(2025), 3 (7): 216-219 **Scientica** 3021-8209

Jurnal Ilmiah Sain dan Teknologi

ANALISIS FORENSIK METADATA EXIF PADA CITRA DIGITAL SEBAGAI POTENSI CELAH KEAMANAN PRIVASI PENGGUNA

Fairuz Fadlurrahman [1], Hendra Setiawan [2]
[1] Universitas Jenderal Achmad Yani, Indonesia
*e-mail: fairuzfadlurrahman@gmail.com

Abstract
User data privacy in the digital realm is frequently overlooked, particularly in the massive activity of digital image exchange on social media. By default, every photo taken using a smartphone camera stores Exchangeable Image File Format (EXIF) metadata containing technical information and the geographical location of the image capture (Geotagging). This study aims to analyze the potential for privacy data leakage through EXIF metadata and test the effectiveness of instant messaging application compression mechanisms in removing these digital footprints. The research method employs a simple digital forensics approach by comparing the metadata structure between original images (raw) from a Samsung Galaxy M15 5G smartphone camera and images that have been transmitted through the WhatsApp application. Research findings indicate that original images expose sensitive data in the form of GPS coordinate points (Latitude and Longitude) with high accuracy, whereas images resulting from WhatsApp transmission have undergone an automatic sanitization process, fully deleting location data. This study concludes that the practice of uploading original photos without metadata editing poses a physical security risk to users; therefore, preventive mitigation steps such as disabling the location tagging feature in camera settings are highly recommended.

Article History
Received: 4 Desember 2025
Reviewed: 7 Desember 2025
Published: 8 Desember 2025

Key Words
Digital Forensics, EXIF Metadata, Geotagging, Privacy Security, OSINT.

Abstrak
Privasi data pengguna dalam ranah digital sering kali terabaikan, terutama dalam aktivitas pertukaran citra digital yang masif di media sosial. Secara standar, setiap foto yang diambil menggunakan kamera ponsel pintar menyimpan metadata *Exchangeable Image File Format* (EXIF) yang memuat informasi teknis serta lokasi geografis pengambilan gambar (*Geotagging*). Penelitian ini bertujuan untuk menganalisis potensi kebocoran data privasi melalui metadata EXIF dan menguji efektivitas mekanisme kompresi aplikasi pesan instan dalam menghapus jejak digital tersebut. Metode penelitian menerapkan pendekatan forensik digital sederhana dengan membandingkan struktur metadata antara citra asli (*raw*) dari kamera ponsel Samsung Galaxy M15 5G dengan citra yang telah ditransmisikan melalui aplikasi WhatsApp. Temuan penelitian menunjukkan bahwa citra asli mengekspos data sensitif berupa titik koordinat GPS (Lintang dan Bujur) dengan akurasi tinggi, sedangkan citra hasil transmisi WhatsApp telah mengalami proses *sanitization* otomatis sehingga data lokasi terhapus sepenuhnya. Penelitian ini menyimpulkan bahwa praktik mengunggah foto asli tanpa penyuntingan metadata menimbulkan risiko keamanan fisik bagi pengguna, sehingga langkah mitigasi preventif seperti menonaktifkan fitur penanda lokasi pada pengaturan kamera sangat disarankan.

Sejarah Artikel
Received: 4 Desember 2025
Reviewed: 7 Desember 2025
Published: 8 Desember 2025

Kata Kunci
Digital Forensics, EXIF Metadata, Geotagging, Keamanan Privasi, OSINT.

PENDAHULUAN

Perkembangan teknologi fotografi pada telepon pintar (smartphone) telah mengubah paradigma dokumentasi masyarakat modern, di mana setiap momen dapat diabadikan dan dibagikan secara instan ke jejaring internet. Namun, kemudahan berbagi citra digital ini membawa implikasi serius terhadap keamanan privasi yang sering kali tidak disadari oleh pengguna awam. Di balik tampilan visual sebuah foto, terdapat lapisan data tersembunyi yang disebut metadata Exchangeable Image File Format (EXIF). Metadata ini awalnya

dikembangkan oleh Japan Electronic Industries Development Association (JEIDA) untuk menyimpan informasi teknis seperti jenis kamera, waktu pengambilan, bukaan lensa (aperture), dan sensitivitas ISO guna memudahkan manajemen aset digital (Pratama, 2019).

Permasalahan muncul ketika fitur Global Positioning System (GPS) pada perangkat seluler terintegrasi dengan modul kamera. Secara otomatis, metadata EXIF kini merekam koordinat geografis (Lintang dan Bujur) di lokasi pengambilan gambar. Data ini bersifat persisten, artinya tetap melekat pada file foto meskipun nama file telah diubah berkali-kali. Jika informasi ini diakses oleh pihak yang tidak berwenang, data tersebut dapat dimanfaatkan untuk melacak keberadaan fisik pengguna secara real-time atau memprofilkan pola aktivitas harian target, sebuah praktik yang dikenal dalam dunia keamanan siber sebagai pengumpulan Open Source Intelligence (OSINT) (Kurniawan, 2020).

