International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

EFFICIENCY AND RELIABILITY OF FORENSIC TOOLS IN RECOVERING ANDROID WHATSAPP DATA: A COMPARATIVE STUDY

Aman Sharma[1], Dr. Bhuvnesh Yadav[1*], Bhavya Sharma[1]
[1]Department of Chemistry, Biochemistry and Forensic Science, Amity School of Applied Sciences, Amity University Haryana.
***Corresponding Author:** Dr. Bhuvnesh Yadav, Email ID: bhuvneshyadav@gmail.com

Abstract
The global increase in mobile phone usage and internet access has contributed to a corresponding rise in cybercrimes, which are not confined to specific geographical regions. Mobile devices involved in criminal activities provide valuable investigative data, thereby increasing the importance of mobile forensics. WhatsApp, as the most widely used instant messaging application, facilitates extensive information exchange. However, frequent application updates and enhanced device security pose challenges to forensic data extraction, necessitating efficient techniques to maximize recoverable data within limited timeframes. This study aims to develop a database of commercially available mobile devices by examining 30 Android smartphones using MSAB XRY and Oxygen Forensic® Detective. Data extraction methods included logical, file system, and physical techniques, applied according to each tool's capabilities. The extracted WhatsApp database comprised media files, call logs, text messages, and application log entries. Statistical analysis revealed significant differences between the tools, with MSAB XRY retrieving a higher volume of WhatsApp-related files compared to Oxygen Forensic® Detective.

Keywords: *Mobile Forensics, WhatsApp, Data Extraction, MSAB XRY, Oxygen Forensic® Detective*

Introduction
The advent of smartphones has revolutionized the communication industry, transforming mobile devices into multifunctional tools. Beyond basic voice communication, these devices now support a wide range of applications, including motion tracking, multimedia services, and instant messaging. The widespread availability of internet access on mobile phones has facilitated the proliferation of messaging platforms such as WhatsApp, Facebook Messenger, and Telegram [1].

Among these, WhatsApp stands out as one of the most widely used instant messaging applications, compatible with Android, iOS, and Windows mobile devices globally. According to estimates in 2024, approximately 2.95 billion users relied on WhatsApp worldwide [2]. The application enables communication via text messages, voice and video calls, file sharing (including audio, video, images, and documents), location sharing, contact sharing, and recently, UPI-based payments in India. Each update introduces new features for users, such as the ability to delete sent messages within an hour or edit messages. Additionally, WhatsApp has launched a business version to facilitate global outreach for companies. The application employs end-to-end encryption, using the Signal encryption protocol to ensure that only the intended sender and recipient can access the exchanged content.

From a forensic perspective, WhatsApp users store data in multiple artifacts across different device locations, which may hold evidential value. On Android devices, these artifacts are typically located in the device's flash memory or Secure Digital (SD) cards. The WhatsApp database comprises two primary file types: msgstore.db and wa.db. The msgstore.db serves as the main chat database, containing message data, chat lists, and SQLite_sequence tables to enhance functionality [3]. The wa.db stores contact information, Android metadata, and SQLite sequences. For investigative purposes, msgstore.db holds the most critical evidentiary information.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The diversity of device models, chipsets, and features complicates forensic investigations [4]. For instance, Samsung's Exynos processors implement enhanced security measures such as DRAM encryption [5]. Qualcomm Snapdragon, based on ARM architecture, incorporates Cortex CPU technology to improve device performance and efficiency [6]. MediaTek employs multiple architecture systems, including ARM Cortex CPU, Dimensity, ARM Immortalis, DORA, Helio G96, and Tri-Cluster [7]. These hardware variations, combined with differing operating system versions, create significant challenges in mobile forensic investigations.

Among mobile operating systems, Android's affordability, flexibility, and efficiency have led to its market dominance. Consequently, the likelihood of Android devices being involved in criminal activities has increased significantly. Android's architecture comprises five layers: the Linux Kernel, hardware abstraction, libraries, applications, and an application framework [8]. WhatsApp operates primarily within the application and application framework layers.

