INTEGRATION: Journal of Multidisciplinary Studies
ISSN 3123-6928 (online)
Vol. 1 Iss. 1 Pg. 145-154
https://ejournal.scmdigi.id/index.php/integration

Comparative analysis of mobile forensic tools for digital evidence recovery using NIST framework

Mutiara Rizqi Oktavirani, Triawan Adi Cahyanto*, Nur Qodariyah Fitriyah, Daryanto
Universitas Muhammadiyah Jember, Jawa Timur, Indonesia
*Correspondence author: triawanac@unmuhjember.ac.id
DOI: https://doi.org/10.65881/integration.v1i1.26

ARTICLE INFO

History:
Submit: 01-20-2026
Revision: 01-25-2026
Accepted: 01-26-2026
Published: 01-30-2026

Keywords:
digital forensic;
mobile forensic;
magnet axiom;
cellebrite physical analyzer;
nist.

ABSTRACT

Purpose: to compare the performance of Magnet Axiom and Cellebrite Physical Analyzer in extracting digital evidence from Google Pixel 5a.
Method: using a quantitative approach with a comparative experimental method. A dataset of Google Pixel 5a digital images was analyzed using two forensic software tools, Magnet Axiom and Cellebrite Physical Analyzer, in accordance with the NIST framework. The process includes preservation, acquisition, examination, analysis, and reporting. The performance of both tools was quantitatively evaluated by counting the number of artifacts recovered across various data categories and was calculated using the 16 NIST mobile forensic criteria.
Findings: the Cellebrite Physical Analyzer outperformed the Axiom Magnet in recovering digital artifacts from the Google Pixel 5a, particularly for internet, geolocation, and social app data, achieving a 75% success rate compared to 56%. The Axiom Magnet performed only slightly better at SMS recovery, but was less effective for complex app data.
Implications: choosing the right forensic tool affects the success of a digital investigation; Cellebrite is more effective for in-depth analysis of modern Android devices, while manual verification is still necessary to ensure the validity of the evidence.
Originality: directly compares the performance of Magnet Axiom and Cellebrite on Google Pixel 5a with high-security stock Android, using the NIST framework to assess the effectiveness of digital data recovery and integrity.

Introduction

The exponential development of telecommunications technology has made mobile devices, especially smartphones, a primary necessity for the global community.

This phenomenon has been accompanied by a shift in the modus operandi of cybercrime, with perpetrators now frequently using mobile devices to plan, carry out, and store evidence of criminal acts (Abdullah et al., 2024; Pandey et al., 2020). Stored digital data, ranging from text messages (SMS) and call logs to contacts and social media metadata, often becomes crucial digital evidence in legal proceedings.

However, challenges in mobile forensics are increasing as device storage capacity and security improve. Criminals are becoming more sophisticated in their use of anti-forensics techniques, such as encrypted data deletion, the use of secure messaging apps, and data manipulation to eliminate digital traces (Almuqren et al., 2024; Quick & Choo, 2013; Rathi et al., 2018). This poses the risk of losing critical data. Therefore, choosing the right forensic software is imperative for investigators to minimize the risk of data recovery failure and ensure the integrity of the evidence is maintained (Lwin et al., 2020; Roy et al., 2016; Tayeb & Varol, 2019).

In the digital forensics industry, Magnet Axiom and Cellebrite Physical Analyzer are among the most dominant software solutions used by law enforcement agencies. Both tools offer comprehensive features for acquisition and analysis, but differ in their working mechanisms and scanning algorithms (Elzahab et al., 2020; Gupchup & Mishra, 2019; Perumal et al., 2017). Previous studies, such as those by Sanap & Mane (2016); Javed et al. (2022), show that no single forensic tool can perfectly recover all types of data from all types of devices. These performance differences are often influenced by compatibility with operating systems, Android versions, and third-party application database structures (Al-Mousa et al., 2022; Mahajan et al., 2013). Therefore, continuous evaluation is necessary to measure the effectiveness of these tools on the latest generation of devices.

