush Kumar Shukla[3]

[1,2,3]University Institute of Technology, R.G.P.V Bhopal (M.P.)

Abstract

Digital devices now dominate the computing field because smartphone adoption rates led to smartphones becoming storage units for very sensitive personal data accessible in one device. The small handheld devices maintain extensive digital traces of user data including SMS communications and email records and call records in addition to payment transactions as well as biometric information and GPS tracking reports. These devices serve as essential evidence materials for digital forensics teams during investigations about cybercrime and law enforcement activities and corporate espionage cases and national security matters. The Cellebrite UFED (Universal Forensic Extraction Device) functions as the top mobile forensic tool by providing leading-edge data acquisition together with decryption and analysis functionalities. The UFED system serves worldwide digital forensic experts and law enforcement and intelligence agencies to extract data from multiple mobile operating systems through logical and physical and multiple layer imaging approaches. This paper conducts a detailed examination of Cellebrite UFED that includes its technical design structure and operational procedures together with its forensic examination workflow. This paper displays a continual workflow of mobile forensic operations starting with gadget capturing and evidence conservation then continuing to investigative data evaluation and producing court-approved summary reports. The tool's practical value is demonstrated through analysis of an actual cyberstalking case which accompanies the research. The paper conducts an in-depth critique of UFED to analyze its advantages alongside constraints as well as the legal, ethical and privacy-related challenges that come with it. By performing multiple analyses the research demonstrates that Cellebrite UFED remains essential for achieving accurate investigations and dependable evidence and upholding judicial standards in present-day digital cases.

Keywords: Mobile Forensics, Digital Evidence, Cellebrite UFED, Smartphone Investigation, Data Extraction, UFED Report, Cybercrime, Android, iOS.

1. INTRODUCTION

In today's hyper-connected digital ecosystem, smartphones have become much more than just communication devices. They function as compact, multifunctional computing platforms that store a vast array of sensitive personal and professional data. From financial applications and health monitoring tools to social networking platforms and corporate email accounts, smartphones encapsulate a digital snapshot of a user's life[1]. Technical devices have gained importance in digital investigations because they trace digital evidence trails from criminal activities.

Mobile forensic investigations have gained more significance because cyber-related crimes including cyberbullying and stalking alongside financial fraud and identity theft and insider threats are appearing

with increasing frequency. The information found within smartphones includes vital evidence comprised of telephone records and text messages alongside software activities and global positioning data as well as internet history and multimedia content and cryptographic communications[1]. The process of accessing mobile device information becomes difficult because security measures advance while encryption protects data and operating systems maintain regular updates. Law enforcement officials together with forensic professionals can lawfully obtain mobile device data through Cellebrite UFED using its scanning capabilities for extracting and analyzing information from protected devices. The tool delivers advanced functionality that offers logical and physical extraction features and enables access to deleted information and lock screen bypass and decoded secure messaging applications.

The research examines how the Cellebrite UFED [9]functions for mobile forensic investigations. A research investigation investigates the technological structure and forensic workflow of UFED while demonstrating practical uses and actual case applications to prove how UFED functions as crucial forensic tool for smartphone evidence retrieval. Data integrity alongside legal compliance and ethical standards play dual roles in establishing their importance during mise en place forensic work in mobile technology investigations.

2. Mobile Forensics

The special discipline of digital forensics called mobile forensics deals with the collection identification and analytical assessment and conservation and display of digital proof stored on smartphones among other cellular devices[1][2]. As mobile devices become an integral part of personal and professional life, they have become critical sources of evidence in criminal, civil, corporate and intelligence investigations. The science of mobile forensics involves the use of forensic-grade tools and methodologies that ensure data integrity and legal admissibility. Unlike traditional computer forensics, which is primarily concerned with standard hardware platforms and file systems, mobile forensics must navigate a dynamic and fragmented ecosystem. Investigators face a wide variety of mobile operating systems (e.g. Android, iOS, HarmonyOS), proprietary hardware configurations, boot loaders and storage formats. In addition, the accelerated pace of mobile OS updates and the use of vendor-specific security enhancements create constant challenges for forensic tool compatibility and access techniques[2][3].