Smartphones are increasingly encountered as evidence in modern criminal investigations. With billions of WhatsApp users worldwide, the application plays a critical role in investigations, increasing the demand for digital forensic analysis. While investigative agencies can trace traditional cellular calls and SMS, WhatsApp's end-to-end encryption prevents access to communications without the user's device, necessitating direct extraction of WhatsApp data from mobile phones.

Prior research has explored various methods for extracting WhatsApp data. A study employing EnCase, UFED, and Oxygen Forensic® Detective on Android, iOS, and Windows mobile phones demonstrated successful data extraction from Android and iOS devices but failed on Windows phones due to advanced security features [9]. Another study focused on forensic analysis of WhatsApp and Line Messenger, emphasizing the extraction of pictures, videos, and audio files [10]. Python programming has also been utilized to extract WhatsApp application data from Android smartphones for forensic analysis [11].

Further studies outlined methods for forensically retrieving WhatsApp data using a WhatsApp Key Extractor and database decryptor, analyzed with SQLite Database Browser [12]. Using this approach, conversations stored in both internal and external memory were retrieved and transformed into readable text formats. Jhala (2015) investigated non-rooted Android devices, decrypting encrypted WhatsApp databases and recovering deleted messages [13].

Despite these studies, research on extracting WhatsApp data from a diverse range of Android devices with varying chipsets remains limited. To address this gap, the present study prepares a database of thirty Android mobile phones to extract all types of WhatsApp data, including text messages, audio/video call records, media files, payment histories, and contacts, using two distinct mobile forensic tools: MSAB XRY and Oxygen Forensic® Detective. This comparative analysis aims to provide actionable insights for digital investigators worldwide and assist in selecting the most effective tool for data extraction from specific mobile devices.

Materials and Methods

This study aims to evaluate the extraction of encrypted and decrypted WhatsApp data from Android smartphones using MSAB XRY and Oxygen Forensic® Detective mobile forensic tools. The investigation focused on recovering a range of WhatsApp artifacts, including text messages, audio and video calls, media files, documents, location data, and payment histories. A comparative analysis was performed to assess the efficiency and completeness of data extraction across both tools.

Collection of Mobile Devices

Thirty Android-based smartphones were randomly selected from seven major manufacturers: Samsung, Oppo, Xiaomi, Vivo, Realme, Lenovo, and Motorola. The devices were categorized

Received: August 02, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

according to their chipset architecture: Exynos, Qualcomm Snapdragon, and MediaTek. Detailed specifications of the selected devices are provided in Tables 1, 2, and 3.

Table 1: Exynos Chipset-Based Mobile Devices

Sr. No.	Mobile Device	Make	Model	Version	Chipset
1.	Android	Samsung	SM-A305F	Android 11	Exynos 7904
2.	Android	Samsung	SM-A127F	Android 13	Exynos 850
3.	Android	Samsung	SM-A135F	Android 13	Exynos 850
4.	Android	Samsung	SM-S908E	Android 13	Exynos 2200
5.	Android	Samsung	SM-A146B	Android 14	Exynos 1330
6.	Android	Samsung	SM-A336E	Android 14	Exynos 1280
7.	Android	Samsung	SM-A546E	Android 14	Exynos 1380

Table 2:Qualcomm-Snapdragon Chipset-Based Mobile Devices

Sr. No.	Mobile Device	Make	Model	Version	Chipset
1.	Android	Samsung	SM-A207F	Android 11	Qualcomm SDM450 Snapdragon 450
2.	Android	Samsung	SM-G770F	Android 13	Qualcomm SM8150 Snapdragon 855
3.	Android	Samsung	SM-G781B	Android 13	Qualcomm SM8250 Snapdragon 865
4.	Android	Samsung	SM-F926B	Android 14	Qualcomm SM8350 Snapdragon 888
5.	Android	Samsung	SM-G990E	Android 14	Qualcomm SM8350 Snapdragon 888
6.	Android	Vivo	V2151	Android 13	Qualcomm SM7325 Snapdragon 778G
7.	Android	Vivo	V2250	Android 13	Qualcomm SM7325 Snapdragon 778G
8.	Android	Xiaomi	Redmi Note 5	Android 8.1	Qualcomm SDM636 Snapdragon 636
9.	Android	Xiaomi	Mi A1	Android 9	Qualcomm MSM8953 Snapdragon 625
10.	Android	Lenovo	A6020 A40	Android 11	Qualcomm MSM8929

