JUPITER
Teknologi Informatika & Komputer
Vol. 6 No. 2 Agustus 2025
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187

ANALISIS METADATA EXIFTOOL DAN FRAMEWORK NIST UNTUK DETEKSI MANIPULASI CITRA

Nathanael Christian Perkasa Trisuwita [1,*], Ryan Putranda Kristianto[1]

[1]Teknik Informatika, Universitas Katolik Darma Cendika, nathanael.christian@student.ukdc.ac.id, ryan@ukdc.ac.id

ABSTRAK

Kebocoran informasi perusahaan sering kali disebabkan oleh penyebaran data melalui media digital, termasuk gambar yang tampak biasa namun menyimpan informasi penting di dalam metadata-nya. Penelitian ini bertujuan untuk menganalisis metadata gambar digital guna mendeteksi indikasi manipulasi yang dapat menjadi petunjuk atas kebocoran informasi perusahaan. Metode yang digunakan adalah studi kasus dengan pendekatan kualitatif melalui pengumpulan sampel gambar, analisis metadata menggunakan perangkat lunak ExifTool, dan interpretasi hasil temuan. Hasil penelitian menunjukkan bahwa metadata gambar dapat mengungkap waktu, lokasi, perangkat yang digunakan, serta riwayat pengeditan gambar yang berpotensi menunjukkan aktivitas manipulatif. Temuan ini membuktikan bahwa metadata merupakan elemen krusial dalam investigasi kebocoran informasi, dan analisis metadata dapat membantu mengidentifikasi sumber serta proses penyebaran gambar manipulatif. Selain itu, penerapan kerangka kerja NIST memberikan struktur sistematis yang dapat dipertanggungjawabkan dalam proses forensik digital. Penelitian ini diharapkan dapat meningkatkan kesadaran perusahaan terhadap pentingnya pengamanan data digital, khususnya metadata gambar, dan mendorong penggunaan alat forensik metadata secara luas dalam praktik keamanan informasi modern.

Kata Kunci: ExifTool, Gambar Digital, Kebocoran Informasi, Metadata, Manipulasi

ABSTRACT

Corporate information leaks are often caused by the distribution of data through digital media, including images that appear ordinary but contain critical information within their metadata. This study aims to analyze digital image metadata to detect signs of manipulation that may indicate corporate information leaks. The method used is a case study with a qualitative approach involving image sample collection, metadata analysis using ExifTool software, and interpretation of findings. The results show that image metadata can reveal the time, location, device used, and editing history of images, all of which may indicate manipulative activity. These findings prove that metadata is a crucial element in investigating information leaks, and metadata analysis can help identify the source and process of manipulated image dissemination. Additionally, the use of the NIST framework provides a systematic and accountable structure for conducting digital forensic investigations. This study is expected to raise corporate awareness of the importance of securing digital data, particularly image metadata, and to encourage the adoption of metadata forensic tools in modern information security practices..

Keywords: *Digital Image, ExifTool, Information Leak, Metadata, Manipulation*

PENDAHULUAN

Dalam era digital saat ini, gambar digital tidak hanya berfungsi sebagai media visual, tetapi juga menyimpan informasi tersembunyi yang dikenal sebagai metadata. Metadata ini mencakup data seperti waktu pembuatan, lokasi geografis, perangkat yang digunakan, dan informasi teknis lainnya yang dapat memberikan konteks penting dalam

berbagai investigasi digital. Dalam konteks kebocoran informasi perusahaan, metadata gambar dapat menjadi sumber informasi awal yang penting untuk menelusuri pelaku, metode kebocoran, serta kronologi kejadian (Fransiskus, 2024; Sulistyo et al., 2020).

Seiring meningkatnya jumlah insiden kebocoran data, muncul kebutuhan akan pendekatan investigasi digital yang tidak hanya akurat, tetapi juga dapat dipertanggungjawabkan secara metodologis. Analisis metadata gambar digital menawarkan pendekatan yang dapat membantu dalam mengungkap jejak digital yang ditinggalkan oleh pelaku, terutama dalam kasus di mana gambar digunakan sebagai media penyebaran informasi rahasia (Apriliani et al., 2020; Satria et al., 2021). Metadata juga dapat membuktikan adanya manipulasi berdasarkan waktu pengeditan, jenis perangkat lunak, serta resolusi file (Syafar et al., 2023).