The goal of mobile forensics is to extract both active and residual (deleted or hidden) data while maintaining forensic integrity - ensuring that the original evidence remains unaltered and fully verifiable.

2.1 Common challenges in mobile forensics

1. Advanced encryption mechanisms Modern smartphones implement sophisticated encryption protocols by default. Android devices use File-Based Encryption (FBE), which encrypts different files with different keys depending on user interaction (e.g. screen unlock). Apple's iOS uses Data Protection Classes, which tie encryption keys to the device passcode and biometric data. These mechanisms severely limit access to raw data without prior authentication or bypass[4].

2. Application sandboxing and data isolation Most mobile operating systems enforce sandboxing, a security architecture that isolates application data in separate containers. Without elevated privileges (such as root access or jailbreaking), forensic tools cannot access certain application data, especially from encrypted or secure applications (e.g. WhatsApp, Signal, ProtonMail)[16][17].

3. Flash memory volatility Mobile devices typically use NAND flash memory, which has high write cycles and data volatility. Deleted data can be quickly overwritten, especially in applications that frequently cache content. This makes recovery of deleted artefacts difficult and requires timely collection.

4. OS fragmentation and update cycles The sheer variety of mobile operating systems and their frequent updates introduce new file systems (e.g., F2FS, APFS, YAFFS2) and access control policies. This constant evolution means that forensic tools must be continually updated to maintain compatibility and reliability in data extraction.
5. The number of smartphones now comes standard with advanced locking capabilities that include biometric identification and secure encryption compartments as well as dual-factor authorization systems. authentication, secure enclaves, and two-factor verification. Accessing data without credentials often
Advanced workarounds including the exploitation of firmware vulnerabilities must be used because they are necessary for successful attacks on these devices. Executors need to perform the workarounds with extraordinary caution in order to protect evidence from alteration and prevent device malfunction[14][19].

3. Cellebrite UFED

UFED creates a forensic platform through Cellebrite that serves the complex data investigation needs of modern mobile use cases. A forensic platform that builds its design capabilities based on meeting current mobile investigative needs exists[9]. It combines The platform contains a strong software intelligence system that works through dedicated hardware interfaces to process data extraction and decoding and analysis. Cellebrite UFED extracts and analyzes data from different mobile devices which includes smartphones, tablets, GPS units together with SIM cards. SSC Cellebrite UFED operates with wide device compatibility because its product supports profiles for more than thirty thousand devices.
Law enforcement personnel can obtain important digital evidence by using UFED despite strong security measures. UFED by Cellebrite enables the extraction of digital data from mobile devices despite encryption barriers as well as pass codes and app-level obfuscation protection systems[17]. Whether dealing with locked devices Through UFED police investigators together with forensic experts receive the tools which help analyze encrypted messaging apps along with other digital platforms.
An investigator requires tools to acquire data that meet forensic and legal requirements.

3.1 Key Features

1. Multi-Mode Data Extraction Cellebrite UFED supports three primary types of data acquisition - logical, The method of data extraction includes logical along with file system then physical formats to support different situations based on device state operating system and legal requirements. scope of the investigation[17].
2. This platform possesses capabilities to bypass PIN patterns and passwords along with other screen lock types in order to obtain access. The platform acquires encrypted data in numerous situations especially when working with older devices that have potentially vulnerable operating systems. It also includes
3. The system includes features to pass through boot loader and secure enclave barriers according to legal authorization[17].
4. UFED performs data decryption and infrastructure for decoding encrypted messages from major platforms including WhatsApp, Telegram, Signal, Snapchat and their equivalents.
5. The platform UFED can decode various encrypted messaging applications including WhatsApp, Telegram, Signal, Snapchat and additional services..

3.2 Extraction techniques

1. Logical Extraction Logical extraction uses standard operating system access protocols[11] (e.g. ADB for Android or iTunes interface for iOS) to retrieve user-visible data such as

- Text messages (SMS) - Call logs and contacts
- Photos and videos - Notes and browser history This method is non-invasive and is often used when full access is not possible due to encryption or user permission restrictions.

2. File System Extraction File system extraction provides a more comprehensive view of the device's data structure. It accesses both user and system directories, allowing investigators to retrieve

- Application data directories - System configuration files - Hidden or protected folders - File timestamps and metadata This technique is critical for understanding application behaviour, tracing data artefacts and identifying anomalies in user activity.

