Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 11 Issue 42 (March 2026) PP. 423-436

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.gaexcellence.com/jistm

COMPARATIVE ANALYSIS OF METADATA IN IMAGE AND VIDEO FILES CAPTURED BY IOS AND ANDROID DEVICES

Hajar Izzati Mohd Ghazali[1], Nurezzlin Natasha Ramli[2], Fatin Nadhirah Zabani [3], Raihana Md Saidi [4]*

[1]Faculty of Computer and Mathematical Sciences, UiTM Cawangan Melaka Kampus Jasin, Melaka, Malaysia
hajarizzati@uitm.edu.my https://orcid.org/0009-0000-4437-3667
[2]Faculty of Computer and Mathematical Sciences, UiTM Cawangan Melaka Kampus Jasin, Melaka, Malaysia
nurezzlinatasha@gmail.com https://orcid.org/0009-0002-9686-8084
[3]Faculty of Computer and Mathematical Sciences, UiTM Cawangan Melaka Kampus Jasin, Melaka, Malaysia
fatinnadhirah@uitm.edu.my https://orcid.org/0009-0002-8833-0305
[4]Faculty of Computer and Mathematical Sciences, UiTM Cawangan Melaka Kampus Jasin, Melaka, Malaysia
raihana@uitm.edu.my https://orcid.org/0009-0007-8701-2408
*Corresponding Author

Article Info:

Article history:
Received date: 20.01.2026
Revised date: 12.02.2026
Accepted date: 22.03.2026
Published date: 31.03.2026

To cite this document:

Ghazali, H. I. M., Ramli, N. N., Zabani, F. N., & Md Saidi, R. (2026). Comparative Analysis of Metadata in Image and Video Files Captured by iOS and Android Devices. *Journal of Information System and Technology Management, 11* (42), 423-436.

Abstract:

This study investigates the extraction and analysis of metadata embedded in image and video files, focusing on the differences between iOS and Android platforms across various file formats. Metadata was extracted using three specialized tools: Metadata2go, ExifMeta, and ExifInfo. The research involved systematically retrieving files from both platforms, organizing them by format and operating system and conducting a comparative evaluation. Eight key metadata attributes were analyzed: device make, model, software version, timestamp, geographic coordinates (longitude and latitude), color space and lens model. Results indicate that iOS devices consistently retain more detailed and structured metadata than Android devices, reflecting architectural differences in metadata handling. This study underscores the critical role of metadata in digital forensics and information management.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

DOI: 10.35631/JISTM.1142025 **Keyword:**

Digital Forensics, Image and Video Files, iOS and Android Comparison, Metadata Analysis, Mobile Device Forensics

© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (http://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact jistm@gaexcllence.com.

Introduction

Metadata plays a fundamental role in the management, organization and analysis of digital media. Embedded within image and video files, metadata provides essential context such as creation date, device specifications, geolocation and software details. These attributes not only enhance user experiences but also hold significant value in digital forensics, legal investigations, content verification and archival processes.

In the mobile ecosystem, devices running on iOS and Android dominate the global market, each with unique system architectures and proprietary approaches to data handling. While both platforms embed metadata within captured media, the extent and consistency of metadata retention can vary depending on the operating system, file type and subsequent actions such as cloud storage or file transfers (Dai et al. 2022; Oh and Hwang, 2022).

Despite the wide use of smartphones for content creation, there is limited comparative analysis done by Steinböck et al. (2024), focusing on the richness and reliability of metadata preserved across iOS and Android environments. Moreover, the effectiveness of metadata extraction tools which are essential for forensic investigations and data verification has remains underexplored in the context of mobile media files and cloud storage platforms (Arizona et al. 2024).

This study addresses these gaps by performing a detailed comparative analysis of metadata in image and video files captured using iOS and Android devices. It evaluates the retention and consistency of metadata across different cloud services using three specialized tools: Metadata2go, ExifMeta, and ExifInfo. The study aims to determine which platform preserves metadata more comprehensively and to assess how extraction tools differ in performance. By identifying strengths and limitations in both platforms and tools, this research contributes practical insights to the fields of digital forensics, mobile computing and data integrity management.