Received: August 02, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

					Snapdragon 415
11.	Android	Motorola	Moto G84	Android 13	Qualcomm SM6375 Snapdragon 695

Table 3:MediaTek Chipset-Based Mobile Device

Sr. No.	Mobile Device	Make	Model	Version	Chipset
1.	Android	Samsung	SM-A346E	Android 14	MediaTek Dimensity 1080
2.	Android	Vivo	V2109	Android 12	MediaTek MT6769V
3.	Android	Vivo	V2130	Android 12	MediaTek Dimensity 920
4.	Android	Oppo	CPH8125	Android 10	MediaTek MT6765 Helio P35
5.	Android	Oppo	CPH1911	Android 11	MediaTek MT6771 Helio P70
6.	Android	Oppo	CPH2213	Android 13	MediaTek Dimensity 800U
7.	Android	Xiaomi Redmi	M2006C3LII	Android 10	MediaTek MT6762G Helio G25
8.	Android	Realme	RMX2189	Android 11	MediaTek MT6765G Helio G35
9.	Android	Realme Narzo	RMX2117	Android 12	MediaTek Dimensity 800U
10.	Android	Realme	RMX3771	Android 13	MediaTek Dimensity 7050
11.	Android	Vivo	V2060	Android 11	MediaTek Dimensity 700
12.	Android	Vivo	V2207	Android 13	MediaTek MT6769Z Helio G85

Research Tools for Data Extraction

Two commercially available forensic tools, MSAB XRY v.10.1.0 and Oxygen Forensic® Detective v.15.4, were employed for data extraction. The study aimed to recover WhatsApp artefacts, including text messages, audio/video calls, images, documents, locations, and other media files. Extraction methods were applied according to the capabilities of each tool for the respective device model and included:

- Logical Extraction: retrieval of application-level data without modifying the file system.
- File System Extraction: access to application databases, system logs, and structured data within the device storage.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Physical Extraction: complete bit-by-bit acquisition of device storage, allowing maximum recovery of encrypted or deleted data.

Physical extraction was prioritized where feasible, followed by file system and logical extractions. Comparative analyses assessed the volume and types of WhatsApp data recovered from both forensic tools.