Kesenjangan keamanan (security gap) terjadi karena kurangnya pemahaman pengguna mengenai sifat data digital. Banyak pengguna beranggapan bahwa privasi mereka terjaga selama tidak menampilkan wajah atau identitas tertulis dalam foto. Padahal, jejak digital dalam metadata sering kali lebih berbahaya karena memberikan bukti forensik lokasi yang akurat. Meskipun beberapa platform media sosial besar telah menerapkan mekanisme penghapusan metadata otomatis, masih banyak wadah pertukaran data lain seperti email, forum diskusi, atau layanan penyimpanan awan (cloud storage) yang mempertahankan keaslian file beserta metadatanya.

METODE

Penelitian ini menggunakan metode analisis forensik digital dengan pendekatan komparatif deskriptif. Objek penelitian difokuskan pada dua sampel citra digital yang identik secara visual namun memiliki riwayat transmisi yang berbeda. Sampel A merupakan citra asli (original) yang diambil langsung menggunakan kamera ponsel pintar berbasis Android dengan fitur penanda lokasi (Geotagging) dalam kondisi aktif. Sampel B merupakan citra yang sama (replikasi dari Sampel A) yang telah melalui proses transmisi (unggah dan unduh) menggunakan aplikasi pesan instan WhatsApp Messenger versi terbaru.

Instrumen penelitian terdiri dari perangkat keras dan perangkat lunak. Perangkat keras yang digunakan adalah satu unit ponsel pintar Samsung Galaxy M15 5G yang menjalankan sistem operasi Android 14 sebagai alat akuisisi citra. Perangkat lunak yang digunakan meliputi aplikasi WhatsApp sebagai media kompresi dan tools analisis metadata berbasis web (EXIF Viewer) yang berfungsi untuk mengekstraksi struktur data header pada file gambar. Penggunaan tools berbasis web dipilih untuk menyimulasikan aksesibilitas yang mudah bagi pengguna umum atau pelaku kejahatan siber (threat actor).

Prosedur pengumpulan dan analisis data dilakukan melalui tiga tahapan sistematis. Tahap pertama adalah akuisisi data, yaitu pengambilan foto sampel di lokasi terbuka dengan memastikan koneksi GPS stabil agar koordinat terekam sempurna. Tahap kedua adalah transmisi data, di mana citra asli dikirimkan ke perangkat lain melalui WhatsApp untuk mendapatkan sampel pembanding yang terkompresi. Tahap ketiga adalah ekstraksi dan komparasi, di mana kedua sampel diunggah ke EXIF Viewer untuk membandingkan parameter kunci seperti Model Perangkat, Waktu Pengambilan, dan Koordinat GPS. Data yang diperoleh kemudian ditabulasikan untuk menentukan tingkat risiko keamanan privasi pada masing-masing sampel.

HASIL DAN PEMBAHASAN

Bagian ini memaparkan temuan data hasil ekstraksi forensik terhadap metadata citra digital serta analisis mendalam mengenai implikasi keamanan privasi yang ditimbulkan. Pengujian dilakukan dengan membandingkan parameter metadata yang muncul pada EXIF Viewer antara citra asli dan citra hasil transmisi.

Hasil

Proses analisis diawali dengan pengunggahan Sampel A (Citra Asli) ke dalam perangkat lunak pembaca metadata. Berdasarkan hasil pemindaian, sistem berhasil membaca dan menampilkan struktur data EXIF yang sangat lengkap. Informasi yang terekam mencakup data perangkat keras seperti merek dan model ponsel, versi perangkat lunak sistem operasi, hingga data teknis fotografi seperti waktu pencahayaan (exposure time) dan bukaan lensa. Temuan yang paling signifikan adalah keberadaan tag GPS yang masih utuh. Data koordinat Lintang (Latitude) dan Bujur (Longitude) terekam hingga enam angka di belakang koma, yang menandakan tingkat akurasi presisi tinggi. Selain itu, data waktu pengambilan gambar (Date Time Original) juga terekam hingga satuan detik, memberikan kronologi waktu yang tepat kapan foto tersebut diambil.

Sebaliknya, pada pengujian terhadap Sampel B (Citra via WhatsApp), ditemukan perbedaan struktur data yang drastis. Sistem analisis menampilkan status bahwa tidak ada data EXIF yang ditemukan atau sebagian besar tag metadata telah dihapus (stripped). Informasi mengenai jenis perangkat, waktu pengambilan, dan yang terpenting data lokasi (GPS), tidak lagi muncul dalam hasil ekstraksi. Perbandingan rinci parameter metadata antara kedua sampel disajikan dalam Tabel 1.