3. Physical extraction creates a bit-by-bit image of the device's memory, including both allocated and unallocated space. This method is particularly useful for

- Recovering deleted files or fragments
- Identifying residual data in slack space
- Analysing corrupted or semi-functional devices Although more intrusive, physical extraction provides the deepest level of forensic insight and is often the method of choice in criminal investigations requiring thorough digital evidence recovery.

4. Cellebrite UFED Mobile Forensic Methodology

The Cellebrite UFED mobile forensic data collection process follows a structured, legally compliant process to ensure both data integrity and admissibility as evidence[15][2][14]. Each step of the workflow is designed to maintain the chain of custody, prevent data tampering, and produce comprehensive, reproducible results that will stand up to legal scrutiny. Below is a breakdown of the standardised five-step forensic methodology[19][18]:

Step 1: Seizure and Preservation

Objective: Prevent data alteration or loss during evidence collection.

Action: Once a device is identified as potential evidence, it is immediately secured using anti-tamper protocols.

Faraday bags or airplane mode are used to isolate the device from wireless communications (e.g. remote wipe, cloud sync).

The device's state (on/off), screen lock status, battery level and environment are carefully documented.

Photographic evidence and written logs establish the initial chain of custody for the device.

Step 2: Identification and Preparation

Objective: Confirm device compatibility and forensic readiness.

Action: Document critical device information: brand, model number, serial/IMEI, operating system version, and any visible damage or modifications.

Validate that the UFED system is updated with the latest firmware, drivers, and extraction protocols, ensuring support for the target device.

Prepare necessary connectors and power sources to facilitate a stable forensic extraction.

Step 3: Data Extraction

Objective: Acquire data from the mobile device using appropriate extraction techniques.

Action:

Connect the device securely via USB, Bluetooth, or proprietary interfaces depending on hardware support and forensic conditions.

Select the appropriate extraction mode (logical, file system, or physical) based on:

Access permissions
Device security settings
Legal authorization (e.g., search warrant, user consent)
Utilize UFED's advanced features for:
Lock bypassing (PINs, patterns, biometric locks)
Decryption of protected data
Handling bricked or semi-functional devices

Step 4: Data Analysis

Aim: Examine and interpret the extracted data for relevance to the investigation.
Action:
Import the extraction package into Cellebrite Physical Analyzer, which allows for deep content analysis, artifact reconstruction, and data correlation.
Categorise and review key data sets, including
Messages (SMS, MMS, encrypted chats)
Call logs, contacts, media files, browser history
Location data via GPS, Wi-Fi logs, and cell tower triangulation
App data from platforms such as WhatsApp, Instagram, or Snapchat
Identify and flag anomalies such as
Deleted or hidden messages
Suspicious app usage
Timeline inconsistencies or falsified metadata

Step 5: Reporting

Objective: Present findings in a clear, legal and auditable format.
Action:
Generate forensic reports in multiple formats including UFDR, XML, PDF and HTML.
Reports typically include
Metadata and hash values for file verification
Timestamps and timeline reconstructions
Geolocation overlays and communication maps
Screenshots or reconstructed conversations from messaging applications
Secure all evidence with proper encryption, access control, and audit trails to maintain evidence integrity for court presentation.

5. Case Study

Cyberstalking Investigation Using Cellebrite UFED Scenario[15][5]
Overview:
A cyberstalking complaint was filed by a female victim who reported receiving a series of threatening messages and suspected that her real-time location was being tracked without her consent[8][10]. The suspect, a known acquaintance, was placed under investigation. Authorities seized the suspect's mobile device - a Samsung Galaxy S10 running Android 11 - as part of the evidence collection process.
Forensic strategy and tools:
- Device: Samsung Galaxy S10 (Android 11)

- Tool Used: Cellebrite UFED with physical analyser - Extraction method: Physical Extraction This technique was chosen due to the likelihood of deleted or hidden data and the need to access encrypted partitions and unallocated memory areas.
- Time required for extraction: Approximately 40 minutes This included device recognition, full memory capture and creation of the extraction image.

Key forensic findings:

1. Recovered deleted messages:

Using physical extraction, investigators recovered WhatsApp messages that had been deleted from the device.