Statistical Analysis

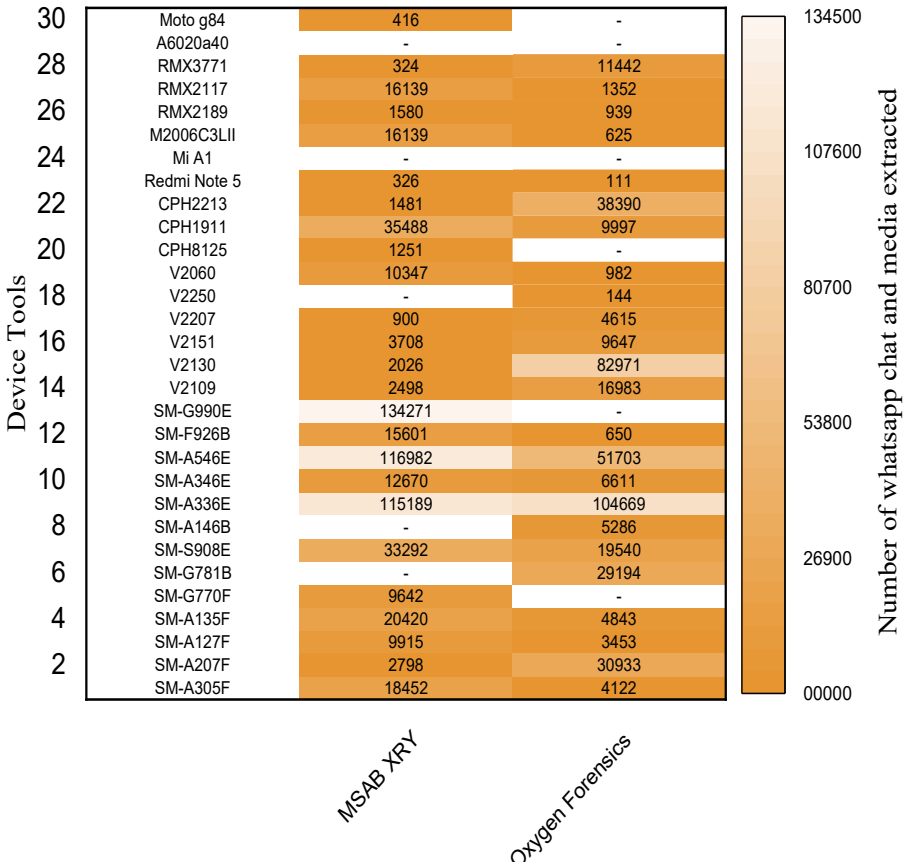
Statistical evaluation was conducted using a Two-Sample t-test to determine significant differences between the amounts of WhatsApp data extracted by MSAB XRY and Oxygen Forensic® Detective. The null hypothesis (H_0) assumed equality of means ($\mu_1=\mu_2$), while the alternative hypothesis (H_1) proposed inequality ($\mu_1\neq\mu_2$), where μ_1 represents the mean of data extracted by MSAB XRY and μ_2 represents the mean extracted by Oxygen Forensic® Detective. A p-value < 0.05 was considered statistically significant. A p-value below this threshold resulted in rejection of H_0, indicating a significant difference in extraction performance between the two tools.

Results

WhatsApp Data Extraction Overview

The study examined WhatsApp data extraction from 30 Android smartphones using MSAB XRY and Oxygen Forensic® Detective. Extracted data included text messages, media files (images, videos, audio), call logs (audio and video), and records of deleted content. Extraction methods applied were Logical, File System, and Physical, depending on device compatibility and tool capabilities.

Across all devices, 17 out of 30 smartphones underwent similar extraction types in both tools. MSAB XRY primarily utilized Logical extraction or its subtype on 24 devices, whereas Oxygen Forensic® Detective employed 14 logical and 7 physical extractions (Figure 1).



International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 1: Heatmap Comparison of Whatsapp data extracted from MSAB XRY and Oxygen Forensics

Tool Performance Comparison

- Overall, MSAB XRY consistently extracted larger volumes of WhatsApp data across most devices, particularly those with Exynos 7904 and MediaTek Dimensity chipsets. Conversely, Oxygen Forensic® Detective exhibited better performance on specific Qualcomm Snapdragon 450 devices, such as the SM-A207F.
- Certain devices showed tool-specific performance where only one tool successfully extracted data. For instance, the SM-G781B device yielded data exclusively via Oxygen Forensic® Detective, whereas the SM-G990E produced data only through MSAB XRY. These differences highlight tool-specific compatibility with device architecture and OS security features.

Chipset-Based Extraction Analysis

- Exynos: MSAB XRY demonstrated superior extraction performance on devices such as SM-A336E and SM-A546E, recovering extensive WhatsApp artifacts. Older Exynos models had slightly lower extraction values, suggesting incremental improvements in data accessibility in newer devices.
- Qualcomm Snapdragon: Extraction success was variable. While Oxygen Forensic® Detective performed optimally on mid-range devices like SM-A207F, MSAB XRY showed higher extraction values for high-end models such as SM-G990E. Lower-end Snapdragon devices exhibited lower recovery rates, possibly due to OS limitations or chipset-specific security configurations.
- MediaTek Dimensity: Extraction results were inconsistent. Some devices, such as CPH1911, produced very high extraction values with MSAB XRY (35,488 artifacts), whereas others, like CPH8125, showed limited recovery. Oxygen Forensic® Detective performed moderately well on devices like V2130, highlighting differences in tool efficiency based on chipset architecture and firmware.