Tabel 1. Perbandingan Informasi EXIF Citra Asli dan Citra Hasil Kompresi

Parameter Metadata	Citra A (original kamera)	Citra B (via Whatsapp	keterangan
Model perangkat	Samsung galaxy M15 5G	-	Data Perangkat Bocor
Perangkat lunak	Android 14	WhatsApp	Jejak Aplikasi Terlihat
Waktu Pengambilan	2025:12:01	-	Waktu Presisi Hilang
GPS Latitude	-6.887147	-	Lokasi Bocor
GPS Longitude	107.526535	-	Lokasi Bocor
Aperture	f/1.8	-	Data Teknis Hilang

Pembahasan

Data yang tersaji pada Tabel 1 memperlihatkan fakta yang cukup mengkhawatirkan mengenai keamanan privasi pada perangkat mobile modern. Pada Sampel A (Citra Asli), terekamnya koordinat GPS dengan presisi tinggi pada perangkat Samsung Galaxy M15 5G menunjukkan bahwa fitur geotagging bekerja secara otomatis di latar belakang tanpa notifikasi yang jelas kepada pengguna. Ketika koordinat tersebut diuji coba ke dalam peta digital, titik lokasi yang muncul sangat akurat, bahkan bisa menunjukkan posisi spesifik sebuah rumah. Bagi seorang ahli IT atau pelaku kejahatan siber, data ini adalah emas dalam pengumpulan informasi intelijen (OSINT) karena memvalidasi keberadaan fisik target pada waktu tertentu.

Sebaliknya, pada Sampel B, hilangnya seluruh metadata setelah dikirim via WhatsApp membuktikan bahwa mekanisme kompresi pada aplikasi tersebut secara tidak sengaja berfungsi sebagai fitur keamanan. Algoritma WhatsApp menghapus data non-visual (seperti EXIF) semata-mata untuk mengecilkan ukuran file agar pengiriman lebih cepat dan hemat kuota. Efek samping positifnya, privasi pengguna jadi terlindungi. Ini menjelaskan mengapa foto yang viral di media sosial sering kali sulit dilacak lokasi aslinya secara forensik—karena jejak digitalnya sudah dicuci oleh sistem aplikasi.

Namun, ada satu celah logika yang sering luput dari perhatian pengguna. Keamanan pada Sampel B ini bergantung penuh pada cara pengguna mengirim file. Jika pengguna mengirim

foto tersebut menggunakan fitur Kirim Dokumen (agar gambar tidak pecah), maka WhatsApp tidak akan melakukan kompresi. Akibatnya, metadata EXIF (termasuk lokasi GPS) akan tetap utuh sampai ke penerima. Artinya, rasa aman saat menggunakan aplikasi pesan instan sebenarnya bersifat semu dan sangat bergantung pada kebiasaan teknis penggunanya.

Oleh karena itu, mengandalkan aplikasi pihak ketiga untuk menjaga privasi bukanlah solusi yang tepat. Pertahanan terbaik adalah memutus akses data dari sumbernya. Jika pengguna mematikan izin lokasi (location permission) pada pengaturan kamera Samsung Galaxy M15 5G mereka, maka foto yang dihasilkan akan bersih dari data pelacakan sejak awal, tidak peduli lewat media apa foto tersebut disebarkan nantinya.

SIMPULAN

Hasil analisis forensik pada penelitian ini menegaskan bahwa citra digital mentah yang diambil langsung dari kamera Samsung Galaxy M15 5G mengandung risiko keamanan privasi yang serius. Metadata EXIF pada foto asli terbukti menyimpan koordinat GPS presisi yang dapat dimanfaatkan untuk pelacakan fisik. Di sisi lain, citra yang telah melalui proses transmisi gambar via WhatsApp terbukti aman dari kebocoran lokasi karena adanya mekanisme penghapusan metadata otomatis. Kendati demikian, pengguna tidak disarankan untuk bergantung sepenuhnya pada fitur keamanan aplikasi, mengingat celah kesalahan manusia (human error) saat memilih metode pengiriman file masih mungkin terjadi. Langkah mitigasi paling efektif adalah mematikan fitur penanda lokasi (geotagging) pada pengaturan kamera ponsel untuk mencegah perekaman data sensitif sejak awal pengambilan gambar.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Hendra Setiawan, S.S., M.Pd., selaku Dosen Pengampu mata kuliah Bahasa Indonesia yang telah memberikan bimbingan dan arahan dalam penyusunan struktur artikel ilmiah ini.

DAFTAR PUSTAKA

Kurniawan, A. (2020). Forensik Digital: Teori dan Praktik Penanganan Bukti Elektronik. Yogyakarta: Penerbit Andi.

Pratama, I. P. A. E. (2019). Handbook Keamanan Jaringan Komputer dan Sistem Informasi. Bandung: Informatika.

Stallings, W. (2018). Cryptography and Network Security: Principles and Practice (7th Ed.). Boston, MA: Pearson Education.

Wijaya, R., & Handoko, L. (2021). Analisis Metadata EXIF Gambar Sebagai Barang Bukti Digital Menggunakan Metode NIST. Jurnal Ilmiah Informatika dan Komputer, 25(2), 112-120.