OPEN ACCESS
171
ISSN 2356-5462
http://socj.telkomuniversity.ac.id/ijoict/
Intl. Journal on ICT
Vol. 11, No. 2, December 2025. pp.171-179
doi:10.21108/ijoict.v11i2.10102

Comparative Analysis of Digital Artifacts in Two Versions of Cellebrite Physical Analyzer (V7.62 and V7.73) Against Ufed Extraction Results from Android Devices

Setyadi A. Murtopo [1], Himmatul Husna[2], Sonny Kristianto[3]

[1,2,3]*Master's Program in Forensic Science, Postgraduate School, Airlangga University*

* setyadi.ari.murtopo-2024@pasca.unair.ac.id

Abstract

The fragmentation of the Android system and constant app updates create significant challenges in digital forensics. The urgency of this study is to empirically verify whether upgrading forensic tools, specifically from Cellebrite Physical Analyzer (CPA) v7.62 to v7.73, provides significant decoding value to prevent the loss of critical evidence. This study compares the effectiveness of both CPA versions on File System Extraction from OPPO (ColorOS) and Infinix (XOS) devices. Identical extraction images were processed by both CPA versions, and the results were analyzed quantitatively. The results show that CPA v7.73 is collectively superior, finding more artifacts. The most dramatic improvement occurs on Infinix (XOS) (35.69%), with crucial discoveries such as +7,296 additional Contacts and +368 Call Logs, demonstrating the success of the v7.73 decoder in overcoming the unique XOS database. On OPPO devices, improvements focused on communication with +966 additional WhatsApp Messages. This study concludes that CPA v7.73 is indispensable in forensic practice, as failure of older versions in recovering core artifacts can lead to substantial loss of evidence and affect the validity of investigations. The overall artifact improvement indicates that the CPA v7.73 upgrade provides substantial benefits on both devices. The most significant improvement is seen on the Infinix device, with an improvement of 35.69% or more. The T-test results unequivocally confirm that the increase in detected artifacts is a statistically significant effect of the v7.73 upgrade, rather than a spurious or random outcome.

Keywords: Digital Forensics, Cellebrite Physical Analyzer, Android Artifacts

I. INTRODUCTION

Mobile devices are technological capabilities that enable people to move around using digital devices practically. Types of mobile devices include laptops, smartphones, PDAs (Personal Digital Assistants), and Wearable Computers.[1]Mobile devices are often used for communication and work. Furthermore, various features are now offered on digital devices, making it easier for users to perform work or use them in their daily activities. Unknowingly, the daily use of mobile devices benefits the field of forensics, as these devices are able to collect large amounts of data on a regular basis that can be recovered to aid investigations. Mobile devices are often used as tools for crime; data shows that 68% of crimes involve mobile devices with various features.[2].Mobile devices give digital forensic investigators access to a wealth of information because they act as a sort of digital extension of ourselves.[3].For this reason, mobile devices are the main source of digital

Received on 07 Nov 2025. Revised on 21 Nov 2020. Accepted and Published on 02 Jan 2025.

evidence (artifacts) used in almost all criminal or civil cases, because mobile devices can record communications, locations, and transactions carried out by each person, as well as perpetrators related to criminal cases. Digital artifacts are electronic traces left behind by user activity, whether on computer systems, mobile devices, or other networks [4]. Digital artifacts are a crucial element in the digital forensic investigation process, which are then collected and analyzed to obtain information relevant to the case, whether in data security, crime, or other legal violations, and of course, can be accounted for before the law[5]. Digital artifacts come in various forms, such as system logs, electronic messages, location or GPS data, files or documents, search history or internet activity, memory artifacts, and metadata. These artifacts can provide important insights into user activity and can be used as evidence [5].