Several messages contained direct threats, derogatory remarks, and repeated inquiries about the victim's whereabouts, establishing a pattern of harassment.

2. Geolocation and GPS Tracking Data:

The UFED physical analyser identified GPS log entries and location history indicating that the suspect had repeatedly visited areas near the victim's home and workplace.

These time stamps coincided with incidents where the victim had reported feeling followed.

3. Browser activity analysis:

Although conducted in incognito mode, the physical extraction method revealed browser cache and remnants of visited pages.

The browsing history included searches related to covert tracking applications, SIM cloning and anonymised communication tools, suggesting deliberate surveillance efforts 4. 4.

4. Outcome and Legal Implications:

The evidence recovered by Cellebrite UFED proved critical to the investigation:

Legal outcome: The recovered data served as the primary digital evidence to obtain a search warrant for the suspect's home and personal cloud storage accounts.

The combination of threatening messages, location logs and online activity established both intent and means, ultimately contributing to a successful prosecution for cyberstalking and digital harassment.

5. Forensic Relevance:

This case highlights the practical strength of Cellebrite UFED in recovering deleted, concealed and encrypted data, even from modern smartphones with advanced security features. The ability to recover information beyond user-accessible areas, including metadata and application remnants, underscores the importance of UFED in time-sensitive, high-impact digital investigations.

6. Advantages of Using Cellebrite UFED

Cellebrite UFED serves as the fundamental tool in mobile forensics practices through its reliable technology[6][17]. technological sophistication and forensic rigour. It delivers technical advantages as well as legal advantages which span two areas. This tool stands as the preferred choice for global investigations mainly because of its strong defensibility features. Several essential advantages exist in making use of Cellebrite UFED.

UFED in digital investigations:

1. UFED from Cellebrite supports a wide range of device profiles amounting to 30,000 entries that embrace legacy and contemporary devices from Android and iOS platforms. The tool supports investigations of both current Android and iOS smartphones. A wide range of support systems allows forensic analysts to access devices for examination[8]. The UFED device supports different kinds of

devices including feature phones and latest flagship smartphones. The tool enables investigations without requiring investigators to maintain different specialized devices[10]. Software updates which happen routinely guarantee that the system operates properly with new versions released. released devices and operating system versions.

2. Digital investigations heavily depend on swift action because digital evidence can automatically be destroyed remotely. or altered. UFED allows investigators to acquire data at high speed through its data acquisition feature for logical and file system and physical extractions. even physical extractions in a matter of minutes.[16][4] Live investigations depend on obtaining data quickly for their success. Investigations ,search and seizure operations, or emergency response scenarios where actionable intelligence is needed immediately.
3. The outstanding feature of UFED enables the user to bypass security protocols on protected devices through disabling and circumventing measures. or encrypted devices. Tool users can easily bypass different security authentication options on multiple Android as well as iOS devices by circumventing their PINs and patterns and passwords[3]. The system provides capabilities to defeat PINs patterns as well as passwords for Android and iOS models and has options to circumvent encryption protocols. These capabilities are particularly important Code-breaking capabilities on encrypted devices help professionals investigate unwillful suspects as well as unidentified secure operational situations[4].
4. Cellebrite UFED enables smooth connection between its feature set and widely used forensic tools. digital forensics ecosystems such as Magnet AXIOM, Relativity, Nuix and other analysis platforms. This The interoperable system framework enables investigators to integrate mobile evidence with other analysis tools through their platform channel[4]. The analysis benefits from integrating digital evidence across computers, network platforms and cloud platforms in order to create complete forensic descriptions. Integration The platform enables automated workflow processing together with team-based collaborative activities between forensic units.
4. The software generates standard and forensically sound reports through UFDR PDF and XML output formats which are recognized in most legal proceedings. accepted in legal proceedings. Every report delivered by Cellebrite UFED contains metadata together with timestamps and hash values and chain-of-custody logs[5]. The software creates custody logs containing evidence proof verification and authenticity measures. This attention to evidentiary Cellebrite UFED maintains standards that enable trustworthiness for court appearances and legal defense evaluation. from legal defence teams.