Salah satu kerangka kerja yang umum digunakan dalam praktik forensik digital adalah framework dari National Institute of Standards and Technology (NIST), yang terdiri dari empat tahap: collection, examination, analysis, dan reporting. Keunggulan pendekatan ini terletak pada standarisasi dan kemampuannya untuk digunakan dalam beragam jenis bukti digital (Afandi et al., 2024; Firdonsyah & Wijayanto, 2022; Khairunnisak et al., 2020). Kerangka kerja NIST sangat membantu memastikan proses akuisisi data dilakukan tanpa mengubah struktur file asli, serta memungkinkan analisis terhadap pola atau anomali yang tidak wajar (Fajar et al., 2024; Mualfah & Ramadhan, 2021).

Penelitian sebelumnya menunjukkan bahwa perangkat lunak seperti ExifTool dapat digunakan secara efisien untuk mengekstrak metadata yang tersembunyi, sehingga dapat mengidentifikasi indikasi penyuntingan (Apriliani et al., 2020; Syafar et al., 2023). Namun, sebagian besar penelitian masih terbatas pada file gambar berformat standar seperti JPEG, tanpa mengeksplorasi potensi forensik dari file manipulatif dalam format non-standar seperti CDR (CorelDRAW), PSD (Photoshop), atau format berbasis ZIP lainnya. Selain itu, belum banyak studi yang menggabungkan analisis metadata dengan penerapan kerangka kerja NIST secara terpadu untuk mendeteksi manipulasi citra digital dalam konteks kebocoran informasi.

Oleh karena itu, penelitian ini berfokus pada analisis metadata lintas format menggunakan ExifTool, yang disusun secara metodologis berdasarkan kerangka kerja forensik digital NIST, guna mengeksplorasi indikasi manipulasi gambar digital sebagai bagian dari upaya investigasi awal terhadap kebocoran informasi.

TINJAUAN PUSTAKA

1. Metadata

   Metadata merupakan informasi yang menyertai file digital, seperti tanggal pembuatan, lokasi, atau perangkat yang digunakan. Informasi ini sangat penting dalam proses forensik digital untuk melacak asal file serta kronologi aktivitas digital (Fransiskus, 2024; Sulistyo et al., 2020). Metadata memungkinkan pelacakan terhadap file yang mengalami perubahan, terutama pada kasus penyebaran informasi yang dimanipulasi (Apriliani et al., 2020; Syafar et al., 2023).

2. *EXIF (Exchangeable Image File Format)*

   EXIF adalah format metadata yang umum tertanam dalam file gambar digital seperti JPEG. EXIF berisi atribut seperti waktu pengambilan gambar, nama perangkat, pengaturan kamera, serta informasi lokasi (Apriliani et al., 2020; Satria et al., 2021).

Informasi ini berguna untuk mengidentifikasi apakah gambar telah dimanipulasi dan software apa yang digunakan dalam proses tersebut (Jaya Syafar et al., 2023).

3. Kerangka Kerja Forensik NIST

   NIST (National Institute of Standards and Technology) menawarkan pendekatan sistematis dalam forensik digital melalui empat tahapan: collection, examination, analysis, dan reporting (Firdonsyah & Wijayanto, 2022; Khairunnisak et al., 2020). Pendekatan ini memastikan validitas dan keutuhan bukti digital tetap terjaga selama proses investigasi. (Afandi et al., 2024) menggunakan metode ini untuk mendeteksi manipulasi file dokumen, sedangkan (Fajar et al., 2024) membuktikan efektivitasnya dalam mendeteksi foto palsu melalui kombinasi clone detection dan metadata analysis.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan studi kasus dengan menerapkan prosedur forensik digital yang merujuk pada kerangka kerja dari *National Institute of Standards and Technology* (NIST). Proses analisis metadata dilakukan melalui empat tahapan utama yang digambarkan dalam flowchart, yaitu *collection*, *examination*, *analysis*, dan *reporting*. Pendekatan ini dipilih karena memberikan struktur kerja yang sistematis dan dapat dipertanggungjawabkan secara metodologis dalam proses investigasi terhadap objek digital.