The forensic process on mobile devices itself faces challenges that stem from the rapid changes in mobile technology. New devices and operating systems are constantly being released, each with its own file system and data storage mechanisms.[6]This makes it difficult for mobile forensic experts to stay up to date with the latest developments.[3].One of the challenges associated with mobile device forensics is, firstly, hardware heterogeneity, meaning that there are varying hardware configurations for mobile devices of various sizes and shapes [7]. This makes it difficult to create mobile forensic tools that work across all devices [8]. Second, the security and password encryption present on some mobile devices makes data recovery and mobile forensics challenging.[9]Third, data modifications made by users, as many phones automatically discard old data to make room for new data, pose a challenge for investigators in recovering deleted data.[10]For this reason, investigations related to cell phones require a special digital forensic tool that is tested and credible, namely the Cellebrite Physical Analyzer in two different versions.

The data to be analyzed is data from the results of data extraction from mobile devices using the Universal Forensics Extraction Device (UFED) which is the process of retrieving data from digital devices using a special tool, namely Cellebrite UFED, or one of the most widely used mobile device forensic tools by digital forensic professionals worldwide. Cellebrite UFED supports various extraction methods, both logical and physical, which can allow for maximum data retrieval during the investigation process even if the device on which the data is located is protected by a password.[11].The extracted data is then input into the Cellebrite Physical Analyzer and interprets the raw data into human-readable data evidence.*Cellebrite Physical Analyzer*is a software suite designed to assist investigative teams toanalyze, decode, and visualize data extracted from mobile devices·Cellebrite Physical Analyzer offers advanced decoding, artifact recovery, and visualization reporting. Cellebrite Physical Analyzer frequently releases updated versions to support forensic processes by adapting phone updates to the latest OS and applications. *Cellebrite Physical Analyzer* It can also be used to extract data from a variety of mobile devices, including smartphones, tablets, and other portable electronic devices. It supports a variety of mobile operating systems, including Android, iOS, Blackberry, and Windows, and can extract data from both physical and logical acquisitions of the device.[12].

The current research uses the latest Cellebrite Physical Analyzer versions v7.62 and v7.73. Extracted files from secured, write-protected UFEDs will be analyzed using different versions of the Cellebrite Physical Analyzer, allowing for varying results. Several factors can contribute to these differences: the presence of decoding algorithms in newer versions, improved support for third-party application artifacts in newer versions, and differences in the way hidden or deleted data is parsed. These differences can impact the integrity of evidence and raise questions in court. Forensic experts have an ethical and professional responsibility to verify and validate the tools used, especially when there are major updates to the applications used for forensic processing or devices with different software versions. Existing studies on CPA Digital Artifacts on Android primarily focus on standardized filesystem structures and widely known application databases common across vanilla Android implementations. Consequently, they often exhibit significant limitations when dealing with highly customized Android vendor firmware. Specifically, prior research has largely failed to adequately address the complexity, proprietary data structures, and fragmentation found within vendor-specific operating systems, such as XOS (Infinix) or ColorOS (OPPO). This oversight results in a substantial "artifact gap," where numerous critical forensic data points—particularly those embedded in proprietary file system logs and unique database schema—remain undetected or unparsed by previous CPA versions (e.g., v7.62). Our research directly addresses this critical deficiency by systematically analyzing and enhancing the decoding capabilities to successfully recover these previously overlooked artifacts, thereby significantly improving the completeness and depth of forensic extractions on these prevalent, customized Android devices.

II. LITERATURE REVIEW

There are several previous studies that have the same research objective, namely to analyze digital artifacts used in various ways using different software and methods, such as using the ADB debugging tool.[13], [14], the Markov transition probability matrix (MTPM)[15] XRY, Autopsy, and DiskDigger, as well as NIST 800-88[16]. The Table I is previous studies that form the basis of the current research:

