SCIEPublish

Article

Forensic Value of Exif Data: An Analytical Evaluation of Metadata Integrity across Image Transfer Methods

Nishchal Soni *

Department of Forensic Science, School of Bioengineering and Biosciences, Lovely Professional University, Phagwara 144005, India

* Corresponding author. E-mail: Nishchal.Soni@lpu.in (N.S.)

Received: 10 April 2025; Accepted: 9 June 2025; Available online: 18 June 2025

ABSTRACT: Exif metadata contained in digital photographs is an important forensic resource, offering authentic information like timestamps, geolocation, and device identifiers. The research assesses the integrity of Exif information on various methods of image transmission, such as USB, email, and messaging platforms like WhatsApp, Telegram, Signal, Instagram, Facebook Messenger, and Snapchat. With the controlled image dataset of Android, iOS phones, and the Flickr Creative Commons collection, we examined metadata preservation using forensic software (Magnet AXIOM, FTK, XRY, ExifTool). Document-based modes and direct transfers (USB, email) maintained all Exif fields and file hashes, providing forensic integrity. Chat/image-based transfers, fueled by compression, effectively remove metadata, changing the file integrity. These results emphasize the necessity of platform-aware evidence handling in order to preserve metadata integrity during digital forensic examinations.

Keywords: Digital forensics; Exif metadata; Image authentication; Metadata integrity; File hash verification

1. Introduction

Today, in the information age, where photographs are taken and shared with unprecedented freedom, metadata is a quiet yet potent witness. Perhaps the most valuable type of embedded data is the Exchangeable Image File Format (Exif)—a protocol that encodes all manner of information about a digital photo, including the date and time of shooting, camera brand and model, image resolution, GPS location, exposure parameters, and software applied in editing. Although frequently underestimated by non-professional users, Exif information is full of great potential for use in areas such as digital forensics, where the tiniest tip hidden in metadata can be the solution to a crime, confirmation of an alibi, or the revelation of digital forgery.

Originally specified by the Japan Electronic Industries Development Association (JEIDA), Exif has since been incorporated into nearly all consumer-level digital cameras and smartphones. This metadata is automatically embedded into image files, making it unnecessary to have to document it manually—a procedure that was routine in the days of analog photography. With the use of mobile phones and social media, photographs have not only become the central part of communication but also become indispensable proof in criminal and civil cases. As such, Exif information has evolved from a technical convenience to a forensic tool.

Over the past few years, cybercrime has risen exponentially. This concerning trend highlights the changing modus operandi adopted by cybercriminals, who use a wide range of advanced methods—including phishing, ransomware, Distributed Denial of Service (DDoS) attacks, identity theft, and specifically, remote access crimes [1,2]—to target vulnerabilities in computer systems. With computer forensic science, images are now not only being seen as pure visual images but also as vessels containing contextual information and trace evidence. For example, law enforcement units increasingly depend on metadata to build timelines, establish authenticity, and find individuals in space and time. Exif information has played a significant role in investigating acts of terrorism, cybercrime, stalking, fraud, and exploitation of children. However, although it holds forensic promise, the credibility of Exif data is compromised by a litany of problems—everything from platform-dependent metadata stripping to intentional modification through the use of anti-forensics.

https://doi.org/10.70322/plfs.2025.10006

Perhaps the most underappreciated threat to the integrity of Exif is not from a hacktivist but from routine user behavior—how pictures get moved around and passed around. Messaging apps such as WhatsApp [3], Signal, and social media sites such as Instagram, Facebook, and Snapchat use compression algorithms to minimize file sizes to enable faster transmission. This strips out or changes a lot of the Exif information in the process, making these files less forensic-worthy. Alternately, methods of sharing such as USB transfer, email attachments, or sending pictures as "documents" tend to leave the metadata intact. Knowing which image transfer processes preserve Exif information—and to what degree—is a critical issue for digital examiners.

Complicating matters further is the development of anti-forensic methods, whereby users intentionally alter or delete Exif metadata to obscure incriminating information. Free programs like ExifTool or commercial image manipulation programs enable users to manipulate metadata fields or delete them entirely. These alterations, however subtle, have severe consequences for the admissibility of evidence in courtrooms. Courts need not only data but guarantees regarding its authenticity, integrity, and provenance.

Based on these dynamics, it is crucial to perform a systematic and empirical analysis of the integrity of Exif data in prevalent image transfer mechanisms. Current literature is either centered on the forensic significance of metadata or on the operation of certain tools, but few integrated studies exist that analyze how Exif data handles when captured from varying smartphones and disseminated through different avenues.

This research intends to bridge that gap. Systematically taking pictures with a wide variety of smartphones (both iOS and Android), transferring them over various platforms and apps, and examining their metadata with forensic software such as Magnet AXIOM, XRY, and FTK, we plan to evaluate:

- Which Exif fields get lost or remain intact based on the transfer process.
- Whether some apps compress or alter metadata on a systematic basis.
- The consistency of Exif data across devices and operating systems.
- The feasibility of using Exif data as reliable forensic evidence under varying conditions.

Additionally, this study reflects on the broader implications of these findings for law enforcement, legal practitioners, and digital forensic professionals. As metadata becomes an increasingly contested area in cyber law and criminal justice, understanding its strengths and vulnerabilities is not just a technical necessity—it is a legal imperative.

In summary, though Exif data is very important for forensic purposes, its usefulness is dependent on the manner in which it is acquired, communicated, and examined. Through bringing illumination to the life cycle of Exif data and identifying where it can be contaminated, this research aims to deliver actionable knowledge to practitioners and researchers of digital forensics. By way of this research, we seek to elevate a superficial knowledge of image metadata into a solid, investigative toolset that can sustain high-stakes judgments in courtrooms and crime scenes both.