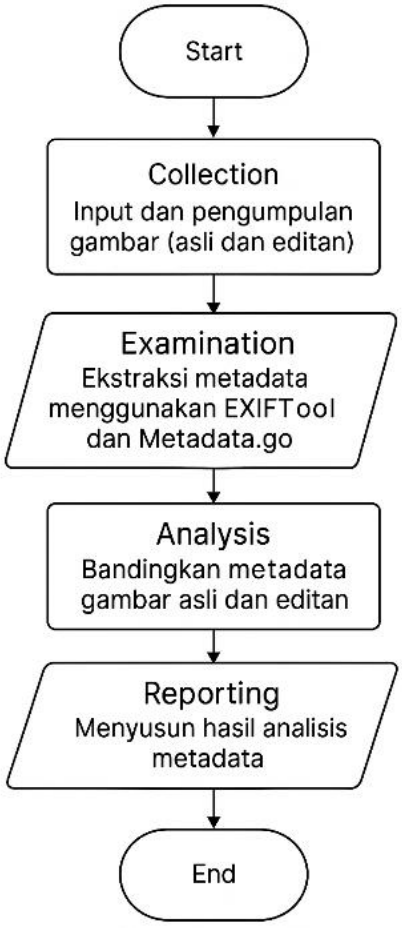
Tahapan pertama adalah *collection*, yaitu proses pengumpulan file gambar digital yang akan dianalisis. Gambar yang digunakan terdiri dari dua jenis: gambar asli dan gambar yang telah dimanipulasi menggunakan perangkat lunak pengolah gambar. Gambar asli dibuat menggunakan Canva dan diekspor dalam format *JPEG*, sedangkan gambar hasil manipulasi diedit menggunakan *CorelDRAW* dan disimpan dalam format *CDR*. Pemilihan dua jenis format ini dilakukan secara sengaja untuk menguji keberhasilan analisis metadata lintas format. *JPEG* dipilih karena merupakan format gambar digital standar yang menyimpan metadata *EXIF* secara lengkap, sementara *CDR* merupakan format grafis vektor yang memiliki struktur metadata berbeda dan tidak selalu kompatibel dengan standar *EXIF*. Dengan demikian, kombinasi ini memberikan tantangan yang lebih kompleks dan relevan dalam konteks forensik metadata. Seluruh proses pengumpulan dilakukan dalam lingkungan laboratorium forensik digital berbasis sistem operasi Windows, dengan perangkat lunak forensik sumber terbuka untuk memastikan kendali terhadap lingkungan eksperimen.

Tahapan kedua adalah *examination*, yaitu proses ekstraksi metadata dari masing-masing file gambar. Pada tahap ini digunakan perangkat lunak **ExifTool versi 13.29**, yang dikenal memiliki kemampuan membaca atribut metadata secara menyeluruh tanpa mengubah file asli. Selain itu, digunakan pula **Metadata.go** untuk mendukung proses pembacaan metadata dari format non-standar. Atribut metadata yang diambil meliputi tanggal pembuatan dan modifikasi (*Create Date* dan *Modify Date*), jenis file (*File Type*), tipe konten (*MIME Type*), resolusi (DPI), dimensi gambar, serta perangkat lunak atau alat pembuat (*Creator Tool*) yang digunakan untuk menghasilkan atau mengedit file. Pemeriksaan ini dilakukan secara non-invasif untuk menjaga integritas dan keaslian file digital, sebagaimana prinsip dasar dalam praktik forensik digital.

Tahapan selanjutnya adalah *analysis*, yaitu tahap analisis perbandingan antara metadata gambar asli dan gambar hasil editan. Perbandingan dilakukan terhadap atribut-atribut penting seperti waktu modifikasi, jenis perangkat lunak, resolusi gambar, tipe

MIME, serta struktur file. Tujuan dari tahap ini adalah untuk mengidentifikasi perbedaan signifikan yang dapat mengindikasikan adanya manipulasi digital. Setiap perubahan yang ditemukan pada metadata menjadi indikator awal dalam proses investigasi, karena dapat menunjukkan aktivitas penyuntingan yang tidak sah, baik dari sisi perangkat lunak yang digunakan maupun waktu perubahan file.

Tahapan terakhir adalah *reporting*, yaitu penyusunan hasil analisis metadata ke dalam bentuk laporan sistematis. Laporan ini berisi temuan perbedaan metadata antara gambar asli dan gambar hasil manipulasi, serta interpretasi teknis terhadap indikasi adanya manipulasi digital. Laporan ini menjadi komponen penting dalam proses investigasi awal terhadap kemungkinan kebocoran informasi perusahaan melalui media gambar, dan dapat dijadikan dasar dalam pelacakan sumber atau pelaku penyebaran file digital yang telah dimodifikasi.



Gambar 1. *Flowchart* Proses Analisis Metadata

Data gambar digital dalam penelitian ini diperoleh dari simulasi internal yang melibatkan pengeditan salah satu gambar menggunakan perangkat lunak pengolah gambar. Seluruh proses dilakukan dalam lingkungan laboratorium forensik digital dengan sistem operasi Windows serta menggunakan perangkat lunak forensik sumber terbuka, guna memastikan bahwa seluruh proses berlangsung dalam kondisi yang terkendali dan dapat direplikasi.