Literature Review

The analysis of metadata in digital media has gained increasing attention due to its relevance in data authenticity, digital forensics and content management. Previous studies by Fakiha (2024); Gupta et al. (2023) have explored how metadata can support file provenance, facilitate forensic investigations and reveal device-specific behaviors. This section provides a review of literature related to cloud storage services, metadata classification frameworks, image metadata

standards and the functionality of metadata extraction tools, which collectively inform the context and significance of the present study.

Cloud Storage

Cloud storage refers to a service model that allows data to be stored remotely and accessed via the internet. It provides users with scalable storage solutions and convenient access from any compatible device. Examples of widely used cloud storage services include Google Drive, Microsoft OneDrive, and Apple iCloud.

Google Drive is a popular platform offered by Google, accessible through a Google account. It enables users to upload, download, edit and sync files across devices (Shreedhar et al., 2022). Similarly, Microsoft OneDrive offered by Microsoft and SharePoint used to supports cross-platform synchronization and includes powerful search functionalities and offline syncing via desktop applications (Riki et al., 2025).

Apple's iCloud service, introduced in 2011, succeeded earlier cloud services like iTools, Mac and MobileMe. The iCloud Drive feature allows Apple users to store and access multimedia and documents across devices with internet access. Apple provides 5 GB of free storage space and facilitates features such as data backup and location sharing (Mühlbacher, 2024).

Recent studies by Aneja et al., (2021); Mishra et al., (2022) have explored the capabilities of cloud storage platforms for managing files embedded with metadata, focusing on how these systems handle data integrity and information retrieval.

Metadata

Metadata refers to data that provides information about other data and is typically classified into six categories: structural, descriptive, preservation, administrative, provenance and definitional metadata (Mosha & Ngulube, 2023; Pacheco et al., 2023; Ulrich et al., 2022). Structural metadata organizes content relationships such as chapters and sections. Descriptive metadata helps identify resources and includes information such as title, subject and creation date (Gerhard, 2022).

Preservation metadata supports long-term data management, while administrative metadata covers governance, access rights and licensing. Attribution metadata records the origin and history of a resource and definitional metadata outlines the design and schema of databases, including tables and column attributes (Vayyala, 2025).

Image Metadata

Digital images often include embedded metadata that describes both technical and descriptive properties. Common standards include EXIF (Exchangeable Image File Format), XMP (Extensible Metadata Platform) and IPTC (Shaliyar & Mustafa, 2022). EXIF metadata is embedded in file types such as JPEG, HEIC and PNG and may contain information such as camera settings, GPS coordinates and timestamps (Soni, 2025; Kalaimagal et al., 2024).

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

Image metadata can be grouped into technical, descriptiveand administrative categories. Technical metadata includes camera specifications like ISO, shutter speed and location data. GPS coordinates are commonly embedded in images captured by smartphones and are considered vital for contextual analysis (Bikash, 2024).

Few research (Dang-Nguyen et al., 2023; Menahil et al., 2021; Faraz et al, 2024) conducted a comparative study on how iOS and Android applications handle image metadata on social media platforms. Their findings revealed that while some platforms preserve metadata, others strip most of it during upload. They proposed a Python-based EXIF extractor system capable of retrieving metadata from images using custom libraries.

Similarly, Bennabhaktula et al., (2022) proposed a forensic analysis framework that uses mobile camera sensor patterns to trace the origin of images. Their method could also establish connections between digital content and social media accounts using mobile camera fingerprinting (MCF), highlighting the forensic potential of image metadata.

Metadata Extraction Tools

Metadata extraction tools retrieve embedded data from images, videos and documents. While default mobile apps typically display only limited metadata such as image format, device model and dimensions have specialized tools which are required to extract detailed EXIF data.

Metadata2go is an online tool capable of extracting metadata from various file types, including GPS coordinates, copyright information and orientation data. However, it does not support exporting data to structured formats like Excel. Other tools, such as ExifMeta and ExifInfo, provide browser-based interfaces for uploading images via drag-and-drop or URL. These tools display metadata and may include glossaries or editing features, although they typically impose file size limits (Zheng et al., 2023).