2. Literature Review

2.1. Prior Studies Utilizing Exif Data in Digital Forensics

The use of Exchangeable Image File Format (Exif) metadata in digital forensics has been extensively investigated, with many research papers emphasizing its central role in image authentication and analysis. Gangwar and Pathania [4] proposed a method of image tampering detection by investigating Exif metadata, thumbnail data, and compression signatures using available tools to determine indications of image tampering. Likewise, Sandoval Orozco et al. [5] studied anomalies in Exif metadata on mobile phones and found problems that may cause extraction failures and interoperability issues among forensic tools.

The application of machine learning methods in digital forensics has also received some attention. Nayerifard et al. [6] carried out a systematic literature review on machine learning in digital forensics and identified that image forensics has gained the most from machine learning methods, especially through the use of convolutional neural networks (CNNs). In addition, Bhagtani et al. [7] gave a summary of recent developments in media forensics, presenting techniques for detecting and measuring manipulations in digital images, videos, and audio.

The use of file system metadata in digital forensics has also been investigated. Buchholz and Spafford [8] explained how file system metadata can be used in forensic analysis to determine file access patterns and timelines. Patel and Sharma [9] also stressed the significance of metadata in digital forensic analysis, pointing out its use in detecting suspicious systems and reducing investigation time.

Within the context of social media forensics, metadata has been utilized to decipher digital evidence. Exif data was noted as the most important factor in verifying digital evidence and constructing events in litigation by a recent survey study.

2.2. Technical Background of Exif Metadata

Exif metadata is embedded information within image files that encompasses a variety of details, including:

- Timestamps: Date and time when the image was captured.
- Geolocation Data: GPS coordinates indicating where the photo was taken.
- Device Information: Make and model of the camera or smartphone used.

This metadata is automatically generated by the capture device and stored in the image file, offering a rich context for every photograph. Exif metadata has a standardized structure, enabling uniform storage and retrieval of this data on various devices and platforms. Nevertheless, according to Sandoval Orozco et al. [5], differences introduced by device manufacturers in the Exif specification may lead to errors during metadata extraction, thereby complicating forensic analysis.

In addition, the metadata extraction process should be carried out with care so that the original image file is not modified. Software such as Meta-Extractor has been created to extract metadata from files of different formats, including images, in a programmatic way so that the integrity of the digital evidence is preserved during the analysis.

2.3. Legal and Ethical Considerations

The application of Exif metadata in the context of the law has been significant, with Exif serving as a means to ensure the integrity and authenticity of digital evidence. That said, detailed metadata, such as geolocation data, poses a threat to privacy. Machado [10] discussed the security concerns and privacy issues associated with the use of Exif metadata, noting the possibility of unauthorized access to sensitive data embedded within image files.

In law, the ethical considerations of metadata have been explored, particularly in relation to the accidental disclosure of confidential data. Conner [11] underscored the requirement that lawyers take reasonable care in avoiding the unintentional passage of sensitive metadata, which may violate client confidentiality.

These points highlight the two-edged sword of Exif metadata: though it is a crucial tool in digital forensics and court cases, it also requires utmost care in handling in order to strike a balance between investigation value and ethical integrity.

3. Objectives

The prime aim of this study is to implement thorough research on Exchangeable Image File Format (Exif) metadata from the viewpoint of digital forensics. For the fulfillment of this overall goal, the study is based on the following precise objectives:

1. Examine Exif Metadata Retention: Find out which Exif fields (e.g., timestamps, location, device ID) are being kept or dropped when transferring images through USB, email, and applications such as WhatsApp, Telegram, Signal, Instagram, Facebook Messenger, and Snapchat.
2. Assess the Impact of Transfer Methods: Investigate how compression and platform-specific processing affect the integrity of Exif metadata and the consistency of file hashes, identifying forensically reliable transfer methods.
3. Compare Android and iOS Exif Structures: Examine platform-specific differences in Exif metadata generated by Android and iOS devices to ensure forensic applicability across operating systems.

By working progressively through these aims, the study hopes to enrich the knowledge database in digital forensics through insights that are capable of optimizing investigative processes as well as helping to develop relevant policies for utilizing metadata within court proceedings.

4. Methodology

This research adopts an empirical approach to analyze the preservation, modification, and removal of Exif metadata across various image transfer methods using a controlled environment. The methodology is divided into three key phases: test environment setup, image capture and transfer, and forensic analysis.

4.1. Test Environment

4.1.1. Devices Used

A diverse set of smartphones was selected to represent a range of manufacturers, operating systems, and camera capabilities. Each device was used to capture images with its stack camera application. The devices included are listed below (Table 1):

Table 1. Represent the devices used during the experiment with their OS and camera Specs.

Device	OS	Rear Camera Specs	Front Camera Specs
Samsung S24 FE	Android	50 MP, f/1.8 + 8 MP, f/2.2 + 12 MP, f/2.2	10 MP, f/2.4
POCO X2	Android	64 MP, f/1.9	20 MP
Samsung A21	Android	16 MP, f/1.8	13 MP
Motorola G7	Android	12 MP, f/2.0	8 MP
Redmi Note 7	Android	48 MP, f/1.8	13 MP
Redmi Note 8 Pro	Android	64 MP, f/1.9	20 MP
Redmi Note 5 Pro	Android	12 MP + 5 MP dual	20 MP
OnePlus Nord	Android	48 MP + 8 MP + 5 MP + 2 MP	32 MP + 8 MP
Realme 5	Android	12 MP + 8 MP + 2 MP + 2 MP	13 MP
RealMe C2	Android	13 MP + 2 MP	5 MP
iPhone 7	iOS	12 MP, f/1.8	7 MP, t/2.2
iPhone 12	iOS	Dual 12 MP, f/1.6 & f/2.4	12 MP, f/2.2

Each phone was reset to its factory settings before testing to eliminate the influence of third-party software. In addition to images captured directly using Android and iOS devices, a set of sample images was sourced from the Flickr Creative Commons dataset. These images contain preserved EXIF metadata and serve as standardized inputs to ensure consistency across devices and transfer methods. Each image from the dataset was subjected to all transfer methods assessed in this study to evaluate any variation in metadata integrity.