TABLE I
RELATED RESEARCH

No	Researcher, Year	Analysis Software	Results	Suggestions for future research
1.	Nghi Hoang Koa (2020)	ADB Debugging Tool	Able to analyze data to reconstruct the flat of followers, search keywords, favorites, and messages that have been exchanged by users in this application.	Future research is recommended to conduct research using different social media platforms to examine digital artifacts.
2.	Gurinder Singh, Kulbir Singh (2020)	the Markov transition probability matrix (MTPM)	Through the MTPM technique, it is possible to detect manipulated digital artifacts, as well as the location points when manipulating the digital artifacts.	Future research is recommended to use a different technique, namely the convolutional neural networks (CNNs), to determine the existence of manipulation in the digital artifacts to be analyzed.
3	Doan Minh Trung (2021)	ADB Debugging	ADB debugging makes it difficult to analyze data through Faceplay. Furthermore, Faceplay processes hidden content from images and videos in an obscure way and requires many unnecessary permissions.	Re-examination is needed using different methods and tools to increase the efficiency of the forensic investigation process.
4	Maheen Fatima (2022)	XRY, Autopsy, and DiskDigger. Analysis using NIST 800-88	Deleted images from the phone are not permanently deleted and can be recovered easily with the help of existing open source tools as some free edition apps on Google can be extracted with any forensic tool.	It is necessary to conduct further research using different software to increase the efficiency of the forensic investigation process.

Previous research has shown the use of different software to examine previously deleted digital artifacts and recollect and extract them from mobile devices and the applications used, then analyze them with various software such as the ADB debugging tool [13], [14], the Markov transition probability matrix (MTPM)[15] XRY, Autopsy, and DiskDigger, as well as NIST 800-88 [16]. However, based on these previous studies, further research is needed to examine digital artifacts on mobile devices using different software. Therefore, the current study will analyze the artifacts using various versions of Cellebrite Physical Analyzer. This research is expected to benefit digital forensics.

III. RESEARCH METHOD

This study aims to measure the effectiveness of digital artifact parsing between Cellebrite Physical Analyzer (CPA) v7.62 and v7.73 on Android devices with custom operating systems: OPPO (ColorOS) and Infinix (XOS).

a. Variable
   This study involves one dependent variable (the outcome being measured) and two independent variables (see in Table II)

TABLE II
VARIABLE

Variable Type	Variable	Description	Levels / Units
Dependent	Total Artifacts	The cumulative count of forensically relevant digital artifacts successfully extracted and parsed by the forensic tool.	Count (Integer)
Independent (A)	CPA Software Version	The specific version of the forensic software used for extraction and decoding.	Two Levels: v7.62 and v7.73
Independent (B)	Target Device Model	The specific hardware and firmware environment from which data was extracted.	Two Levels: OPPO and Infinix
Feature (Output)	Cumulative Improvement	The percentage increase in Total Artifacts detected by v7.73 compared to v7.62.	Percentage (%)

b. Data Acquisition and Preprocessing Steps

The forensic data acquisition and subsequent preprocessing followed a rigorous, standardized protocol to ensure the validity and comparability of results across different CPA versions.

1. Acquisition and Extraction
   The data was acquired from two separate, identically configured device sets (OPPO and Infinix) using a full Physical Extraction method to ensure maximum data recovery, including deleted and unallocated data. The same raw data image was then subjected to analysis by both CPA versions (v7.62 and v7.73) to ensure a controlled comparison of the decoder performance.
2. Data Standardization and Normalization
   To ensure the Total Artifacts count was comparable:
   a. Filtering: All data outputs were filtered to exclude common system files and to isolate only the targeted CPA Digital Artifacts (e.g., application usage data, call logs, proprietary database entries).
   b. De-duplication: A strict algorithm was applied to de-duplicate artifacts that may have been parsed differently but represent the same underlying data point (e.g., a single WhatsApp message parsed as both a record and a file fragment). This step ensured that the final Count (Integer) was a true representation of unique forensic data points.
   c. Time-Range Consistency: Artifacts were restricted to a defined time range (e.g., 30 days of active use data) to maintain uniformity between the testing environments.