Operating System Version and Patch-Level Effects

- Device Operating System versions significantly influenced extraction outcomes. Devices running Android 14 (e.g., SM-A336E, SM-A546E) generally yielded high extraction values. However, certain models such as SM-A146B had incomplete data with MSAB XRY, likely due to security patches and updated encryption mechanisms.
- Older Operating System versions (Android 8.1, 9, 11) displayed low extraction rates or no retrievable data, suggesting better tool compatibility with modern Android builds and the limitations of legacy OS support.
- Patch levels also played a role in the extraction. Devices with recent security patches (2024) still allowed substantial data recovery, indicating that forensic tools are regularly updated to handle contemporary Android protections. Conversely, older patch levels (e.g., Mi A1, A6020 A40) often failed to produce extractable data, likely due to outdated support in forensic software.

Statistical Analysis

- Two-sample t-tests were performed to compare the average number of WhatsApp artefacts extracted by MSAB XRY and Oxygen Forensic® Detective.
- The WhatsApp data extracted from mobile phones indicated no statistical difference for all Exynos, Qualcomm-Snapdragon and MediaTek, as the p-value is greater than the significance value of 0.05.
- For Exynos-based mobile phones, the p-value of the Two-Tailed t-test was found to be 0.95, which indicated no significant difference among the means of the three software. For Qualcomm-

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Snapdragon-based mobile phones, the p-value of the Two-Tailed t-test was found to be 0.46, which indicated no significant difference among the means of the three software. For MediaTek-based mobile phones, the p-value of the Two-Tailed t-test was found to be 0.95, which indicated no significant difference among the means of the three software's (Table 4).

Table 4: Two-Tailed t-test analysis for Exynos, Qualcomm-Snapdragon and MediaTek chipsets Android mobile phone devices

S.No.	Devices	t-Statistics	p-value
1.	Exynos	0.05	0.95
2.	Qualcomm-Snapdragon	0.73	0.46
3.	MediaTek	0.06	0.95

Device-Specific Observations

- High-end Exynos and MediaTek devices produced the largest number of WhatsApp artefacts.
- Mid-range Snapdragon devices exhibited selective tool efficiency, highlighting the need to match forensic tools with device architecture for optimal results.
- Devices with newer OS versions generally showed higher extraction success but occasional missing data, emphasizing the evolving challenge posed by frequent security updates (Figure 2).