4.1.2. Forensic Tools Used

The following digital forensic tools were employed for metadata extraction and analysis:

- Magnet AXIOM—Comprehensive analysis suite capable of parsing image metadata and correlating evidence [12].
- XRY (MSAB)—Mobile data extraction tool for logical and physical data recovery, including media metadata [13].
- FTK (Forensic Toolkit)—A widely-used forensic tool for in-depth file analysis and Exif metadata extraction [14].
- ExifTool—Open-source command-line application for reading, writing, and editing Exif metadata [15].

4.2. Image Capture and Transfer

4.2.1. Image Capture Protocol

- Each device captured 10 unique images under similar lighting conditions (indoor daylight) and framing (same object/background) to maintain standardization.
- Images were captured at the device's stock camera app with its default settings.
- No editing or post-processing was applied before the transfer phase to ensure metadata integrity.

4.2.2. Transfer Methods

Each image was transferred using the following methods:

1. USB Cable Transfer
2. Email (as attachment)
3. Telegram
    - Chat mode (compressed)
    - Document mode (uncompressed)
4. Signal
    - Chat mode
    - Document mode
5. WhatsApp
    - Image mode (compressed)
    - Document mode (uncompressed)
6. Instagram
7. Facebook Messenger
8. Snapchat

4.2.3. Preservation of Hash Values

- MD5 and SHA-256 hash values were generated for all original images before transfer using HashMyFiles.
- Post-transfer images were compared against the original hashes to verify file integrity.
- This step allowed clear determination of whether files had been altered during the transfer process (e.g., compression, format change, metadata removal).

4.3. Analysis Process

4.3.1. Metadata Extraction

- All images were imported into FTK and Magnet AXIOM, where metadata was extracted and cataloged.
- Fields examined included: timestamp, geolocation, camera make/model, ISO, resolution, editing software, orientation, and thumbnail presence.
- ExifTool was used for command-line validation and batch metadata dumps.

4.3.2. Cross-Comparison

- Each transferred image was matched against its original version.
- Metadata presence or absence was documented for each Exif tag category.
- Comparative tables were created to show tag retention/loss based on transfer method and device.

4.3.3. Compression *vs.* Exif Removal Patterns

- Platforms like Instagram, Snapchat, and WhatsApp image mode showed evidence of compression.
- Compression effects were correlated with metadata stripping patterns:
    - Loss of geotags and timestamps
    - Removal of camera make/model
    - Thumbnail alterations
- Signal and Telegram (in document mode) retained full metadata, affirming their suitability for forensic workflows.

5. Results

The experiments were conducted on a controlled dataset—10 images captured under standardized conditions with multiple devices and transferred through various methods. In this section, we describe our technical findings related to Exif retention, the impact of transfer platforms, and integrity verification via hash analysis.

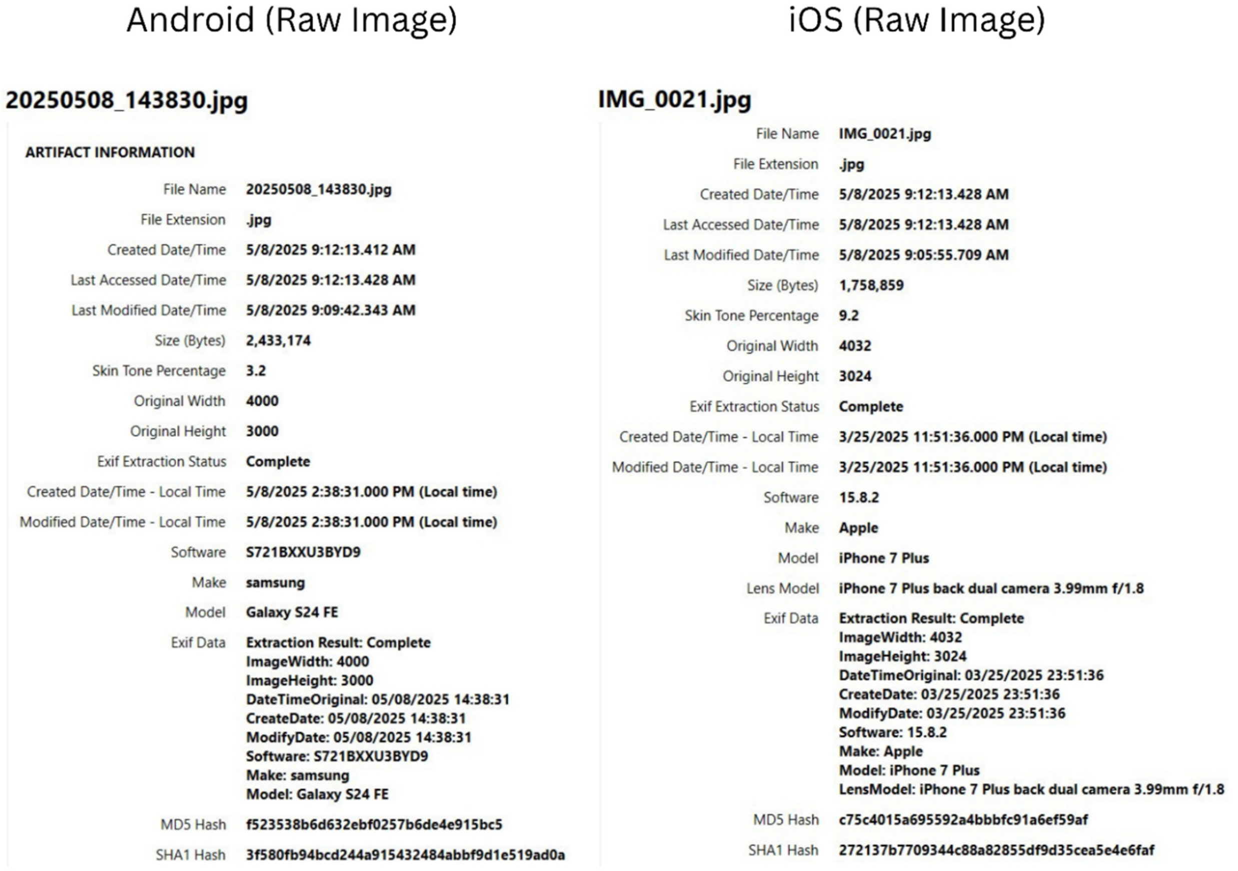
5.1. Comparison of Exif Metadata Structure: Android vs. iPhone

To assess platform-specific differences in metadata generation, we compared the Exif structures of two images—one captured using an Android device (Samsung Galaxy S24 FE) and the other using an iPhone (iPhone 7 Plus). Both devices embedded a largely consistent set of standard Exif fields, including timestamp (DateTimeOriginal, CreateDate, ModifyDate), image dimensions (ImageWidth, ImageHeight), device manufacturer (Make) and model (Model), and software version.