Methodology

The iOS image captured by an iPhone 6s retained detailed metadata including file name, make, model, software version, date and time, GPS coordinates (latitude and longitude), color space and lens model. In contrast, the Android counterpart (vivo 1906) provided comparable metadata with slight variations in the GPS coordinates and lacked lens model information. The sample image used in this analysis is depicted in Figure 1.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

ANDROID_1.jpg iOS_1.jpg

Figure 1: Sample Of Image Captured for Extraction and Analysis

This study followed a structured four-step methodology to extract and analyze metadata from image and video files captured using iOS and Android devices. Figure 2 depicted the process of the research.

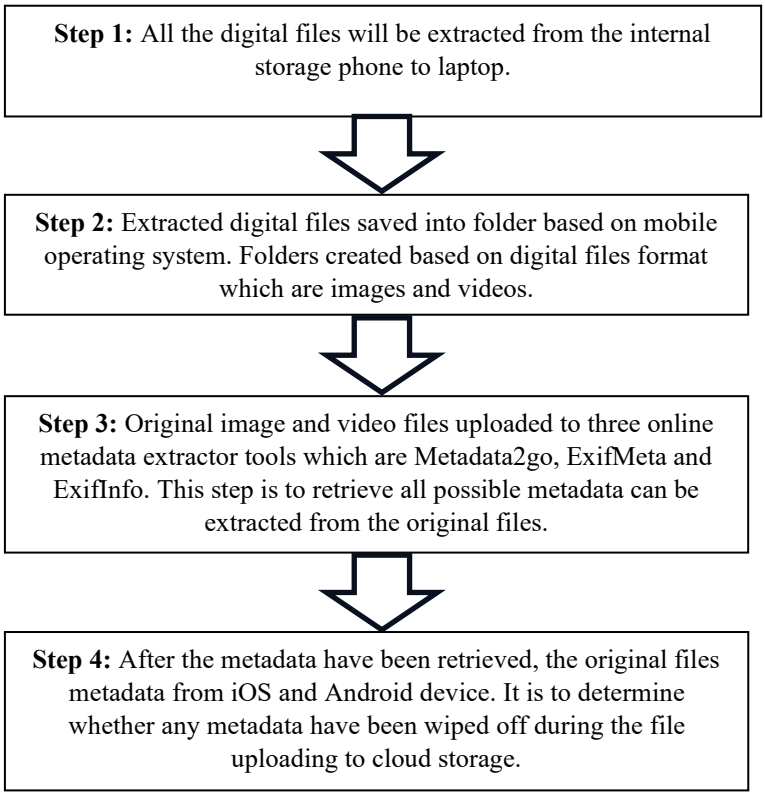

Figure 2: The Extraction and Analysis Flow

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

Step 1: Digital image and video files were first extracted directly from the internal storage of both iOS and Android smartphones to ensure that the original metadata remained intact. The files were then transferred to a laptop, creating a controlled environment for subsequent analysis. This step minimized the risk of metadata alteration that could occur if files were shared through messaging apps, cloud services, or social media platforms.

Step 2: Once transferred, the files were systematically organized into folders based on two criteria: the mobile operating system (iOS or Android) and the file format (image or video). This categorization was essential to enable structured comparison and to highlight differences in metadata attributes between platforms and media types. It also simplified the tracking of files and reduced the possibility of misclassification during analysis.

Step 3: The original files were then uploaded individually to three online metadata extraction tools namely Metadata2go, ExifMeta and ExifInfo. These tools were selected because they are accessible, widely used in digital forensic and research contexts and capable of retrieving a broad spectrum of metadata attributes. Using multiple tools helped mitigate tool-specific limitations and increased the reliability of the metadata extraction process.

Step 4: The retrieved metadata was carefully analyzed to evaluate its completeness, consistency and accuracy. Key attention was given to detecting whether metadata loss occurred during file transfer, particularly attributes like device details, capture date and time, GPS coordinates, and technical camera settings. The comparison also aimed to identify variations in how iOS and Android devices embed metadata in both images and videos. By cross-checking outputs across the three tools, inconsistencies or omissions could be identified, ensuring a more robust interpretation of the results. This methodology enabled a detailed comparative analysis of metadata integrity and richness across the two major mobile operating systems and ensured consistency using multiple extraction tools.