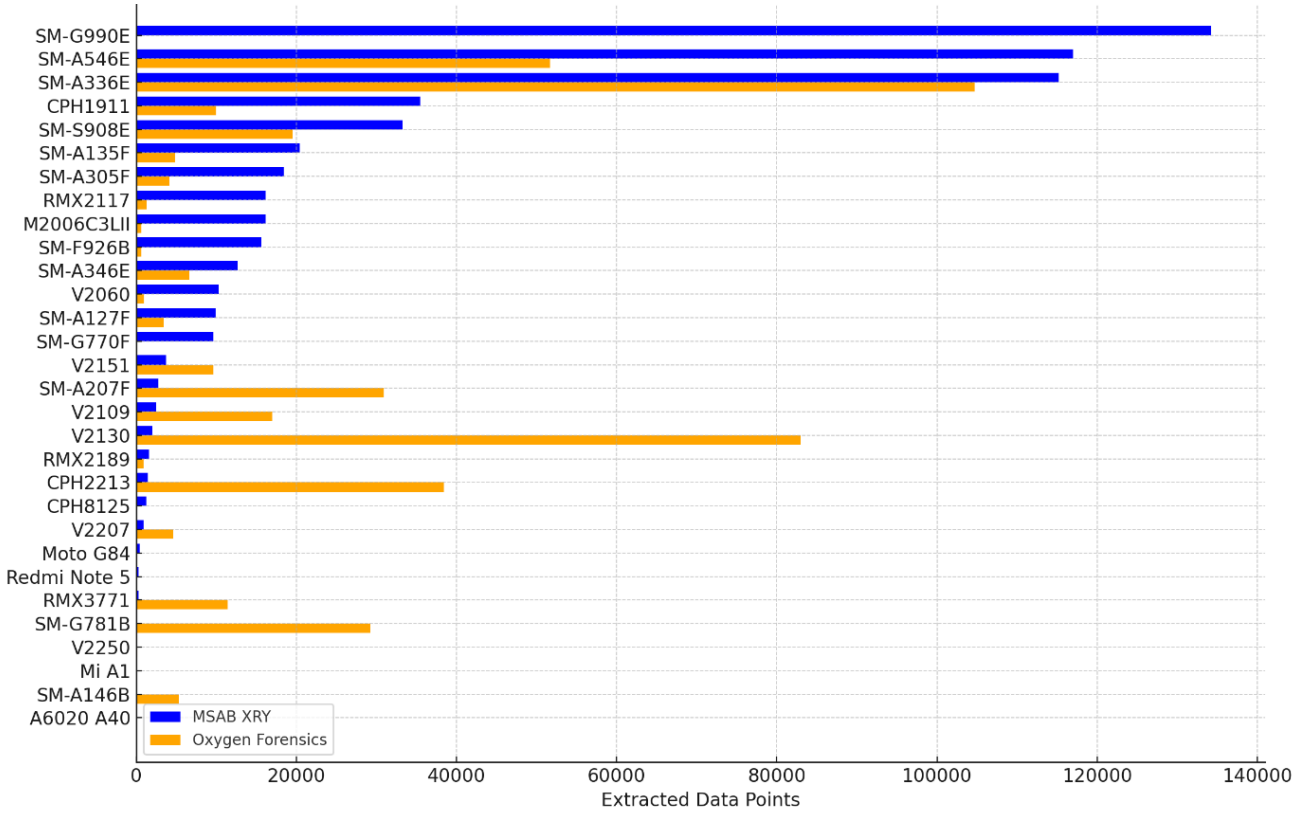


Figure 2: Device Comparison of Data Extraction for MSAB XRY and Oxygen Forensic® Detective

Summary of Findings

1. MSAB XRY is generally more effective across diverse Android devices, particularly for Exynos and MediaTek chipsets.

Received: August 02, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Oxygen Forensic® Detective demonstrates selective superiority on certain Snapdragon devices.
3. Extraction success is influenced by OS version, patch level, and chipset type, emphasizing the need for a multifaceted approach in mobile forensics.
4. Statistical analysis confirms a significant overall difference in performance, with MSAB XRY outperforming Oxygen Forensic® Detective on average.

Discussion

Several prior studies have attempted to evaluate the effectiveness of forensic tools in recovering WhatsApp data from mobile devices, though with varying scope and methodology. For instance, Shortall and Azhar [9] compared EnCase, UFED, and Oxygen Forensic® Detective across Android, iOS, and Windows platforms, finding reliable extractions for Android and iOS but limited success on Windows devices due to heightened security. Similarly, Alissa et al. [10] conducted a comparative study of WhatsApp forensic tools, emphasizing the recovery of media artefacts such as images and audio files, but their analysis was restricted to a smaller set of devices. Sahu [11] proposed Python-based methods for WhatsApp database extraction from Android devices, demonstrating flexibility but requiring programming expertise, which limits widespread forensic applicability. Kunang and Khristian [12] introduced a decryption-based approach using WhatsApp Key Extractor and SQLite Browser, successfully retrieving deleted conversations, though their focus was confined to application-level artefacts. More recently, Umar et al. [14] assessed multiple forensic tools using NIST metrics, highlighting variations in completeness and accuracy of recovered data. Compared to these works, the present study extends the scope by systematically analyzing thirty Android smartphones with diverse chipsets and OS versions, and by directly comparing two advanced commercial tools, MSAB XRY and Oxygen Forensic® Detective thereby providing a more comprehensive and practical evaluation for forensic practitioners.