To ensure that the investigation process meets legal and scientific standards, the application of a structured methodology is a must. The framework developed by the National Institute of Standards and Technology (NIST) has become the de facto standard for digital forensics (Ayers et al., 2014; Kent et al., 2006; Kusumadewa et al., 2024). The NIST method requires four main stages: Preservation, Acquisition, Examination and Analysis, and Reporting. This approach ensures that each step in the handling of evidence is well documented, replicable, and maintains the chain of custody. Although much research has been conducted on the comparison of forensic tools (Elzahab et al., 2020; Osho & Ohida, 2016; Riadi et al., 2017), there is still a specific literature gap regarding data recovery performance on modern Android devices with high security standards, such as the Google Pixel 5a. Several previous studies have applied the NIST method (Riadi et al., 2020, 2021; Yudhana et al., 2020); however, this study differs in terms of the forensic tools and target device used. This device uses the stock Android operating system with strict security and encryption features, which represent a real challenge for investigators today (Do et al., 2015; Huber et al., 2016).

Based on this background, this study focuses on a comparative analysis of the performance of Magnet Axiom and Cellebrite in extracting digital evidence from a Google Pixel 5a. This study aims to measure the success rate based on data completeness, artifact accuracy, and category coverage in recovering various categories of data, including SMS, call logs, media, web browsing history, and social application data, using NIST methods as a procedural guide. This study is novel in that it evaluates the comparative performance of Magnet Axiom and Cellebrite on a modern stock Android device with enhanced security features, an area that has received limited empirical investigation. The results of this study are expected to provide empirical data-

based recommendations for forensic practitioners in choosing the most effective tools for comprehensive mobile investigations.

Method

This study uses a quantitative, comparative experimental approach. The objective is to measure and compare the effectiveness of two digital forensic software programs, namely Magnet Axiom and Cellebrite Physical Analyzer, in recovering digital evidence. The investigation process was carried out in accordance with the work standards issued by the National Institute of Standards and Technology (NIST) SP 800-86, which covers four main stages: preservation, acquisition, examination, and reporting.

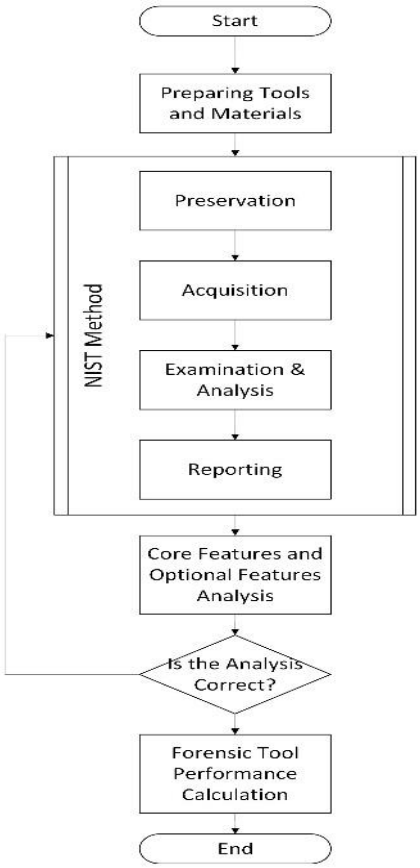

Figure 1 research stages
Source: primary data, processed

NIST framework

The application of the NIST framework in this study is described as follows: (1) Preservation: this stage focuses on protecting the integrity of the source digital data. The dataset in the form of a Google Pixel 5a digital image (disk image) is secured in an isolated condition to prevent data changes. Researchers ensure that the data is not modified during handling by calculating a hash value (MD5 or SHA-256) before and after the analysis to validate data integrity. (2) Acquisition: at this stage, data from the Google Pixel 5a forensic image is imported into multiple forensic tools. This process aims to copy all digital information from storage media to a controlled, secure environment. Magnet Axiom and Cellebrite Physical Analyzer are used to read the file system structure and extract raw data for further processing. (3) Examination and analysis: this is the core stage of the investigation. Researchers conduct an in-depth scan of the

acquired data to identify, filter, and classify evidence. The focus of the analysis includes: (a) Messages & communications: SMS, call logs, and instant messaging app data (WhatsApp, Telegram, etc.). (b) Media: image, video, and audio files. (c) Activity data: web browsing history, emails, and GPS geolocation logs. (d) System data: contact lists and installed applications. The findings from both tools are then manually verified to ensure data accuracy and completeness. (4) Reporting: the final stage documents the entire procedure and forensic findings. The report is structured to list a comparison of the amount of data successfully recovered by each tool, as well as the success rate based on measurement criteria.

Tools and materials

This study uses the hardware and software specifications and data set in Table 1.