7. Limitations and Ethical Considerations

The powerful capabilities of Cellebrite UFED come with various operational obstacles in mobile forensics applications. Both technical constraints and ethical dimensions must be understood completely for using Cellebrite UFED in a legal and responsible manner[12][13]. The uncontrolled limitations affect the evidence reliability and the investigation's credibility. the credibility of the investigation.

7.1 Technical Limitations

Despite its advanced technical abilities the Cellebrite UFED deals with various operational restrictions together with adaptability problems because mobile device technology continues to advance.

Limited effectiveness with advanced encryption techniques:

Device manufacturers regularly enhance device security which makes forensic tools fall behind in their capacity to extract protected information. The encryption measures integrated in Apple devices through Secure Enclave and Android full-disk encryption make it extremely difficult for forensic extraction activities. The analysis of evidence becomes impossible when such cases occur.

High cost of ownership:

UFED exists as a commercial tool that demands heavy initial capital outlay while costing schools significant expenses for software maintenance as well as continuous training and support. The high cost of the tool prevents many smaller law enforcement agencies and developing-region organizations from accessing its functionalities.

Lack of open source transparency:

Cellebrite UFED functions through closed-source code that hinders independent control checks together with community verification and peer review procedures. Forensic science principles of result reproducibility and verification become difficult to achieve because of these concerns.

7.2 Ethical and legal concerns

The widespread application of UFED technology needs precise enforcement of legal protocols and ethical boundaries to both defend constitutional rights and make evidence admission possible.

Invasion of privacy risks:

UFED enables users to obtain profound examination of individual digital lives that reveals entire content including confidential communications and picture files in addition to health records alongside app activity. Inappropriate supervision of data access enables privacy breaches that violate both protections for personal data and human rights stipulations.

Consent and legal authorisation:

Public device inquiries need to follow complete compliance with valid legal permission like attorney-approved warrants in combination with subpoenas and user-provided consent. Police must abide by local digital search laws during investigations because deviations from proper processes result in potential court disputes which may eliminate evidence as well as wasted court resources.

Chain of custody and data integrity:

The evidentiary value of extracted data becomes compromised through any kind of improper handling or unauthorized changes to the information. A clear auditable trail concerning custody operations should exist for investigators along with certified methods during their analysis to validate evidence authenticity throughout the judicial process.

8. Future Scope and Recommendations

As mobile technology continues to evolve in complexity and capability, the field of mobile forensics must adapt accordingly. While Cellebrite UFED has established itself as a leader in device-level data extraction, future developments should aim to extend its reach, improve transparency, and leverage emerging technologies to more effectively address investigative challenges.

8.1 Broader support for encrypted and niche applications

With the increasing adoption of secure messaging platforms such as Signal, Threema and other decentralised or privacy-focused applications, forensic tools need to evolve to include robust support for extracting and parsing encrypted application data. Many of these platforms use end-to-end encryption and obfuscation techniques that limit the scope of current tools. Extending UFED's compatibility with these applications will be critical to maintaining investigative relevance.

8.2 Integration with cloud and IoT ecosystems

Mobile devices are now intricately connected to cloud services and Internet of Things (IoT) devices, creating hybrid digital footprints. The next generation of forensic tools must be able to correlate cloud-based artefacts (such as synchronised application data, cloud backups and authentication logs) with local

device data. In addition, integrating forensic capabilities for IoT devices - such as wearables, smart home hubs and automotive systems - can provide a more holistic investigative framework.

8.3 Incorporate forensic AI and automation

The sheer volume of data extracted from modern devices presents a significant challenge to manual review. Integrating artificial intelligence (AI) and machine learning modules into the UFED ecosystem could revolutionise analysis by enabling automated pattern recognition, behavioural profiling, timeline generation and anomaly detection. This would dramatically reduce investigator workload and improve the speed and accuracy of results in high-value investigations.

8.4 Standardising

UFDR reports for interoperability The Universal Forensic Data Report (UFDR) is a key output format used by Cellebrite. However, interoperability challenges arise when attempting to share UFDR data across different forensic platforms or jurisdictions. Moving to a more open, standardised and transparent reporting schema would facilitate collaborative investigations, improve cross-tool compatibility and foster greater confidence in the presentation of digital evidence during litigation.