Understanding WhatsApp's device-centric data storage model is essential for forensic investigations. The application stores messages, media, and logs in a local Database Management System (DBMS), while servers temporarily retain encrypted messages and delete them post-delivery, rendering server-side recovery infeasible. Consequently, device-level acquisition remains the primary source of actionable evidence.

Modern Android devices implement advanced security measures, including file-based encryption, hardware-backed key storage, and verified boot, challenging traditional extraction methods. Legacy tools such as WhatsApp DB/Key Extractor and Elcomsoft WhatsApp Explorer were limited to older Android versions [10, 14], necessitating updated solutions like MSAB XRY and Oxygen Forensic® Detective.

This study systematically evaluated WhatsApp artifact extraction across 30 Android devices with Exynos, Qualcomm Snapdragon, and MediaTek chipsets. MSAB XRY demonstrated higher consistency in logical extraction, particularly for Exynos and MediaTek devices, efficiently recovering text messages, media files, and call logs. Oxygen Forensic® Detective excelled selectively on certain Snapdragon devices, though it failed on some models (e.g., SM-G770F, SM-G990E, CPH8125, Moto G84). Tool-specific performance variations correlated with chipset architecture, operating system version, and security patch level. High-end devices generally yielded more recoverable artifacts, while older or heavily patched devices displayed limited extraction (Table 5).

Received: August 02, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 5: Device-Chipset-Tool Extraction Summary

Chipset	Device Examples	MSAB XRY Extraction	Oxygen Forensic® Detective Extraction	Observations
Exynos 7904/850	SM-A336E, SM-A546E	High (full artifacts)	Moderate	MSAB XRY excels in media recovery
Qualcomm Snapdragon	SM-A207F, SM-G990E	Moderate	High on mid-range	Tool performance device-specific
MediaTek Dimensity	CPH1911, CPH8125	High / variable	Moderate	Extraction depends on the firmware

Quantitative analysis via two-sample t-tests revealed no statistically significant difference in mean artefact recovery across chipsets ($p>0.05$), yet qualitative assessment highlighted MSAB XRY's superior retrieval of media artefacts and Oxygen Forensic® Detective's broader extraction capabilities, including full file system and physical acquisition.

Overall, forensic tool selection should be guided by device architecture, operating system build, and investigation requirements. The findings emphasize the need for adaptive methodologies and continuous tool updates to counter evolving Android security mechanisms, ensuring robust and comprehensive WhatsApp evidence recovery in forensic investigations.

Conclusion

This study systematically evaluated the efficiency and reliability of two widely used forensic tools, MSAB XRY and Oxygen Forensic® Detective, in extracting WhatsApp artifacts from thirty Android smartphones representing a broad spectrum of manufacturers, chipsets, and operating system versions. The findings reveal that while both tools are capable of retrieving valuable evidentiary data such as text messages, call logs, and media files, their performance is highly device- and chipset-dependent. MSAB XRY demonstrated consistently higher efficiency, particularly with Exynos and MediaTek devices, while Oxygen Forensic® Detective showed selective superiority on certain Snapdragon-based models. These outcomes highlight the importance of aligning forensic tool selection with the technical specifications of target devices in order to maximize data recovery.

Furthermore, the results underscore the influence of operating system versions and security patch levels on forensic success. Devices running the latest Android builds allowed significant extraction, though certain models demonstrated partial recoveries due to recent encryption updates. This finding emphasizes the dynamic nature of mobile forensics, where continuous adaptation of tools is necessary to address evolving security features.

Compared with earlier studies that either focused on fewer devices, single chipset categories, or limited tool comparisons, the present work offers a more comprehensive dataset and a direct head-to-head analysis of two advanced commercial solutions. By highlighting tool-specific strengths and limitations across diverse hardware and software environments, this research provides practical guidance for forensic investigators in selecting the most suitable tool for casework.