Table 1 tools and materials specification

Nu.	Component	Specifications/description
1	Hardware	• Processor: 9th Generation Intel Core i5 • RAM: 16 GB DDR4 • Storage: 512 GB SSD (For temporary storage and application installation)
2	Software	• Magnet Axiom: Latest version used for processing, analysis, and reporting. • Cellebrite Physical Analyzer: Latest version used for logical acquisition, physical extraction (simulation from images), and in-depth analysis.
3	Object	• Device: Digital image (smartphone image) Google Pixel 5a. • Content: The dataset contains simulations of active user data (SMS, call logs, photos, videos, social app history, location data, and system files).

Source: primary data, processed

Research procedure

The research procedure was carried out through a series of sequential steps as follows: (1) Environment preparation: installing and configuring Magnet Axiom and Cellebrite Physical Analyzer on a high-specification computer. This process ensures that the operating system is free from interference that could affect forensic performance. (2) Dataset processing: Importing Google Pixel 5a digital image files into each forensic application. Both tools are configured to perform a deep scan to maximize data recovery, including deleted data. (3) Data extraction and collection: after the scanning process is complete, the extracted data is categorized by type (messages, contacts, media, etc.). Researchers record the total number of artifacts found by each tool. (4) Verification and validation: the extraction results from both tools are compared directly. Data found by one tool but not found by the other is analyzed to determine the cause (e.g., differences in database parsing or application version support). (5) Performance calculation: tool performance is measured using core and optional feature standards in mobile forensics. The success rate is calculated using the following equation (1):

$$Success\ Rate\ (\%) = \left(\frac{Number\ of\ Criteria\ Met}{Total\ Criteria\ (16\ NIST\ Standards)}\right) \times 100\% \qquad (1)$$

The criteria include the ability to recover SMS, call logs, contacts, images, videos, audio, documents, web browsing history, emails, geolocation, and social media application data.

Results and discussion

This section presents the implementation of digital forensic analysis based on the NIST framework, applied to a forensic image dataset of a Google Pixel 5a. It focuses on a quantitative and qualitative evaluation of the capabilities of two leading forensic tools, Magnet Axiom and Cellebrite Physical Analyzer.

Implementation of forensic analysis on Google Pixel 5a

The analysis process began with the preservation stage to ensure the integrity of the device image data was maintained. The data hash value was verified before and after the process. Next, in the acquisition stage, both software programs successfully loaded the dataset without data corruption. The core stage of the research involved examination and analysis, during which both tools were used to extract various types of digital artifacts.

Comparative data recovery analysis

The results of data extraction from Magnet Axiom and Cellebrite Physical Analyzer were compared quantitatively. A summary of the findings is presented in Table 2.

Table 2 quantitative comparison of digital data recovery

Data type/artifact	Cellebrite Physical Analyzer	Magnet Axiom	Notes
Messages & communications			
Short message service	132	135	Magnet Axiom is slightly superior in the number of SMS messages found.
Call logs	164	42	Cellebrite records complete details (incoming, outgoing, missed)
Phone contacts	770	113	Cellebrite successfully recovered contacts integrated with social media
Media & documents			
Audio files	740	740	Both are capable of recognizing audio files
Video files	391	391	Cellebrite: 76 files were unplayable.
Documents	6	6	Cellebrite: 1 document was unreadable.
Internet & application activity			
Web browsing history	5,685	113	Significant difference; Cellebrite is much more comprehensive
Email	207	0	Magnet Axiom had difficulty recovering email details
Social media applications	448 entries	0	Cellebrite extracts messages and media from FB, WA, IG, etc.
Geolocation (GPS/location)	48,615 points	83 points	Cellebrite provides very detailed location tracking.

Source: primary data, processed

Analysis of findings by category

Communication and contact data: Magnet Axiom showed slightly better performance in recovering SMS messages (135 messages compared to 132). However, Cellebrite Physical Analyzer was far superior in recovering *Call Logs* and *Contacts*. Cellebrite successfully extracted 770 contacts, which included contact information linked to social media accounts, while Magnet Axiom only found 113 contacts. Media and documents: both tools are capable of recognizing the presence of multimedia files. However, data validity is a concern. Of the 391 videos found by Cellebrite, 76 were

corrupt or unplayable, and one document was unreadable. This indicates that even though the file headers were successfully scanned, the body data may have been deleted or fragmented, as is common with overwritten data.

Internet, social media, and geolocation data: there is a huge performance gap in this category. Cellebrite Physical Analyzer successfully extracted 5,685 web browsing history entries and 48,615 geolocation points. In contrast, Magnet Axiom found only 113 web histories and 83 location points. Similarly, for social media applications (WhatsApp, Telegram, Instagram, etc.), Cellebrite successfully recovered 448 message and attachment entries, while Magnet Axiom failed or provided only minimal data. These results indicate that Cellebrite Physical Analyzer demonstrates superior performance in recovering network-based and application-level artifacts, while Magnet Axiom shows limited effectiveness in these data categories.