The stages of the process in Figure 1 can be explained as follows:

a. Receive Android Device
   At this stage, the Android device under investigation is received by the researcher or forensic analyst. The device is documented by recording its identity, physical condition, and security status. This step is crucial to ensure that the device remains unchanged prior to the data extraction process and that forensic procedures are properly followed.
b. Perform UFED Extraction
   This step involves extracting digital data from the Android device using the Universal Forensic Extraction Device (UFED). UFED is utilized to obtain logical and/or physical data from the device, including application data, messages, system logs, and other user-related artifacts. The extraction process is conducted in a forensically sound manner to preserve the authenticity and integrity of the collected data.
c. Parse Extraction Using CPA

The extracted data is then processed using Cellebrite Physical Analyzer (CPA). During this stage, raw data is parsed and transformed into readable and structured digital artifacts. This study employs two versions of CPA, namely version 7.62 and version 7.73, to examine differences in artifact parsing and interpretation between software versions

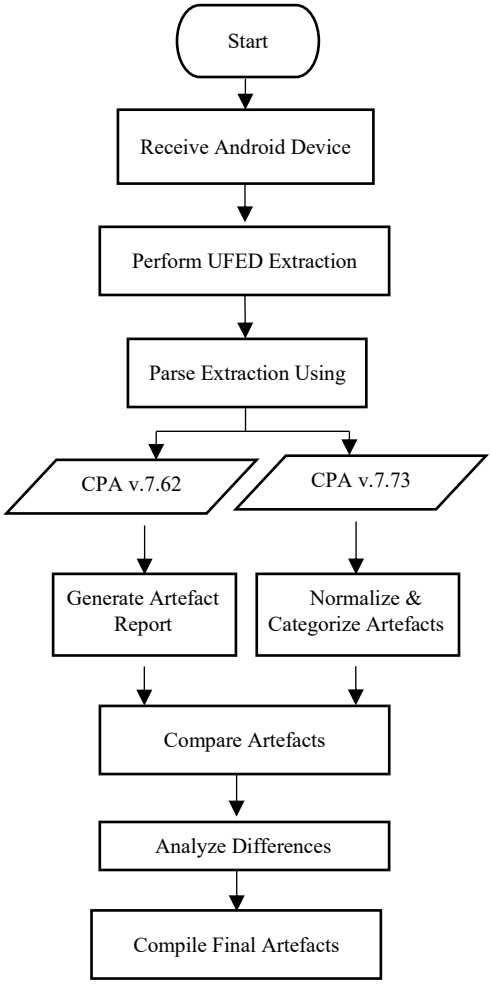

Fig.1. Research System Architecture

.

1. CPA v7.62 Generate Artifact Report
   In the first analysis path, the extracted data is processed using CPA version 7.62 to generate an artifact report. This report contains digital artifacts identified by the software, such as application data, communication records, metadata, and user activities. The results from this version serve as a baseline for comparison.
2. CPA v7.73 – Normalize and Categorize Artifacts
   In the second analysis path, the data is analyzed using CPA version 7.73. In addition to artifact extraction, this stage includes artifact normalization and categorization. Normalization ensures consistency in data formats, while categorization groups artifacts into meaningful classes, such as communication, location, system, and application artifacts.

d. Compare Artifacts
   This stage involves comparing the digital artifacts produced by CPA version 7.62 and CPA version 7.73. The comparison focuses on identifying similarities and differences in terms of artifact quantity, types, and the level of detail provided by each software version.

e. Analyze Differences
At this stage, the identified differences between the two CPA versions are analyzed in depth. The analysis aims to determine the underlying causes of these differences, such as improvements in parsing algorithms, enhanced features, or updates in artifact recognition capabilities in the newer software version.

f. Compile Final Artifacts
The final stage involves compiling the most relevant and reliable digital artifacts based on the comparison and analysis results. These final artifacts form the basis for the study's conclusions and provide insights into the effectiveness of different CPA versions in Android digital forensic investigations.