This structured approach ensured a systematic comparative analysis of metadata integrity and richness across iOS and Android platforms. By organizing files by platform and type, employing multiple metadata extraction tools and emphasizing cross-validation, the study minimized bias and provided reliable insights into platform-specific metadata practices.

Results and Discussions

The analysis of original image metadata from iOS and Android devices revealed notable differences in metadata availability and completeness.

Original Image Metadata Comparison (iOS vs Android)

These results suggest that iOS devices may preserve richer metadata natively compared to certain Android models, particularly in relation to hardware-specific attributes such as lens models and software build versions. The standardized ecosystem of iOS ensures that metadata fields are consistently embedded across devices, reducing variability and enhancing completeness. This uniformity contrasts with the fragmented Android environment, where differences among manufacturers and device tiers often result in missing or inconsistent metadata.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

The consistent structure and detailed metadata observed in iOS files provide significant advantages for digital forensic applications, as they enable more accurate device attribution, improved traceability of media files and stronger support for verifying authenticity. For example, reliable timestamps, geolocation data and detailed camera parameters strengthen evidentiary value by allowing investigators to reconstruct events with greater confidence. Table 1 illustrates these comparative differences, highlighting how the robustness of iOS metadata contributes to forensic reliability, whereas Android devices may present challenges due to omissions or inconsistencies in metadata fields.

Table 1: Original Image Metadata Comparison (iOS vs Android)

Metadata	*iOS Camera*	*Android Camera*
File Name	IOS_1.JPG	ANDROID_1.jpg
Make	Apple	vivo
Model	iPhone 6s	vivo 1906
Software	15.7.7	1906-user 11...
Date & Time	2023:08:11 17:31:16	2023:08:11 17:37:25
Longitude	102° 22' 2.95" E	102° 22' 3.3" E
Latitude	2° 8' 49.08" N	2° 8' 48.82" N
Color Space	sRGB	sRGB
Lens Model	4.15mm f/2.2	Not Available

Original Video Metadata Comparison (iOS vs Android)

When comparing the original video metadata, the iOS video (MOV format) demonstrated a higher level of metadata completeness compared to the Android video (MP4 format), as presented in Table 2. The iOS file contained detailed attributes such as device make and model, software version, creation date, GPS coordinates, frame rate, bitrate and codec information. In contrast, the Android file retained only basic technical attributes such as frame rate and codec, while omitting critical fields including device identification, software version, creation date and geolocation data.

This inconsistency highlights fundamental differences in how the two platforms handle metadata. iOS devices benefit from a closed and standardized ecosystem, ensuring uniform embedding of metadata across all devices and formats. Conversely, the Android ecosystem is fragmented, with device-specific firmware and varied encoding processes often discarding or failing to embed non-essential metadata during video recording. Such omissions can significantly reduce the evidentiary value of Android video files in forensic contexts, as the absence of timestamps, device identifiers, and location data limits traceability and authenticity verification.

The comparison of bitrates further reinforces this distinction. The iOS video exhibited a higher bitrate (47.9 Mbps compared to 14.5 Mbps on Android), suggesting that Apple prioritizes quality retention and richer encoding standards, even at the expense of larger file sizes. This not only enhances playback quality but may also contribute to the preservation of more detailed metadata during encoding. By contrast, Android devices particularly for mid-range or budget models that may prioritize storage efficiency and compatibility, leading to lower bitrates and metadata reduction.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

Together, these findings emphasize that while both platforms provide essential technical information, iOS devices generally preserve a broader and more detailed set of metadata attributes in video files, making them more reliable for forensic analysis and digital evidence validation.

Table 2: Original Video Metadata Comparison (iOS vs Android)

Metadata	*iOS Camera*	*Android Camera*
File Name	IOS_6.MOV	ANDROID_6.mp4
Make	Apple	Not Available
Model	iPhone 6s	Not Available
Software	15.7.7	Not Available
Creation Date	2023:08:11 17:48:40	Not Available
Longitude	102° 22' 3.36" E	Not Available
Latitude	2° 8' 48.84" N	Not Available
Frame Rate	30 fps	30 fps
Avg. Bitrate	47.9 Mbps	14.5 Mbps
Codec	H.264	H.264