Forensic tool performance calculation

To assess overall effectiveness, the performance of both tools was evaluated based on 16 mobile forensic criteria standards (core and optional features) derived from the NIST methodology. These standards encompass recovery capabilities across all data categories discussed previously. Cellebrite Physical Analyzer: Successfully met 12 of 16 criteria, Success Rate = $\frac{12}{16} \times 100\% = 75\%$. Magnet Axiom: Successfully met 9 of 16 criteria, Success Rate = $\frac{9}{16} \times 100\% = 56.25\% \approx 56\%$.

These results indicate that Cellebrite Physical Analyzer demonstrates greater compliance with NIST-based mobile forensic criteria than Magnet Axiom. A higher success rate suggests that Cellebrite is more likely to provide comprehensive forensic artifacts across multiple data categories, thereby reducing the risk of incomplete evidence acquisition. This overall performance assessment is consistent with earlier category-based results, where Cellebrite outperformed Magnet Axiom in internet, social media, and geolocation data recovery. However, meeting a forensic criterion does not necessarily imply complete or error-free data recovery, as data integrity issues such as corruption or partial artifacts were still observed. Overall, the results suggest that Cellebrite Physical Analyzer is better suited for investigations requiring extensive artifact coverage. In contrast, Magnet Axiom may be more limited when evaluated against comprehensive NIST-based forensic standards.

Discussion

The results of this study demonstrate that Cellebrite Physical Analyzer significantly outperforms Magnet Axiom in recovering digital evidence from Google Pixel 5a devices, particularly in comprehensive forensic investigations. The most pronounced differences were observed in the extraction of complex user activity artifacts, including web browsing history, geolocation data, and content from social media applications. These findings are consistent with prior studies that report variations in forensic tool performance across device architectures, operating system versions, and application data structures. Previous research by Sanap & Mane (2016); Javed et al. (2022) similarly concluded that no single forensic tool can fully recover all categories of mobile data, especially when dealing with encrypted or application-level artifacts. The substantially higher volume of geolocation points and web history entries recovered by Cellebrite in this study suggests more effective database parsing and decryption mechanisms for the Android file system and application data structures used by the Google Pixel 5a.

This observation aligns with the findings of Mahajan et al. (2013); Al-Mousa et al. (2022), who emphasized that the effectiveness of mobile forensic tools is strongly influenced by their ability to adapt to evolving Android security mechanisms and third-party application databases. Cellebrite's superior performance in recovering network-based and location-based artifacts indicates stronger support for modern Android encryption schemes and application cache analysis. Such capabilities are increasingly critical, as contemporary Android devices store user activity data across multiple encrypted databases and sandboxed application directories.

Although Magnet Axiom demonstrated slightly superior performance in basic SMS recovery, its limited ability to extract detailed email records, social media communications, and geospatial information significantly restricts its effectiveness for investigations requiring reconstruction of a suspect's digital behavior. Similar limitations were also reported by Osho & Ohida (2016); Riadi et al. (2017), who found that Magnet Axiom was more effective for traditional communication artifacts but less effective when dealing with complex application-level data on newer Android platforms. The minimal web browsing history and the absence of recoverable social media artifacts in this study further suggest that the tool version used may not yet fully support the data structures and security implementations present on stock Android devices such as the Google Pixel 5a.

From a practical perspective, these findings indicate that Cellebrite Physical Analyzer is better suited for mobile forensic cases that require in-depth analysis of internet activity, instant messaging applications, and location-based evidence. This state supports earlier work by Perumal et al. (2017); Elzahab et al. (2020), which highlighted Cellebrite's relative strength in handling application artifacts and encrypted data. Magnet Axiom may still be applicable for targeted or limited forensic tasks, such as basic SMS or call log analysis; however, it is less appropriate as a primary tool for comprehensive investigations involving modern Android devices with advanced security features.

Furthermore, the presence of corrupted or unreadable multimedia files recovered by Cellebrite highlights an important limitation of automated forensic extraction, a concern also raised by Quick & Choo (2013); Tayeb & Varol (2019). A high recovery rate does not necessarily guarantee data integrity or evidentiary usability, particularly when dealing with overwritten or fragmented storage blocks. Therefore, forensic practitioners should not rely solely on automated tool output; they must manually verify and validate extracted artifacts to ensure the reliability and admissibility of digital evidence.