However, certain differences were observed:

- Lens Information: The iPhone image included a LensModel field specifying the exact lens configuration (e.g., focal length and aperture), whereas the Android counterpart did not populate this field. This suggests that iOS devices may embed more granular optical data by default.
- Software Tag Format: The Software field differed in format; iOS listed the iOS version number (e.g., 15.8.2), while the Android device included a firmware/build ID (e.g., S721BXXU3BYD9), reflecting platform-specific metadata conventions.

Other than the above, the overall Exif metadata structure and tag presence were consistent across both platforms, indicating that both Android and iOS devices comply with the standard Exif schema for core metadata fields relevant to forensic investigations (See Figure 1).



Android (Raw Image)

20250508_143830.jpg

ARTIFACT INFORMATION

File Name	20250508_143830.jpg
File Extension	.jpg
Created Date/Time	5/8/2025 9:12:13.412 AM
Last Accessed Date/Time	5/8/2025 9:12:13.428 AM
Last Modified Date/Time	5/8/2025 9:09:42.343 AM
Size (Bytes)	2,433,174
Skin Tone Percentage	3.2
Original Width	4000
Original Height	3000
Exif Extraction Status	Complete
Created Date/Time - Local Time	5/8/2025 2:38:31.000 PM (Local time)
Modified Date/Time - Local Time	5/8/2025 2:38:31.000 PM (Local time)
Software	S721BXXU3BYD9
Make	samsung
Model	Galaxy S24 FE
Exif Data	Extraction Result: Complete ImageWidth: 4000 ImageHeight: 3000 DateTimeOriginal: 05/08/2025 14:38:31 CreateDate: 05/08/2025 14:38:31 ModifyDate: 05/08/2025 14:38:31 Software: S721BXXU3BYD9 Make: samsung Model: Galaxy S24 FE
MD5 Hash	f523538b6d632ebf0257b6de4e915bc5
SHA1 Hash	3f580fb94bcd244a915432484abbf9d1e519ad0a

iOS (Raw Image)

IMG_0021.jpg

File Name	IMG_0021.jpg
File Extension	.jpg
Created Date/Time	5/8/2025 9:12:13.428 AM
Last Accessed Date/Time	5/8/2025 9:12:13.428 AM
Last Modified Date/Time	5/8/2025 9:05:55.709 AM
Size (Bytes)	1,758,859
Skin Tone Percentage	9.2
Original Width	4032
Original Height	3024
Exif Extraction Status	Complete
Created Date/Time - Local Time	3/25/2025 11:51:36.000 PM (Local time)
Modified Date/Time - Local Time	3/25/2025 11:51:36.000 PM (Local time)
Software	15.8.2
Make	Apple
Model	iPhone 7 Plus
Lens Model	iPhone 7 Plus back dual camera 3.99mm f/1.8
Exif Data	Extraction Result: Complete ImageWidth: 4032 ImageHeight: 3024 DateTimeOriginal: 03/25/2025 23:51:36 CreateDate: 03/25/2025 23:51:36 ModifyDate: 03/25/2025 23:51:36 Software: 15.8.2 Make: Apple Model: iPhone 7 Plus LensModel: iPhone 7 Plus back dual camera 3.99mm f/1.8
MD5 Hash	c75c4015a695592a4bbbfc91a6ef59af
SHA1 Hash	272137b7709344c88a82855df9d35cea5e4e6faf

Figure 1. Comparison of EXIF data extracted using Magnet AXIOM from images captured on Android and iOS devices.

5.2. Exif Retention Comparison Table

Our analysis focused on several key Exif fields: timestamp, geolocation (GPS coordinates), device make/model, resolution, and thumbnail data. Each transfer method was evaluated for its ability to preserve these fields. The table below summarizes our comparative findings based on the following image transfer methods: USB cable transfer, Email attachments, Telegram (document mode and chat mode), Signal (document mode and chat mode), WhatsApp (document mode and image mode), Instagram, Facebook Messenger, and Snapchat (See Table 2).

Table 2. Represents the results of experiments in multiple conditions.

Exif Field	USB	Email Attachments	Telegram (Doc)	Telegram (Chat)	Signal (Doc)	Signal (Chat)	WhatsAp p (Doc)	WhatsAp p (Image)	Instagram	Facebook Messenger	Snapchat
Timestamp	✓	✓	✓	X	✓	X	✓	X	X	X	X
Geolocation	✓	✓	✓	X	✓	X	✓	X	X	X	X
Device Make/ Model	✓	✓	✓	X	✓	X	✓	X	X	X	X
Resolution	✓	✓	✓	✓*	✓	✓*	✓	✓*	✓*	✓*	✓*
Editing Software	✓	✓	✓	X	✓	X	✓	X	X	X	X
Thumbnail Data	✓	✓	✓	X	✓	X	✓	X	X	X	X
% Fields Retained	100%	100%	100%	16.67%	100%	16.67%	100%	16.67%	16.67%	16.67%	16.67%

Notes: ✓ indicates full retention of the Exif field; X indicates the field is removed or not reliably recovered; ✓* indicates that the resolution field is retained but altered, with width and height differing from the original raw image due to resizing or compression; % Fields Retained calculated as the percentage of the six Exif fields (Timestamp, Geolocation, Device Make/Model, Resolution, Editing Software, Thumbnail Data) fully retained per transfer method.