iOS Image Metadata Consistency Across Cloud Storage Platforms

The metadata consistency across cloud storage platforms was evaluated using three extraction tools used in this research which are Metadata2go, ExifMeta and ExifInfo to assess whether metadata integrity was preserved after uploading and retrieving files from Google Drive, iCloud Drive and OneDrive. As shown in Tables 3 to 5, both Metadata2go and ExifInfo consistently extracted complete metadata across all tested platforms. Key attributes, including device make and model, software version, capture date and time, GPS coordinates, color space and lens model, were retained without alteration. This suggests that major cloud services do not inherently strip or alter embedded metadata during upload, storage, or download. From a forensic perspective, this finding is significant as it reinforces the evidentiary reliability of files transmitted through mainstream cloud environments, provided that the metadata was intact at the point of upload.

In contrast, ExifMeta exhibited persistent limitations. Although it was able to capture common metadata attributes such as make, model, software version, color space and lens model, it consistently failed to extract critical tags such as capture date/time and GPS coordinates. These omissions are more likely attributable to tool-level parsing errors or limited tag support rather than actual metadata loss during storage. Nonetheless, the inability to retrieve these essential attributes reduces the forensic utility of ExifMeta when used as a standalone tool. In practical scenarios, where timestamps and geolocation data are critical for establishing provenance, chronology and spatial context, reliance on ExifMeta alone could result in incomplete or misleading conclusions.

A cross-platform analysis further revealed notable differences between iOS and Android devices. iOS files demonstrated richer metadata preservation across cloud platforms, maintaining uniform access to attributes such as make, model, software version, capture date and GPS coordinates. This reflects Apple's closed and standardized ecosystem, where uniform encoding and consistent metadata embedding practices are enforced across devices. By contrast, Android files, particularly video formats, displayed systemic gaps in descriptive metadata, with missing fields persisting regardless of the cloud service or extraction tool used.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

These gaps likely stem from Android's fragmented ecosystem, variations in manufacturer firmware and encoding processes that often prioritize file size or playback compatibility over metadata richness.

For digital forensic practitioners, these findings highlight two key insights. First, the cloud storage environment itself does not compromise metadata integrity and therefore cloud-hosted media can generally be considered reliable in terms of metadata preservation. Second, the reliability of metadata extraction is heavily dependent on both the mobile platform as in iOS vs. Android and the chosen extraction tool. The limitations of certain tools, particularly ExifMeta, emphasize the need for multi-tool validation strategies to avoid overlooking critical metadata. Moreover, the systemic discrepancies between iOS and Android devices underscore the importance of platform awareness, as the evidentiary completeness of metadata can vary significantly depending on the device of origin.

Table 3: iOS Image Metadata Consistency Across Cloud Storage (Metadata2go)

Metadata	*Camera*	*Google Drive*	*iCloud Drive*	*OneDrive*
Make	Apple	Apple	Apple	Apple
Model	iPhone 6s	iPhone 6s	iPhone 6s	iPhone 6s
Software	15.7.7	15.7.7	15.7.7	15.7.7
Date & Time	2023:08:11 17:31:16	Same	Same	Same
GPS (Lat, Long)	Present	Present	Present	Present
Color Space	sRGB	sRGB	sRGB	sRGB
Lens Model	Present	Present	Present	Present

Table 4: iOS Image Metadata Consistency Across Cloud Storage (ExifInfo)

Metadata	*Camera*	*Google Drive*	*iCloud Drive*	*OneDrive*
Make	Apple	Apple	Apple	Apple
Model	iPhone 6s	iPhone 6s	iPhone 6s	iPhone 6s
Software	15.7.7	15.7.7	15.7.7	15.7.7
Date & Time	2023:08:11 17:31:16	Same	Same	Same
Longitude	102° 22' 2.95" E	Same	Same	Same
Latitude	2° 8' 29.08" N	Same	Same	Same
Color Space	sRGB	sRGB	sRGB	sRGB
Lens Model	Present	Present	Present	Present

Table 5: iOS Image Metadata Consistency Across Cloud Storage (ExifMeta)

Metadata	*Camera*	*Google Drive*	*iCloud Drive*	*OneDrive*
Make	Apple	Apple	Apple	Apple
Model	iPhone 6s	iPhone 6s	iPhone 6s	iPhone 6s
Software	15.7.7	15.7.7	15.7.7	15.7.7
Date & Time	[object Object]	[object Object]	[object Object]	[object Object]
Longitude	Not Available	Not Available	Not Available	Not Available