Finally, while this study provides a comparative evaluation based on NIST-derived mobile forensic criteria, it is important to acknowledge its limitations. The analysis was conducted on a single device model and dataset; thus, tool performance may vary across different Android versions, device manufacturers, and software revisions. Nevertheless, the results reinforce the applicability of the NIST forensic framework for assessing both quantitative recovery performance and qualitative artifact reliability, while also providing empirical evidence on the effectiveness of forensic tools on modern stock Android devices with enhanced security mechanisms.

Conclusions

This study evaluated the performance of two widely used mobile forensic tools, Magnet Axiom and Cellebrite Physical Analyzer, in extracting digital evidence from a

Google Pixel 5a device using the NIST forensic framework. Based on both quantitative recovery metrics and qualitative artifact assessment, the results demonstrate clear differences in the capabilities of the two tools when applied to a modern Android device with enhanced security mechanisms. Overall, Cellebrite Physical Analyzer exhibited superior performance in recovering a wide range of digital artifacts, particularly those related to internet activity, geolocation, and social media applications. The tool successfully met 12 out of 16 NIST-based mobile forensic criteria, achieving a success rate of 75%, compared to Magnet Axiom's 56%. This indicates that Cellebrite provides broader forensic coverage and is more effective for comprehensive investigations that require reconstructing user behavior and digital activity patterns.

Although Magnet Axiom showed slightly better performance in basic SMS recovery, its limitations in extracting application-level artifacts, such as emails, social media communications, and detailed web browsing histories, reduce its suitability for in-depth mobile forensic investigations. These findings confirm that tool effectiveness is highly dependent on the type of data being targeted, as well as compatibility with the underlying operating system and application data structures. The study also highlights an important limitation of automated forensic tools: a higher recovery rate does not necessarily guarantee data integrity or usability. The presence of corrupted or unreadable multimedia files underscores the need for manual verification and expert validation to ensure the reliability and admissibility of digital evidence in legal contexts.

In practical terms, this research suggests that Cellebrite Physical Analyzer is a more appropriate primary tool for forensic examinations involving modern Android devices, particularly in cases requiring extensive artifact coverage and analysis of complex user activity. Magnet Axiom may still be valuable for targeted or supplementary analysis, especially for traditional communication artifacts such as SMS and call logs. However, it should not be relied upon as the sole tool for comprehensive investigations. Finally, while this study provides empirical insight into the performance of mobile forensic tools on a Google Pixel 5a device, the findings are limited to a single dataset and device model. Future research should extend this evaluation to multiple Android devices and operating system version, broaden testing beyond Android to include other platforms such as iOS across different usage scenarios, and incorporate various forensic tool releases to validate further and generalize the conclusions. In addition, future studies should focus on evaluating tool capabilities in recovering strongly encrypted and permanently deleted data, as well as on developing more specific measurement standards for emerging data types as technology continues to evolve.

References

Abdullah, K. N., Kamal, S. N.-I. M., Ibrahim, O., Tan, Y.-L., Mokhtar, N. A., & Shoid, M. S. M. (2024). Adoption of Digital Forensic Practice: A Framework Development for Malaysian Organizations. *Journal of Electrical Systems*, *20*(10s), 5764–5773. https://journal.esrgroups.org/jes/article/view/6437

Al-Mousa, M. R., Al-Zaqebah, Q., Saeb Al-Sherideh, A., Al-Ghanim, M., Samara, G., Al-Matarneh, S., & Asassfeh, M. (2022). Examining Digital Forensic Evidence for Android Applications. *2022 International Arab Conference on Information Technology (ACIT)*, 1–8. https://doi.org/10.1109/ACIT57182.2022.9994221

Almuqren, A., Alsuwaelim, H., Rahman, M. M. H., & Ibrahim, A. A. (2024). A Systematic Literature Review on Digital Forensic Investigation on Android Devices. *Procedia Computer Science*, *235*, 1332–1352. https://doi.org/10.1016/j.procs.2024.04.126

Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics*.

https://doi.org/10.6028/NIST.SP.800-101r1

Do, Q., Martini, B., & Choo, K.-K. R. (2015). A Cloud-Focused Mobile Forensics Methodology. *IEEE Cloud Computing*, *2*(4), 60–65. https://doi.org/10.1109/MCC.2015.71