Analysis

- USB & Email Attachments: Direct data transfer via USB cables and email attachments consistently retained the full suite of Exif fields with no alterations.

- Document Modes (Telegram, Signal, WhatsApp): These modes preserved all critical metadata fields (timestamp, geolocation, device info, editing software, *etc.*) with negligible compression-induced variations in resolution, ensuring forensic validity.
- Chat/Image Modes (Telegram, Signal, WhatsApp, Instagram, Facebook Messenger, Snapchat): When images are transferred as "images" (*i.e.*, in chat mode) or uploaded through social media, aggressive compression algorithms strip Exif metadata. Although a basic thumbnail or downscaled resolution value may remain, critical fields are missing, undermining the forensic potential.

This table represents a clear dichotomy in methods: document-oriented transfers maintain forensic integrity, while commonly used chat and social media transfers exhibit substantial metadata loss.

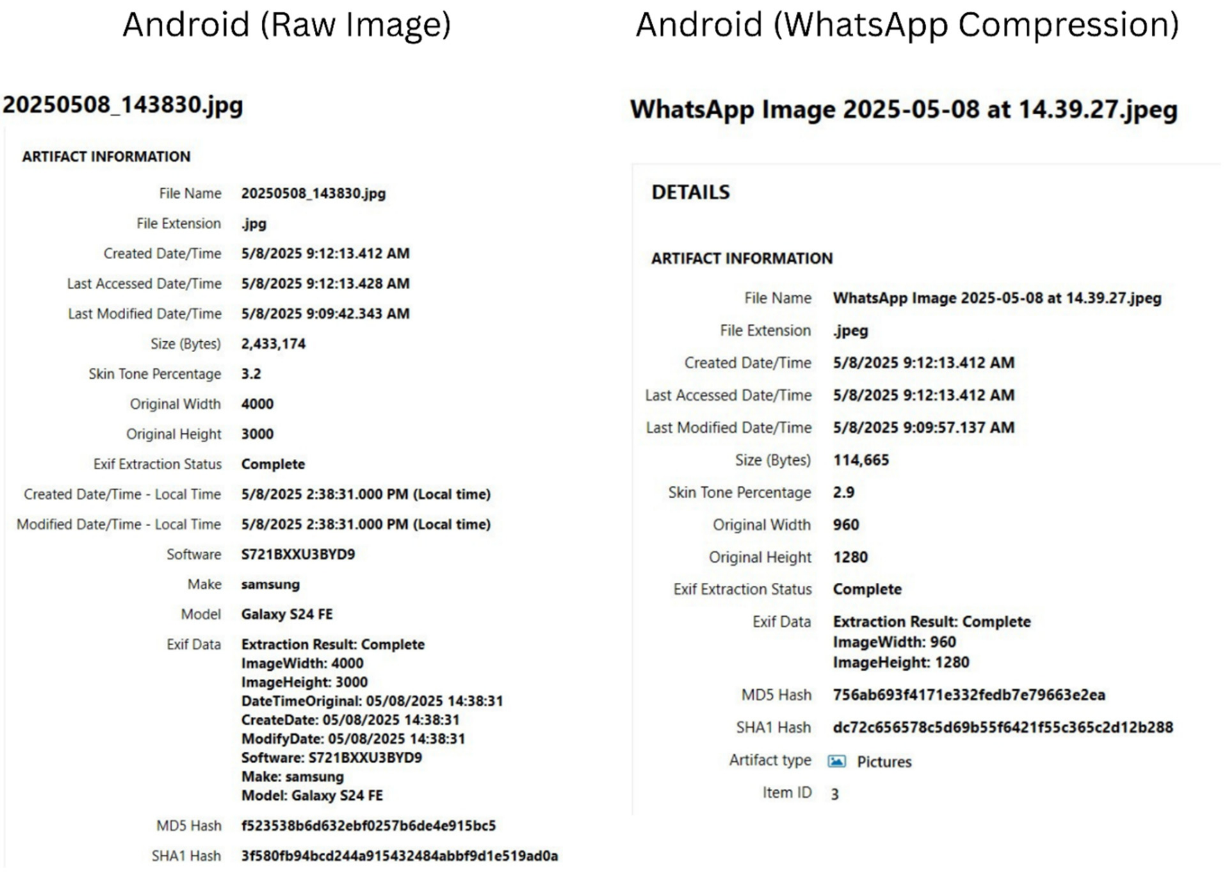
The analysis of EXIF data from the Flickr Creative Commons dataset images, after applying all transfer methods, revealed patterns consistent with those observed in the originally captured images. This consistency supports the generalizability of the findings and validates the reliability of the identified trends in metadata alteration and preservation across different platforms and devices.

5.3. Platform Impact Summary

A detailed review of the platforms revealed that system-level processing and intentional design choices affect metadata retention:

- Compression Algorithms:
  Social media platforms such as Instagram and Snapchat, as well as in-app chat transfers on WhatsApp, automatically compress images to decrease file size and optimize network efficiency (See Figures 2 and 3). As a result, there is evidence that the compression leads to:
  - Elimination of Geolocation Data: As shown in our extraction logs, metadata fields for GPS coordinates are completely absent after compression.
  - Alteration of Timestamps & Device Info: The original capture time and device identifiers are lost or replaced with generic values, complicating the task of verifying the image's origin.
- Privacy Filters:
  Many modern applications have incorporated privacy-preserving techniques to strip sensitive metadata. For instance, the use of privacy filters in Facebook Messenger and Snapchat was found to remove critical Exif fields even when the image quality was ostensibly maintained for display purposes.
- Platform Proof:
  Verification logs indicate that images transferred using WhatsApp's image mode display a dramatic file size reduction (up to 40–80% smaller), correlating with the complete loss of geolocation, device-specific details, and editing software information. In contrast, the same images transmitted using WhatsApp document mode retained nearly identical file sizes and full metadata. Similar patterns were observed on Telegram and Signal between their document versus chat modes, confirming that the retention is a deliberate design choice rather than a by-product of compression artifacts.