Latitude	Not Available	Not Available	Not Available	Not Available
Color Space	sRGB	sRGB	sRGB	sRGB
Lens Model	Present	Present	Present	Present

These findings highlight the variability in performance across metadata extraction tools. Metadata2go and ExifInfo are more reliable in capturing a comprehensive metadata set, especially for forensic purposes that require timestamp and geolocation data. ExifMeta deficiencies could hinder certain analyses and should be noted when selecting tools for forensic investigations.

Android Video Metadata Consistency Across Cloud Storage

Android video metadata remained consistent across all tested cloud platforms with respect to core technical parameters such as frame rate, bitrate and codec. This indicates that basic playback information is preserved reliably regardless of the storage or transfer medium. However, essential descriptive metadata including device make, model, software version, creation date and GPS coordinates were consistently absent across all storage locations and extraction tools. This absence suggests that the limitation is systemic, originating from the way Android devices embed or fail to embed metadata at the point of recording, rather than being caused by subsequent file handling or cloud storage processes.

As shown in Table 6, the lack of descriptive metadata in Android videos presents significant challenges in digital forensic investigations. Without attributes such as device identifiers or timestamps, it becomes more difficult to establish the provenance of a file, authenticate its source, or reconstruct a precise chronological sequence of events. Furthermore, the absence of GPS data eliminates the possibility of geospatial validation, which is often critical in correlating video evidence with real-world locations.

In contrast, iOS video metadata demonstrated greater resilience across cloud platforms. Attributes such as make, model, software version, creation date and GPS coordinates were consistently preserved alongside technical parameters, even after uploading and re-downloading from cloud services. This consistency reflects Apple's standardized approach to metadata embedding, which ensures uniformity and reduces the likelihood of information loss during storage or transfer. For forensic purposes, this preservation enhances the evidentiary value of iOS videos, as investigators can rely on metadata to verify authenticity, establish device provenance and reconstruct timelines with higher accuracy.

These findings underscore a key distinction between the two platforms: while both preserve technical playback metadata, iOS devices maintain a richer and more consistent set of descriptive attributes across environments, whereas Android devices exhibit systemic omissions that limit forensic reliability. Practitioners must therefore adapt their investigative strategies, accordingly, using supplementary evidence to compensate for Android metadata gaps while leveraging the richer metadata available in iOS files.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

Table 6: Android Video Metadata Consistency Across Cloud Storage (All Extractors)

Metadata	*Camera*	*Google Drive*	*iCloud Drive*	*OneDrive*
Make/Model/Software	Not Available	Not Available	Not Available	Not Available
Creation Date	Not Available	Not Available	Not Available	Not Available
Frame Rate	30 fps	30 fps	30 fps	30 fps
Avg. Bitrate	14.5 Mbps	14.5 Mbps	14.5 Mbps	14.5 Mbps
Codec	H.264	H.264	H.264	H.264

Overall, iOS devices demonstrated superior metadata retention and consistency across formats and platforms. The choice of extraction tool also significantly impacted the results, where Metadata2go and ExifInfo outperformed ExifMeta. Android content, particularly video, showed limited metadata, which may affect its utility in forensic workflows. These findings underscore the importance of selecting both appropriate devices and robust tools when metadata integrity is critical.

Conclusion and Future Work

This study conducted a comparative evaluation of metadata completeness in image and video files generated by iOS and Android devices, with additional analysis of their behavior after uploading to cloud storage. The findings revealed that iOS devices consistently retained a richer set of metadata attributes, including timestamps, GPS coordinates and lens model information, thereby supporting stronger traceability and authenticity in digital forensics. In contrast, Android devices, particularly in video files, exhibited significant omissions in descriptive metadata such as device make, model, creation date and geolocation. These systemic gaps reduce the evidentiary value of Android media files and pose challenges for forensic practitioners tasked with source authentication and event reconstruction.