In conclusion, while no single tool guarantees complete recovery across all devices, MSAB XRY generally demonstrates broader reliability in Android WhatsApp investigations. However, the complementary strengths of Oxygen Forensic® Detective suggest that a multi-tool strategy remains the best practice for digital forensic laboratories. Future research should continue to evaluate tool

Received: August 02, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

performance against emerging smartphone architectures and encryption methods, ensuring that forensic methodologies evolve in step with rapid technological advancements.

Conflict of Interest

There is no conflict of interest among the authors.

References

[1] J. Ohme, M. M. P. Vanden Abeele, K. Van Gaeveren, W. Durnez, and L. De Marez, "Staying Informed and Bridging 'Social Distance': Smartphone News Use and Mobile Messaging Behaviors of Flemish Adults during the First Weeks of the COVID-19 Pandemic," *Socius: Sociological Research for a Dynamic World*, vol. 6, pp. 1–14, 2020, doi: 10.1177/2378023120950190.

[2] Statista, "Number of WhatsApp users worldwide from 2019 to 2024," *Statista Research Department*, 2020. [Online]. Available: https://www.statista.com.

[3] C. Anglano, "Forensic analysis of WhatsApp Messenger on Android smartphones," *Digital Investigation*, vol. 11, no. 3, pp. 201–213, 2014, doi: 10.1016/j.diin.2014.04.003.

[4] M. Ashawa and I. Ogwuche, "Forensic Data Extraction and Analysis of Left Artifacts on Emulated Android Phones: A Case Study of Instant Messaging Applications," *Circulation in Computer Science*, vol. 2, no. 11, pp. 1–7, 2017, doi: 10.22632/ccs-2017-252-67.

[5] T. Lee, D. Kim, and J. Kim, "Exynos 1080: High-performance, low-power CPU and GPU with AMIGO," in *Proc. IEEE Hot Chips 33 Symposium (HCS)*, 2021, pp. 1–16, doi: 10.1109/HCS52781.2021.9567394.

[6] G. Gambo, "Qualcomm Snapdragon: ARM-based Cortex CPU technology to improve device performance and efficiency," *Connection Science*, 2023.

[7] C. L. Lee, C. P. Chung, S. Y. Cheng, J. K. Lee, and R. Lai, "Accelerating AI performance with the incorporation of TVM and MediaTek NeuroPilot," *Connection Science*, vol. 35, no. 1, pp. 1–17, 2023, doi: 10.1080/09540091.2023.2272586.

[8] H. Saleous, M. Ismail, S. H. AlDaajeh, N. Madathil, S. Alrabaee, K. K. R. Choo, and N. Al-Qirim, "COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities," *Digital Communications and Networks*, 2023, doi: 10.1016/j.dcan.2022.06.005.

[9] A. Shortall and M. A. H. Bin Azhar, "Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms," in *Proc. 6th Int. Conf. Emerging Security Technologies (EST)*, 2015, pp. 1–6, doi: 10.1109/EST.2015.16.

[10] K. Alissa et al., "A comparative study of WhatsApp forensics tools," *SN Applied Sciences*, vol. 1, no. 11, pp. 1–13, 2019, doi: 10.1007/s42452-019-1312-8.

[11] S. Sahu, "An Analysis of WhatsApp Forensics in Android Smartphones," *International Journal of Engineering Research*, vol. 3, no. 5, pp. 306–310, 2014, doi: 10.17950/ijer/v3s5/514.

[12] Y. N. Kunang and A. Khristian, "Implementation of forensic procedures for WhatsApp applications on Android phones," in *Proc. Annual Research Seminar*, Dec. 2016, vol. 2, no. 1, pp. 1–6.

[13] K. Y. Jhala and G. L. Patel, "WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non-Rooted Android Devices," *Journal of Information Technology & Software Engineering*, vol. 5, no. 2, pp. 1–5, 2015, doi: 10.4172/2165-7866.1000147.

[14] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 12, pp. 69–75, 2017, doi: 10.14569/ijacsa.2017.081210.

Received: August 02, 2025