These findings are supported by our forensic extraction logs obtained via FTK and Magnet AXIOM. The logs clearly indicate that platforms prioritizing faster loading and bandwidth optimization systematically remove metadata components to protect user privacy, albeit at the cost of evidentiary value.



Android (Raw Image)

20250508_143830.jpg

ARTIFACT INFORMATION

File Name	**20250508_143830.jpg**
File Extension	**.jpg**
Created Date/Time	**5/8/2025 9:12:13.412 AM**
Last Accessed Date/Time	**5/8/2025 9:12:13.428 AM**
Last Modified Date/Time	**5/8/2025 9:09:42.343 AM**
Size (Bytes)	**2,433,174**
Skin Tone Percentage	**3.2**
Original Width	**4000**
Original Height	**3000**
Exif Extraction Status	**Complete**
Created Date/Time - Local Time	**5/8/2025 2:38:31.000 PM (Local time)**
Modified Date/Time - Local Time	**5/8/2025 2:38:31.000 PM (Local time)**
Software	**S721BXXU3BYD9**
Make	**samsung**
Model	**Galaxy S24 FE**
Exif Data	**Extraction Result: Complete** **ImageWidth: 4000** **ImageHeight: 3000** **DateTimeOriginal: 05/08/2025 14:38:31** **CreateDate: 05/08/2025 14:38:31** **ModifyDate: 05/08/2025 14:38:31** **Software: S721BXXU3BYD9** **Make: samsung** **Model: Galaxy S24 FE**
MD5 Hash	**f523538b6d632ebf0257b6de4e915bc5**
SHA1 Hash	**3f580fb94bcd244a915432484abbf9d1e519ad0a**

Android (WhatsApp Compression)

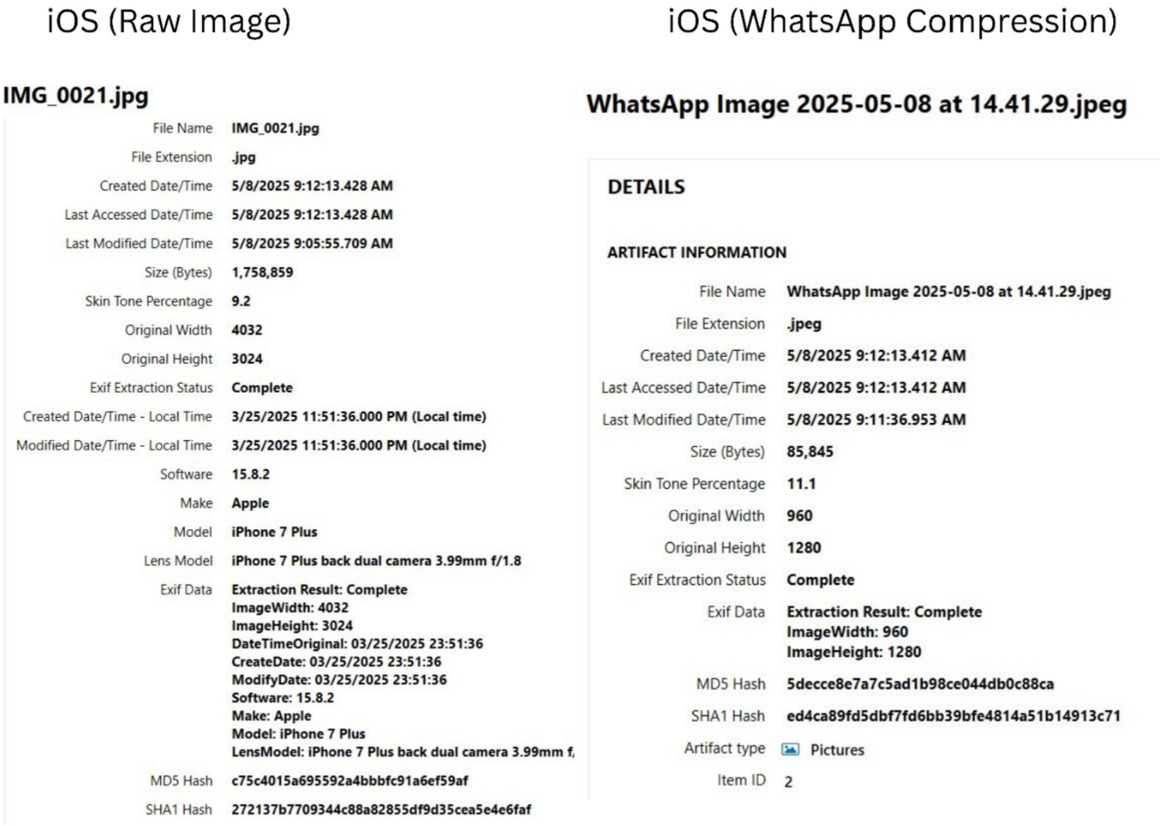
WhatsApp Image 2025-05-08 at 14.39.27.jpeg

DETAILS

ARTIFACT INFORMATION

File Name	**WhatsApp Image 2025-05-08 at 14.39.27.jpeg**
File Extension	**.jpeg**
Created Date/Time	**5/8/2025 9:12:13.412 AM**
Last Accessed Date/Time	**5/8/2025 9:12:13.412 AM**
Last Modified Date/Time	**5/8/2025 9:09:57.137 AM**
Size (Bytes)	**114,665**
Skin Tone Percentage	**2.9**
Original Width	**960**
Original Height	**1280**
Exif Extraction Status	**Complete**
Exif Data	**Extraction Result: Complete** **ImageWidth: 960** **ImageHeight: 1280**
MD5 Hash	**756ab693f4171e332fedb7e79663e2ea**
SHA1 Hash	**dc72c656578c5d69b55f6421f55c365c2d12b288**
Artifact type	Pictures
Item ID	3

Figure 2. Comparison of EXIF data extracted using Magnet AXIOM from an image captured on an Android device and the same image transferred via WhatsApp's in-chat method. The results show that all EXIF metadata was stripped due to compression, hash values were altered, and the creation, access, and modified timestamps were reset to reflect the time of transfer.