The study also evaluated three metadata extraction tools, identifying Metadata2go and ExifInfo as more reliable compared to ExifMeta, which demonstrated limited support for certain EXIF tag groups and struggled with extracting date and location information. These results underline the importance of tool diversity, cross-validation and platform-specific awareness in digital forensic workflows, as reliance on a single extraction tool or platform may lead to incomplete or misleading interpretations.

For future research, the dataset should be broadened to cover a wider range of smartphone models, operating system versions and recording conditions to strengthen the generalizability of the findings. Additionally, investigating how metadata degrades through processes such as file editing, compression and sharing via social media platforms would provide valuable insights into real-world challenges. Such work could inform the development of standardized forensic guidelines and best practices for preserving metadata integrity, ensuring that digital evidence remains accurate, reliable and admissible in investigative and legal contexts.

Acknowledgements: The authors would like to express their gratitude to the Faculty of Computer and Mathematical Sciences (FSKM) for providing the necessary facilities and support for this research. We also acknowledge the International Conference on Mathematical Sciences and Statistics (MIC3ST 2025) for the platform to present and refine the preliminary findings of this work.

Funding Statement: No funding.

Conflict of Interest Statement: The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the International Journal of Information System and Technology Management (JISTM)

Ethics Statement: This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.

Author Contribution Statement: All authors contributed significantly to the development of this manuscript. Raihana Md Saidi and Nurezzlin Natasha Ramli were responsible for the conceptualization, methodology, data curation and overall supervision of the study. They also handled data collection, analysis, and interpretation of results. Hajar Izzati Mohd Ghazalli and Fatin Nadhirah Zabani contributed to the literature review, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript prior to submission.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 42 (March 2026) PP. 423-436

References

Aneja, P., Bhatia, A., & Shankar, A. (2021). A Review of Secure Cloud Storage-Based on Cloud Computing. Advances in Intelligent Systems and Computing, 923–933. https://doi.org/10.1007/978-981-15-9927-9_88

Arizona, N. D., Muhammad Agung Nugroho, Syujak, A. R., Rizqi Kurniawan Saputra, & Istri Sulistyowati. (2024). Metadata Forensic Analysis as Support for Digital Investigation Process by Utilizing Metadata-Extractor. Journal of Intelligent Software Systems, 3(2), 27–27. https://doi.org/10.26798/jiss.v3i2.1503

Bennabhaktula, G. S., Alegre, E., Karastoyanova, D., & Azzopardi, G. (2022). Camera model identification based on forensic traces extracted from homogeneous patches. Expert Systems with Applications, 206, 117769. https://doi.org/10.1016/j.eswa.2022.117769

Bikash L. (2025). Development of an Indoor localization and positioning system in non-GPS environment using standalone smart phones and its implementation in construction site photo management application. Proceedings of Digital Frontiers in Buildings and Infrastructure International Conference Series, 13–23. https://submission.dfbi.org/index.php/dfbi/article/view/2520

Dai, H., Wang, Y., Kent, K. B., Zeng, L., & Xu, C. (2022). The State of the Art of Metadata Managements in Large-Scale Distributed File Systems — Scalability, Performance and Availability. IEEE Transactions on Parallel and Distributed Systems, 33(12), 3850–3869. https://doi.org/10.1109/tpds.2022.3170574

Dang-Nguyen, D.-T., Sjøen, V. V., Le, D.-H., Dao, T.-P., Tran, A.-D., & Tran, M.-T. (2023). Practical Analyses of How Common Social Media Platforms and Photo Storage Services Handle Uploaded Images. Lecture Notes in Computer Science, 164–176. https://doi.org/10.1007/978-3-031-27818-1_14

Fakiha, B. (2024). Unlocking Digital Evidence: Recent Challenges and Strategies in Mobile Device Forensic Analysis. Journal of Internet Services and Information Security, 14(2), 68–84. https://doi.org/10.58346/jisis.2024.i2.005

Faraz Hyder, M. F., Arshad, S., & Fatima, T. (2024). Toward social media forensics through development of iOS analyzers for evidence collection and analysis. Concurrency and Computation. https://doi.org/10.1002/cpe.8074

Gerhard Bissels. (2022). Metadata for digital collections. Journal of EAHIL, 18(4), 27–28. https://doi.org/10.32384/jeahil18547