Elzahab, R. M. A., Al-Rahmawy, M. F., & Hamza, T. T. (2020). Comparative Study of Different Mobile Forensic Tools for Extracting Evidence from Android Devices. *Mansoura Journal for Computer and Information Sciences*, *16*(1), 1–12. https://doi.org/10.21608/mjcis.2020.321070

Gupchup, N., & Mishra, N. (2019). A Systematic Survey on Mobile Forensic Tools Used for Forensic Analysis of Android-Based Social Networking Applications. In *Data, Engineering and Applications* (pp. 205–215). Springer Singapore. https://doi.org/10.1007/978-981-13-6351-1_16

Huber, M., Taubmann, B., Wessel, S., Reiser, H. P., & Sigl, G. (2016). A flexible framework for mobile device forensics based on cold boot attacks. *EURASIP Journal on Information Security*, *2016*(1), 17. https://doi.org/10.1186/s13635-016-0041-4

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access*, *10*, 11065–11089. https://doi.org/10.1109/ACCESS.2022.3142508

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response*. https://doi.org/10.6028/NIST.SP.800-86

Kusumadewa, R. B., Syaifuddin, S., & Sari, Z. (2024). Comparative Analysis of Forensic Digital Evidence on Android Smartphone based Instant Messaging Using NIST Framework. *Jurnal Repositor*, *4*(3). https://doi.org/10.22219/repositor.v4i3.31109

Lwin, H. H., Aung, W. P., & Lin, K. K. (2020). Comparative Analysis of Android Mobile Forensics Tools. *2020 IEEE Conference on Computer Applications(ICCA)*, 1–6. https://doi.org/10.1109/ICCA49400.2020.9022838

Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. *International Journal of Computer Applications*, *68*(8), 38–44. https://doi.org/10.5120/11602-6965

Osho, O., & Ohida, S. O. (2016). Comparative Evaluation of Mobile Forensic Tools. *International Journal of Information Technology and Computer Science*, *8*(1), 74–83. https://doi.org/10.5815/ijitcs.2016.01.09

Pandey, A. K., Tripathi, A. K., Kapil, G., Singh, V., Khan, M. W., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Current Challenges of Digital Forensics in Cyber Security. In *Critical Concepts, Standards, and Techniques in Cyber Forensics* (pp. 31–46). https://doi.org/10.4018/978-1-7998-1558-7.ch003

Perumal, S., Navarathnam, S., Vosse, C. De, Samsuddin, S. B., & Samy, G. N. (2017). Comparative Studies on Mobile Forensic Evidence Extraction Open Source Software for Android Phone. *Advanced Science Letters*, *23*(5), 4483–4486. https://doi.org/10.1166/asl.2017.8922

Quick, D., & Choo, K.-K. R. (2013). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation*, *10*(3), 266–277. https://doi.org/10.1016/j.diin.2013.07.001

Rathi, K., Karabiyik, U., Aderibigbe, T., & Chi, H. (2018). Forensic analysis of encrypted instant messaging applications on Android. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 1–6.

https://doi.org/10.1109/ISDFS.2018.8355344

Riadi, I., Sunardi, S., & Sahiruddin, S. (2020). Perbandingan Tool Forensik Data Recovery Berbasis Android menggunakan Metode NIST. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *7*(1), 197–204. https://jtiik.ub.ac.id/index.php/jtiik/article/view/1921

Riadi, I., Umar, R., & Firdonsyah, A. (2017). Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(5), 3–8. https://www.researchgate.net/publication/317620078

Riadi, I., Umar, R., & Syahib, M. I. (2021). Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(1), 45–54. https://doi.org/10.29207/resti.v5i1.2626

Roy, N. R., Khanna, A. K., & Aneja, L. (2016). Android phone forensic: Tools and techniques. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 605–610. https://doi.org/10.1109/CCAA.2016.7813792

Sanap, V. K., & Mane, V. (2016). Comparative Study and Simulation of Digital Forensic Tools. *International Conference on Advances in Science and Technology*. https://www.ijcaonline.org/proceedings/icast2015/number1/24217-3002/

Tayeb, H. F., & Varol, C. (2019). Android Mobile Device Forensics: A Review. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 1–7. https://doi.org/10.1109/ISDFS.2019.8757493

Yudhana, A., Fadlil, A., & Setyawan, M. R. (2020). Analysis of Skype Digital Evidence Recovery based on Android Smartphones Using the NIST Framework. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(4), 682–690. https://doi.org/10.29207/resti.v4i4.2093