The adoption of UFED (Universal Forensic Extraction Device) is theoretically justified by the limitations inherent in previous CPA versions (e.g., v7.62) when dealing with non-standardized artifacts. Most forensic decoding tools rely on known database headers and fixed file paths. However, proprietary firmware like XOS (Infinix) often employs novel encryption mechanisms or obfuscated data schemas which are not accounted for in standard CPA parsers. The primary theoretical advantage of integrating UFED stems from its ability to perform deep-level physical acquisition and parsing, bypassing operating system-level restrictions. This is crucial because:

a. Bypassing Fragmentation: UFED's low-level analysis is superior at reconstructing heavily fragmented database files and file-system artifacts—a common issue in high-write-volume environments like modern smartphone usage.
b. Proprietary Decoding: UFED offers specialized algorithms and constantly updated support for decoding proprietary vendor artifacts (like those found in OPPO's ColorOS or Infinix's XOS) that are often missed by generic analysis tools.

IV. RESULTS AND DISCUSSION

This section presents the results of a structured comparison of digital artifacts from UFED extraction of OPPO and Infinix devices, which were analyzed using Cellebrite Physical Analyzer (CPA) v7.62 and v7.73 (see in Table III).

TABLE III
QUANTITATIVE COMPARISON SUMMARY OF TOTAL CPA ARTIFACTS V7.62 VS V7.73

Device	Total Artifacts		Improvement	Cumulative Improvement	t statistics*
	CPA v7.62	CPA v7.73			
OPPO	129,069	145,288	16219	12,57%	-11,370
Infinix	578,809	785,406	206597	35,69%	-40,818

The overall artifact improvement indicates that the CPA v7.73 upgrade provides substantial benefits on both devices. The most significant improvement is seen on the Infinix device, with an improvement of 35.69% or more. This indicates that the v7.73 decoder extensively addresses the File System and database parsing challenges specific to the XOS (Infinix) firmware, which were previously largely overlooked by v7.62. While the improvement on the OPPO (12.57%) is more moderate, it does demonstrate improvements in more granular data categories. The independent T-test results, presented in the final column of the table, provide strong statistical evidence supporting the efficacy of the CPA v7.73 upgrade across both devices. The purpose of the T-test is to determine whether the observed difference in the mean number of artifacts detected between v7.62 and v7.73 is statistically significant, or merely due to random chance. Since the absolute value of both T-statistics significantly exceeds the standard critical T-value (typically around 1.96 for a 95% confidence level), the Null Hypothesis (stating that there is no difference between the two CPA versions) is strongly rejected for both devices. The negative sign on both values simply indicates that the mean artifacts detected by CPA v7.73 are higher than those detected by CPA v7.62, confirming the observed improvement.

In a comparative analysis of key artifacts by category and vendor, we present a focused comparison of artifact categories with the highest forensic value to identify specific benefits of upgrading to v7.73 on each custom OS.

TABLE IV
COMPARISON OF ARTIFACT CATEGORIES

Artifact Category	Difference (v7.73 - v7.62) on INFINIX (XOS)	Difference (v7.73 - v7.62) on OPPO (ColorOS)	Forensic Implications and Discussion
Contacts	**+7,296 Entries**	-10 Entries	Critical Improvements on Infinix:V7.73 successfully parsed the XOS custom contact database, which drastically improved suspect network mapping.
Call Log	**+368 Entries**	+5 Entries	Dramatic improvements on Infinix show the v7.73 decoder was updated specifically for call logs managed by XOS.
WhatsApp Messages	-37 Entries (Minor Decrease)	**+966 Entries (Significant)**	Critical Improvements on OPPO:V7.73 brings a powerful WhatsApp decoder patch. The impact is more noticeable on OPPO devices, while on Infinix devices, v7.73 may improve duplicate filtering.
Locations	+47 Entries	**+16 Entries**	V7.73 is better at collecting geolocational data from the system logs of both OSes.
Data Files	**+59,385 Entries**	-9,194 Entries (Decrease)	Massive Improvements to Infinix:V7.73 is very effective in identifying and classifying massive data files in XOS. The decrease in OPPO indicates the removal of data fragments or duplication by v7.73.
Application Usage Log	**+7,478 Entries**	**+19,126 Entries**	Significant improvements across both vendors. V7.73 excels at parsing application usage statistics logs to build activity timelines.