Gupta, K., Damilola Oladimeji, Cihan Varol, Rasheed, A., & Narasimha Shahshidhar. (2023). A Comprehensive Survey on Artifact Recovery from Social Media Platforms: Approaches and Future Research Directions. Information, 14(12), 629–629. https://doi.org/10.3390/info14120629

Kalaimagal S., Madhumitha Seshaiah, S Harini, D Keerthi, & Aakash Udayakumar. (2024). Implementation of Multi-Format EXIF Metadata Extraction from Images. 300–305. https://doi.org/10.1109/icdcc62744.2024.10961287

Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W. B., Mansoor, K., & Rubab, S. (2021). Forensic Analysis of Social Networking Applications on an Android Smartphone. Wireless Communications and Mobile Computing, 2021, 1–36. https://doi.org/10.1155/2021/5567592

Mishra, H., Sihag, V., Choudhary, G., Dragoni, N., & You, I. (2022). Cloud Storage Client Forensic: Analysis of MEGA Cloud. Lecture Notes in Electrical Engineering, 1099–1110. https://doi.org/10.1007/978-981-19-5037-7_79

Mosha, N. F., & Ngulube, P. (2023). Metadata Standard for Continuous Preservation, Discovery, and Reuse of Research Data in Repositories by Higher Education

Institutions: A Systematic Review. Information, 14(8), 427. https://doi.org/10.3390/info14080427

Mühlbacher, J. (2024). Drag-n-Share : Streamlined File Sharing across Devices. Campus02.At. https://doi.org/10.58023/1127

Oh, J., Lee, S., & Hwang, H. (2022). Forensic Recovery of File System Metadata for Digital Forensic Investigation. IEEE Access, 10, 111591–111606. https://doi.org/10.1109/access.2022.3213030

Pacheco, A., Guardado, C., & Cristina, M. (2023). A metadata model for authenticity in digital archival descriptions. Archival Science, 23. https://doi.org/10.1007/s10502-023-09422-w

Riki Afrianto, Nusivera, S., & Haikal, H. (2025). Cloud Storage Ethics in Industrial Engineering: A Comparative Analysis of Microsoft OneDrive and SharePoint. Journal Mobile Technologies (JMS), 3(2), 49–55. https://doi.org/10.59431/jms.v3i2.633

Shaliyar, M., & Mustafa, K. (2022). Metadata Analysis of Web Images for Source Authentication in Online Social Media. Springer Proceedings in Mathematics & Statistics, 75–88. https://doi.org/10.1007/978-981-19-9307-7_7

Shreedhar, T., Panda, R., Podanev, S., & Bajpai, V. (2021). Evaluating QUIC Performance over Web, Cloud Storage and Video Workloads. IEEE Transactions on Network and Service Management, 1–1. https://doi.org/10.1109/tnsm.2021.3134562

Soni, N. (2025). Forensic Value of Exif Data: An Analytical Evaluation of Metadata Integrity across Image Transfer Methods. Perspectives in Legal and Forensic Sciences, 2(2), 10006–10006. https://doi.org/10.70322/plfs.2025.10006

Steinböck, M., Bleier, J., Rainer, M., Urban, T., Utz, C., & Lindorfer, M. (2024). Comparing Apples to Androids: Discovery, Retrieval, and Matching of iOS and Android Apps for Cross-Platform Analyses CCS CONCEPTS. https://doi.org/10.1145/3643991.3644896

Ulrich, H., Kock-Schoppenhauer, A.-K., Deppenwiese, N., Gött, R., Kern, J., Lablans, M., Majeed, R. W., Stöhr, M. R., Stausberg, J., Varghese, J., Dugas, M., & Ingenerf, J. (2022). Understanding the Nature of Metadata: Systematic Review. Journal of Medical Internet Research, 24(1), e25440. https://doi.org/10.2196/25440

Vayyala, R. (2025). Metadata Management and Its Role in Data Governance. Data Governance, DevSecOps, and Advancements in Modern Software, 47–72. https://doi.org/10.4018/979-8-3373-0365-9.ch003

Zheng, C., Shrivastava, A., & Owens, A. (2023). EXIF as Language: Learning Cross-Modal Associations Between Images and Camera Metadata. ArXiv.org. https://arxiv.org/abs/2301.04647