iOS (Raw Image)

IMG_0021.jpg

File Name	**IMG_0021.jpg**
File Extension	**.jpg**
Created Date/Time	**5/8/2025 9:12:13.428 AM**
Last Accessed Date/Time	**5/8/2025 9:12:13.428 AM**
Last Modified Date/Time	**5/8/2025 9:05:55.709 AM**
Size (Bytes)	**1,758,859**
Skin Tone Percentage	**9.2**
Original Width	**4032**
Original Height	**3024**
Exif Extraction Status	**Complete**
Created Date/Time - Local Time	**3/25/2025 11:51:36.000 PM (Local time)**
Modified Date/Time - Local Time	**3/25/2025 11:51:36.000 PM (Local time)**
Software	**15.8.2**
Make	**Apple**
Model	**iPhone 7 Plus**
Lens Model	**iPhone 7 Plus back dual camera 3.99mm f/1.8**
Exif Data	**Extraction Result: Complete** **ImageWidth: 4032** **ImageHeight: 3024** **DateTimeOriginal: 03/25/2025 23:51:36** **CreateDate: 03/25/2025 23:51:36** **ModifyDate: 03/25/2025 23:51:36** **Software: 15.8.2** **Make: Apple** **Model: iPhone 7 Plus** **LensModel: iPhone 7 Plus back dual camera 3.99mm f,**
MD5 Hash	**c75c4015a695592a4bbbfc91a6ef59af**
SHA1 Hash	**272137b7709344c88a82855df9d35cea5e4e6faf**

iOS (WhatsApp Compression)

WhatsApp Image 2025-05-08 at 14.41.29.jpeg

DETAILS

ARTIFACT INFORMATION

File Name	**WhatsApp Image 2025-05-08 at 14.41.29.jpeg**
File Extension	**.jpeg**
Created Date/Time	**5/8/2025 9:12:13.412 AM**
Last Accessed Date/Time	**5/8/2025 9:12:13.412 AM**
Last Modified Date/Time	**5/8/2025 9:11:36.953 AM**
Size (Bytes)	**85,845**
Skin Tone Percentage	**11.1**
Original Width	**960**
Original Height	**1280**
Exif Extraction Status	**Complete**
Exif Data	**Extraction Result: Complete** **ImageWidth: 960** **ImageHeight: 1280**
MD5 Hash	**5decce8e7a7c5ad1b98ce044db0c88ca**
SHA1 Hash	**ed4ca89fd5dbf7fd6bb39bfe4814a51b14913c71**
Artifact type	Pictures
Item ID	2

Figure 3. Comparison of EXIF data extracted using Magnet AXIOM from images captured on iOS and images transferred using WhatsApp in-chat image transfer method, shows that all the exif data is wiped because of the compression and the hash values are also changed, the creation, access, and modified date time are also new and related to when the image was transferred.

5.4. Hash Verification

To substantiate our findings on metadata alteration, we conducted integrity verification using MD5 and SHA-256 hash algorithms. For each image, hash values were calculated immediately after capture (serving as the baseline) and then again after each transfer method. Our observations were as follows.

5.4.1. USB & Email Transfers

- Findings:
  Images transferred via USB cables and email attachments maintained identical hash values compared to the original captures.
- Technical Explanation:
  These transfer methods perform a bit-for-bit copy of the original file. Since no compression, resizing, or re-encoding is involved, all Exif metadata remains intact, and the calculated hash values are completely consistent with the baseline.

5.4.2. Document Mode Transfers (Telegram, Signal, WhatsApp Document Mode)

- Findings:
  When images are sent as documents (*i.e.*, file attachments that preserve the original format and quality), the hash values remain identical to those of the original files.
- Technical Explanation:
  In document mode, these applications transmit the file without applying any compression or re-encoding. As a result, the files retain all original content—including Exif metadata—and yield precisely the same MD5 and SHA-256 checksums as the unaltered images. This confirms the integrity of the metadata and overall file structure, making document mode transfers ideal for forensic purposes.

5.4.3. Non-Document (Chat/Image) Mode Transfers (WhatsApp Image Mode, Instagram, Snapchat, Telegram Chat Mode, Signal Chat Mode, *etc.*)

- Findings:
  For all non-document or chat modes, the hash values of the transferred images are entirely different from the originals.
- Technical Explanation:
  In these modes, images undergo significant compression and re-encoding to optimize for faster transmission and reduced data usage. This processing not only reduces the file size but also removes or alters much of the Exif metadata. As the compression algorithms re-encode the image data, even minor alterations in pixel values lead to completely different hash values. Unlike document mode, the changes are not incremental; instead, the transformation results in a binary-level modification that completely invalidates the original checksums. For instance, an image originally hashed as "c75c4015a695592a4bbbfc91a6ef59af" in its unaltered state might result in an entirely different hash, such as "5decce8e7a7c5ad1b98ce044db0c88ca" after being processed by WhatsApp's chat mode, clearly indicating a complete re-encoding.

5.4.4. Summary of Observations

- Preservation of Hash Values:
  - USB & Email & Document Mode Transfers: Identical hash values confirm that these methods produce an exact duplicate of the original image file without any alteration, ensuring that all Exif metadata is preserved.
- Alteration of Hash Values:
  - Non-Document (Chat/Image) Mode Transfers: Drastic changes in the computed hash values demonstrate that these methods alter the image file—primarily through compression and re-encoding—thereby stripping or modifying the critical Exif metadata.

The hash verification process, therefore, serves as both a qualitative and quantitative measure of the integrity of transferred images. Methods that maintain the original hash (such as document mode transfers) guarantee that the forensic integrity remains uncompromised, whereas methods that alter the hash (chat/image modes) raise significant concerns regarding the retention of Exif metadata, thereby diminishing the evidentiary value of the images in forensic investigations.