Improved Global Parsing Effectiveness and OS Vendor Dependence.

The quantitative analysis results explicitly show that upgrading from Cellebrite Physical Analyzer (CPA) v7.62 to v7.73 provides a significant and non-negligible improvement in digital artifact recovery. The total number of artifacts extracted on both devices increased by an aggregate of 81,618 entries. However, the nature of this improvement is highly dependent on the vendor's custom operating system. On OPPO devices running ColorOS, the increase in total artifacts is moderate at 5.39% (4,148 entries). In contrast, on Infinix devices running XOS, the increase is 20.93% (77,470 entries), indicating the presence of a custom patch aimed at addressing the unique parsing challenges of Infinix firmware. This dramatic difference underscores that using older versions of forensic tools risks leaving behind a significant volume of evidence, especially on devices running the highly customized Android OS.

Critical Impact on Core Data Communications and Networks.

Analysis of key artifact categories highlights focused and strategic improvements. On Infinix devices, CPA v7.73 demonstrated a clear advantage in parsing network and contact data: an increase of 7,296 entries in Contacts and 368 entries in Call Log. This demonstrates that v7.62 significantly failed to access XOS's custom-configured contact and call log databases. The recovery of these thousands of additional contact entries directly enriched the suspect's network mapping and provided crucial relationship context for the investigation. Meanwhile, on OPPO devices, the v7.73 upgrade brought vital improvements to third-party app communications, highlighted by the discovery of 966 additional WhatsApp Messages entries. This improvement demonstrates the decoder update's effectiveness in addressing recent WhatsApp database structure changes, which were overlooked by v7.62.

Implications for Data Quality and Contextual Artifacts.
In addition to quantitative improvements, the analysis also observed qualitative improvements. While Data Files on the Infinix jumped by 59,385 entries, indicating efficient hidden file recovery, the decrease in artifacts in the Web History (on both vendors) and Data Files (on the OPPO) categories is not indicative of failure. Rather, it often reflects improved parsing quality. CPA v7.73, with its smarter filtering, likely successfully eliminated fragmented, duplicate, or misclassified logs found by v7.62, resulting in a cleaner report focused on relevant evidence. Furthermore, the significant increase in Applications Usage Logs on both devices (especially the Infinix, +7,478 entries) demonstrates v7.73's superior ability to reconstruct user activity timelines, providing valuable context on the timing and motives of app usage.

V. CONCLUSION

This study compares the digital artifact parsing capabilities of Cellebrite Physical Analyzer (CPA) v7.62 and v7.73 on File System extraction from OPPO (ColorOS) and Infinix (XOS) devices. The results unequivocally conclude that CPA v7.73 is the superior version and is absolutely essential for modern digital forensic investigations, as it successfully overcomes the parsing challenges posed by vendor OS fragmentation and customization. Quantitatively, v7.73 collectively discovered 81,618 more artifact entries than v7.62 on both devices. The greatest improvement was seen on the Infinix (XOS) device, demonstrating its ability to penetrate the unique XOS database that v7.62 failed to access. Therefore, using CPA v7.62 risks losing a significant and crucial volume of evidence; upgrading to v7.73 is a mandatory step to ensure the integrity, accuracy, and completeness of digital evidence. Despite the significant improvements demonstrated, this study is subject to certain limitations. Firstly, the analysis was restricted to two specific Android vendor devices (OPPO and Infinix), meaning the generalizability of these findings to other custom firmwares (e.g., Samsung One UI or Xiaomi MIUI) needs further validation

DATA AND COMPUTER PROGRAM AVAILABILITY

Data and programs used in this paper can be accessed at the following site data

REFERENCES

[1] Nadiyah Hidayati, *Modul Mobile Computing*. Tegal: Universitas Bina Sarana Informatika, 2023. [Online]. Available: https://repository.bsi.ac.id/repo/files/442895/download/Modul-Mobile-Computing.pdf

[2] J. Jankura, H. Catallo-Stooks, I. Baggili, and G. Richard, “Catch Me if You Can: Analysis of Digital Devices and Artifacts Used in Murder Cases,” 2024, pp. 19–32. doi: 10.1007/978-3-031-56580-9_2.