JUPITER
Teknologi Informatika & Komputer
Vol. 6 No. 2 Agustus 2025
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187

HASIL DAN PEMBAHASAN

1. *Collection*

   Tahap ini melibatkan pengumpulan dua jenis file gambar digital yang akan dijadikan objek analisis metadata. File pertama merupakan gambar asli berformat .jpg, sedangkan file kedua merupakan hasil manipulasi yang telah disimpan dalam format .cdr (CorelDRAW). Pemilihan dua file dengan format berbeda ini bertujuan untuk membandingkan perbedaan signifikan dalam metadata, termasuk perubahan pada jenis file dan atribut lainnya.

Gambar 2. Gambar Asli

Gambar 3. Gambar Setelah Diedit

Gambar asli didesain menggunakan Canva dan diekspor dalam format JPEG tanpa dilakukan penyuntingan lanjutan. Sementara itu, gambar hasil edit telah dimodifikasi menggunakan perangkat lunak pengolah grafis berbasis vektor, yaitu CorelDRAW, dan kemudian disimpan dalam format dokumen aplikasi (.cdr). Pemilihan dua aplikasi ini menunjukkan variasi konteks penggunaan serta perbedaan struktur metadata. Kedua file dianalisis secara menyeluruh untuk mengidentifikasi potensi manipulasi berdasarkan atribut metadata yang terekam.

2. *Examination*

Pada tahap ini, dilakukan ekstraksi metadata dari kedua file gambar menggunakan aplikasi **EXIFTool versi 13.29**. EXIFTool dipilih karena kemampuannya membaca atribut tersembunyi secara menyeluruh tanpa mengubah isi file asli, sesuai dengan prinsip forensik digital yaitu *integritas bukti*.

Metadata yang dikumpulkan meliputi:

a. **Create Date** (waktu pembuatan file)
b. **File Type** (jenis file)
c. **MIME Type** (tipe konten file)
d. **Resolution** (X/Y DPI)
e. **Creator Tool** dan informasi pembuat lainnya

```
ExifTool Version Number         : 13.29
File Name                       : DesainHPPrototype.jpg
Directory                       : .
File Size                       : 126 kB
Zone Identifier                 : Exists
File Modification Date/Time     : 2025:05:10 21:04:07+07:00
File Access Date/Time           : 2025:05:10 22:11:53+07:00
File Creation Date/Time         : 2025:05:10 22:06:32+07:00
File Permissions                : -rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Little-endian (Intel, II)
Orientation                     : Horizontal (normal)
X Resolution                    : 96
Y Resolution                    : 96
Resolution Unit                 : inches
Y Cb Cr Positioning             : Centered
Exif Version                    : 0210
Components Configuration        : Y, Cb, Cr, -
Flashpix Version                : 0100
Color Space                     : Uncalibrated
Exif Image Width                : 1587
Exif Image Height               : 2245
Ads Created                     : 2025-05-10
Ads Ext Id                      : 1df2848d-6917-4162-a4f9-12864e74c1f3
Ads Fb Id                       : 525265914179588
Ads Touch Type                  : 2
Title                           : Desain HP Prototype - 1
Author                          : nathanaelchristianpt
Creator Tool                    : Canva (Renderer) doc=DAGnjLY27k0 user=UAD3-ENHnFU brand=BAD3-N2FBSM template=
Image Width                     : 1587
Image Height                    : 2245
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1587x2245
Megapixels                      : 3.6
```

Gambar 4. Metadata EXIF gambar asli

```
ExifTool Version Number         : 13.29
File Name                       : DesainHP.cdr
Directory                       : .
File Size                       : 610 kB
File Modification Date/Time     : 2025:05:12 10:01:52+07:00
File Access Date/Time           : 2025:05:12 10:02:29+07:00
File Creation Date/Time         : 2025:05:12 10:01:52+07:00
File Permissions                : -rw-rw-rw-
File Type                       : ZIP
File Type Extension             : zip
MIME Type                       : application/x-vnd.corel.zcf.draw.document+zip
Warning                         : Unrecognized MIMEType application/x-vnd.corel.zcf.draw.document+zip
Create Date                     : 2025:05:12 09:57:27+07:00
Modify Date                     : 2025:05:12 10:01:52+07:00
Metadata Date                   : 2025:05:12 10:01:52+07:00
Format                          : application/x-vnd.corel.zcf.draw.document+zip
Fonts Used                      :
Creator                         : Nathanael Christian
Last Author                     : Nathanael Christian
Sided                           :
Folds                           :
Type                            :
Industry                        :
Product Name                    : CorelDRAW
Locale                          : 1033
Embedded Ole Objects            : false
Core Version                    : 2510
Keywords                        :
Notes                           :
Title                           :
Subject                         :
Rights                          :
Revision                        : 1
Category                        :
Product Id                      : 0
App Version                     : 2520
Build Number                    : 313
Platform                        : 0
Fonts Embedded                  : false
Language                        : 1033
Identifier                      : b4eeb7b3-231c-4a57-be3e-51b1060c6d23
Instance ID                     : b4eeb7b3-231c-4a57-be3e-51b1060c6d23
Document ID                     : 1ae5e72f-6aad-492a-9aad-25ffe72e6884
Derived From                    :
Rating                          : 0
Num Pages                       : 1
Num Layers                      : 1
Page Width                      : 2100000
Page Height                     : 2970000
Page Dimensions                 : 210 x 297 mm
Page Size Name                  : A4
Page Orientation                : 1
Resolution X                    : 300
Resolution Y                    : 300
```