6. Discussion

This research systematically analyzes the behavior of Exif metadata over different image transfer modes and finds a significant difference between document-based and chat/image-based protocols. Direct transfers (USB, email) and document modes (WhatsApp, Telegram, Signal) always maintain Exif fields—timestamps, geolocation, device identifiers—along with the same file hashes, which guarantee forensic integrity. By contrast, chat and image modes, as well as social media sites (Instagram, Snapchat, Facebook Messenger), utilize compression and re-encoding, which removes important metadata and changes file hashes, thereby reducing evidentiary value. Adding Flickr Creative Commons images confirmed these trends within standardized datasets, which further established the generalizability of the results.

Cross-platform comparison between Android and iOS showed slight platform-specific variations, like iOS integrating lens model information and different software tag formats, but both conformed to fundamental Exif requirements, validating their forensic usability. Graphs displaying metadata loss (e.g., WhatsApp chat mode) gave an intuitive display of compression's effect, making results more interpretable.

The research highlights the vulnerability of Exif data to loss due to standard user behavior, particularly on bandwidth-constrained platforms. This risk is exacerbated by the possibility of attacks by malicious actors who may take advantage of compression as an anti-forensic measure, intentionally hiding evidence without the use of specialized tools. Admissibility in court relies on the integrity of metadata, which requires strict acquisition procedures to maintain a chain of custody. Where privacy issues and anti-forensic threats are noted, technical and procedural considerations dominate here, supporting platform-aware handling of evidence in order to realize the greatest forensic value.

These results add value to digital forensics by providing investigators with actionable recommendations. Through the identification of transfer mechanisms that protect metadata, the research teaches investigators about best practices in evidence collection and emphasizes the necessity of developer cooperation to meet user experience and forensic requirements. Since digital images remain central to investigations, understanding how to preserve metadata is crucial for achieving justice.

7. Conclusions

This study validates the forensic value of Exif metadata and the deep effect of image transfer processes on its integrity. Controlled tests on Android, iOS devices, and Flickr Creative Commons images illustrated that transfers via USB, email, and document-based transmissions (WhatsApp, Telegram, Signal) retain Exif information—timestamps, location, device information—and retain file hashes, which guarantee evidentiary dependability. In contrast, chat/image-based transfers and social media sites, fueled by compression, remove metadata, generating modified hashes and eroding forensic value. These findings stress that an image's forensic value goes beyond Its visible content to the handling of the metadata after capture. Forensic practitioners need to embrace stringent acquisition habits in order to maintain metadata, while stakeholders such as developers and lawyers need to appreciate the implications of prevalent sharing practices. In a more digital world, the protection of metadata integrity is a foundation of efficient and equitable forensic investigations.

Author Contributions

Conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review & editing, visualization, supervision, and project administration: N.S.

Ethics Statement

Not applicable, as this study did not involve humans or animals.

Informed Consent Statement

Not applicable, as this study did not involve humans.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Funding

This research received no external funding.

Declaration of Competing Interest

I declare no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

References

1. Soni N, Kaur M, Aziz K. Decoding digital interactions: An extensive study of TeamViewer's forensic artifacts across Windows and Android platforms. *Forensic Sci. Int. Digit. Investig.* **2024**, *51*, 301838. doi:10.1016/j.fsidi.2024.301838.
2. Soni N, Kaur M, Bhardwaj V. A forensic analysis of AnyDesk remote access application by using various forensic tools and techniques. *Forensic Sci. Int. Digit. Investig.* **2024**, *48*, 301695. doi:10.1016/j.fsidi.2024.301695.
3. Soni N. Forensic analysis of WhatsApp: A review of techniques, challenges, and future directions. *J. Forensic Sci. Res.* **2024**, *8*, 019–024. doi:10.29328/journal.jfsr.1001059.
4. Gangwar A, Pathania S. Authentication of digital image using Exif metadata and decoding properties. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2018**, *3*, 1–7.
5. Sandoval Orozco AL, Arenas González DM, García Villalba LJ, Hernández-Castro J. Analysis of errors in Exif metadata on mobile devices. *Multimed. Tools Appl.* **2015**, *74*, 4735–4763. doi:10.1007/s11042-013-1837-7.
6. Nayerifard T, Amintoosi H, Ghaemi Bafghi A, Dehghantanha A. Machine learning in digital forensics: A systematic literature review. *arXiv* **2023**, arXiv:2306.04965.
7. Bhagtani K, Yadav AKS, Bartusiak ER, Xiang Z, Shao R, Baireddy S, et al. An overview of recent work in media forensics: Methods and threats. *arXiv* **2022**, arXiv:2204.12067.
8. Buchholz F, Spafford E. On the role of file system metadata in digital forensics. *Digit. Investig.* **2004**, *1*, 298–309. doi:10.1016/j.diin.2004.10.002.
9. Patel D, Sharma P. Meta data as a part of digital forensic investigation. *Int. J. Sci. Res. Dev.* **2015**, *3*, 812–814.
10. Machado J. EXIF Metadata—Privacy and Security. ResearchGate. Available online: https://www.researchgate.net/publication/365411189_EXIF_Metadata_-_Privacy_and_Security (accessed on 28 December 2024).
11. Conner KR. Ethical Issues Concerning Metadata. Holland & Knight Insights. Available online: https://www.hklaw.com/en/insights/publications/2006/03/ethical-issues-concerning-metadata (accessed on 28 December 2024).
12. Magnet Forensics. Magnet AXIOM [Computer Software]. Magnet Forensics. Available online: https://www.magnetforensics.com/products/magnet-axiom/ (accessed on 10 April 2025).
13. MSAB. XRY [Computer Software]. MSAB. Available online: https://www.msab.com/products/xry/ (accessed on 10 April 2025).
14. Exterro. Forensic Toolkit (FTK) 8.0.0 [Computer Software]. Exterro. Available online: https://www.exterro.com/ftk-product-downloads/forensic-toolkit-ftk-8-0-0 (accessed on 10 April 2025).
15. Harvey P. ExifTool (Version 12.50) [Computer Software]. Available online: https://exiftool.org/ (accessed on 10 April 2025).