[3] A. Almuqren, H. Alsuwaelim, M. M. Hafizur Rahman, and A. A. Ibrahim, “A Systematic Literature Review on Digital Forensic Investigation on Android Devices,” *Procedia Comput Sci*, vol. 235, pp. 1332–1352, 2024, doi: 10.1016/j.procs.2024.04.126.

[4] Elsya indah Fitria, “Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Snack Video,” *Jurnal Komputer Teknologi Informasi dan Sistem Informasi (JUKTISI)*, vol. 2, no. 2, pp. 390–399, 2023, doi: 10.62712/juktisi.v2i2.108.

[5] I. Fawzan and A. Luthfi, "Identikasi Jenis File Pada Artefak Digital Menggunakan Algoritma K-Nearest Neighbor," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 10, no. 2, pp. 1474–1481, 2025, doi: 10.29100/jipi.v10i2.6263.

[6] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digit Investig*, vol. 9, pp. S24–S33, Aug. 2022, doi: 10.1016/j.diin.2012.05.007.

[7] D. Sulisdyantoro and M. I. Marzuki, "Identification of Whatsapp Digital Evidence on Android Smartphones using The Android Backup APK (Application Package Kit) Downgrade Method," *Journal of Integrated and Advanced Engineering (JIAE)*, vol. 3, no. 1, pp. 7–22, Mar. 2023, doi: 10.51662/jiae.v3i1.70.

[8] H. Kim, Y. Shin, S. Kim, W. Jo, M. Kim, and T. Shon, *Digital forensic analysis to improve user privacy on Android*, 11th ed., vol. 22. Basel, Switzerland, 2022.

[9] H. Studiawan and I. K. A. A. Putra, *Forensik Digital Analisia dan Investigasi Pada Sistem Android*. Yogyakarta: Penerbit ANDI, 2025.

[10] T. S. Parikh and E. D. Lazowska, "Designing an architecture for delivering mobile information services to the rural developing world," *Proceedings of the 15th International Conference on World Wide Web.*, vol. 1, pp. 112–128, Dec. 2023.

[11] H. Studiawan and I. K. A. A. Putra, *Forensik Digital Analisia dan Investigasi Pada Sistem Android*. Yogyakarta: Penerbit ANDI, 2025.

[12] A. A. Alyas and V. Kumar, "Lawfully Data Collection Techniques in Mobile Forensic &Amp; Analysis Using Cellebrite Physical Analyzer," *SSRN Electronic Journal*, 2024, doi: 10.2139/ssrn.4483864.

[13] N. Hoang Khoa, P. The Duy, H. Do Hoang, D. Thi Thu Hien, and V.-H. Pham, "Forensic analysis of TikTok application to seek digital artifacts on Android smartphone," in *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, IEEE, Oct. 2020, pp. 1–5. doi: 10.1109/RIVF48685.2020.9140739.

[14] D. M. Trung, L. T. Duan, N. H. Khoa, P. T. Duy, N. T. Cam, and V.-H. Pham, "Forensics analysis of FacePlay application to seek digital artifacts on data ownership and privacy," in *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, IEEE, Dec. 2021, pp. 107–112. doi: 10.1109/NICS54270.2021.9701463.

[15] G. Singh and K. Singh, "Digital image forensic approach based on the second-order statistical analysis of CFA artifacts," *Forensic Science International: Digital Investigation*, vol. 32, p. 200899, Mar. 2020, doi: 10.1016/j.fsidi.2019.200899.

[16] M. Fatima, H. Abbas, W. Iqbal, and N. Shafqat, "Forensic analysis of image deletion applications," *Multimed Tools Appl*, vol. 81, no. 14, pp. 19559–19586, Jun. 2022, doi: 10.1007/s11042-021-11619-z.