9. Conclusion

While working in mobile forensic investigations the Cellebrite UFED stands as a vital tool which delivers unmatched capability to extract and analyze digital evidence from mobile devices and smartphones. The world-wide legal acceptance of Cellebrite UFED results from its ability to defeat security features while delivering inaccessible data recovery and its presentation power of investigator findings. Smartphones serve as crucial evidence sources due to their extensive use for all aspects of communication and business transactions and social networking activities. Cellebrite UFED serves investigators by offering necessary tools to discover truth in cyberstalking events and fraud operations and corporate espionage investigations and terrorism-based cases. Herbalife Limited started as a health supplement company in 1980. Improper or unjustified extractions which damage privacy rights might cause evidence to become inadmissible during legal proceedings. Forensic tools including UFED must adapt to the swift technological developments in mobile devices which exist in the future. Future effectiveness of Cellebrite UFED depends on three key elements: enhancement of encrypted platform support while integrating cloud and IoT systems and implementing artificial intelligence for automated analysis to stay relevant in the digital environment.

References

1. Casey, E. (2019). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.
2. Quick, D., & Choo, K.-K. R. (2018). Mobile device forensics: Current state of research. IEEE Access, 6, 58006–58019. https://doi.org/10.1109/ACCESS.2018.2871085
3. Zdziarski, J. (2018). Practical mobile forensics. Syngress.
4. Khan, A., Baig, Z. A., & Salah, K. (2020). Digital forensics for the next Internet revolution: Current trends, research challenges, and future directions. Computer & Security, 97, 101901. https://doi.org/10.1016/j.cose.2020.101901
5. Cellebrite. (2021). UFED Series – Product overview and technical specifications. Retrieved from https://www.cellebrite.com/en/ufed/

6. Cellebrite. (2022). UFED Physical Analyzer user guide. Retrieved from https://www.cellebrite.com/en/resources/
7. Al Mutawa, N., Baggili, I., & Marrington, A. (2016). Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9, S24–S33. https://doi.org/10.1016/j.diin.2012.05.009
8. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1
9. Mahalik, H., & Ranjan, P. (2022). A comprehensive review of digital forensic tools for smartphones. International Journal of Digital Crime and Forensics (IJDCF), 14(1), 1–17. https://doi.org/10.4018/IJDCF.2022010101
10. Azfar, A., Choo, K.-K. R., & Liu, L. (2017). Forensic taxonomy of Android social apps. Journal of Digital Forensics, Security and Law, 12(4), 7–22. https://doi.org/10.15394/jdfsl.2017.1478
11. Raghavan, S. (2013). Digital forensic research: Current state of the art. CSI Transactions on ICT, 1(1), 91–114. https://doi.org/10.1007/s40012-013-0008-7
12. Karpisek, F., Baggili, I., & Breitinger, F. (2015). WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages. Digital Investigation, 15, 110–118. https://doi.org/10.1016/j.diin.2015.09.002
13. van Baar, R. B., van Beek, H. F., & van Eijk, E. J. (2014). Digital forensics and cyber crime: First International ICST Conference. Springer.
14. Lessard, J., & Kessler, G. C. (2010). Android forensics: Simplifying cell phone examinations. Small Scale Digital Device Forensics Journal, 4(1), 1–12.
15. Husain, M. I., Sridhar, R., & Olsen, R. S. (2011). Android forensics: Automated data collection and reporting from a mobile device. Digital Investigation, 8(S3), S118–S125. https://doi.org/10.1016/j.diin.2011.05.007
16. Anglano, C., Canonico, M., & Guazzone, M. (2017). Forensic analysis of Telegram Messenger on Android smartphones. Digital Investigation, 23, 31–49. https://doi.org/10.1016/j.diin.2017.09.002
17. Tso, F. P., & Zhu, Y. (2021). Secure enclaves and mobile forensics: An emerging area of challenge. IEEE Security & Privacy, 19(3), 38–45. https://doi.org/10.1109/MSEC.2021.3056425
18. Maras, M. H. (2014). Computer forensics: Cybercriminals, laws, and evidence (2nd ed.). Jones & Bartlett Learning.
19. International Association of Computer Investigative Specialists (IACIS). (2021). Mobile Device Forensics Training Manual. IACIS.org