Gambar 5. Metadata EXIF gambar hasil edit

Hasil ekstraksi menunjukkan bahwa kedua file memiliki perbedaan signifikan pada berbagai atribut penting. Misalnya, pada gambar hasil edit, nilai pada atribut Software menunjukkan aplikasi yang digunakan untuk menyunting gambar, sementara atribut ini kosong atau berbeda pada gambar asli. Selain itu, atribut Modify Date dan Create Date mengalami pergeseran waktu yang dapat menunjukkan kapan file dimodifikasi.
Perbedaan dalam atribut MIME Type dan Resolution juga memberikan petunjuk bahwa file telah disimpan ulang dalam format yang berbeda atau diubah kualitas visualnya. Semua perbedaan ini merupakan *indikator awal* yang penting dalam proses investigasi digital, karena dapat mengarahkan penyidik untuk mendeteksi adanya potensi manipulasi atau rekayasa pada file.

3. *Analysis*

Pada tahap ketiga ini, analisis dilakukan dengan membandingkan metadata dari gambar asli dan hasil edit. Tujuan dari perbandingan ini adalah untuk mengidentifikasi atribut metadata yang mengalami perubahan akibat proses manipulasi. Perbedaan atribut tersebut dapat menjadi indikator penting dalam mengungkap adanya modifikasi file yang tidak sah.
Atribut-atribut metadata yang diamati meliputi informasi teknis seperti MIME type, Image Width, Image Height, serta informasi temporal seperti Create Date dan Modify Date. Selain itu, atribut seperti Software dan Color Space juga diperhatikan karena dapat menunjukkan adanya penggunaan aplikasi pengedit gambar atau perubahan format warna yang tidak sesuai dengan standar file asli.
Perbedaan atribut yang ditemukan menunjukkan bahwa metadata dapat memberikan informasi yang akurat mengenai proses manipulasi digital. Dengan menganalisis metadata ini, investigasi forensik dapat mengetahui tidak hanya bahwa file telah diedit, tetapi juga kapan, dengan apa, dan dalam kondisi seperti apa perubahan itu terjadi. Tabel berikut menyajikan hasil perbandingan metadata antara file gambar asli dan file hasil edit:

Tabel 1. Analisa metadata Gambar A dan Gambar B

Metadata	Gambar Asli	Gambar Manipulasi	Indikasi
File Type	JPEG	ZIP	File berubah format, bukan lagi gambar langsung
MIME Type	image/jpeg	application/x-vnd.corel.zcf.draw.document+zip	MIME bukan tipe gambar → potensi manipulasi
Create Date	2025-05-10	2025-05-12	File edit dibuat setelah file asli
Resolution (DPI)	96	300	Peningkatan resolusi → kemungkinan editing
Creator Tool	Canva	CorelDRAW	Software pembuat berbeda → bukti manipulasi

Temuan pada penelitian ini sejalan dengan studi (Apriliani et al., 2020) yang menunjukkan bahwa metadata dapat digunakan untuk mendeteksi keaslian gambar melalui informasi teknis seperti waktu pembuatan, aplikasi pengedit, dan resolusi. Namun, penelitian ini memperluas konteks dengan menggunakan format CDR, yang tidak secara eksplisit menyimpan metadata EXIF sebagaimana format JPEG. Pendekatan ini memperkuat hasil yang ditunjukkan oleh (Jaya Syafar et al., 2023), mengenai pentingnya kombinasi antara format file dan perangkat lunak pengedit

dalam proses analisis metadata. Dengan demikian, penelitian ini membuktikan bahwa bahkan file yang tampaknya tidak menyimpan metadata secara konvensional tetap dapat dianalisis secara forensik apabila menggunakan pendekatan dan alat yang tepat.

4. *Reporting*

Tahap ini merupakan penyusunan laporan hasil akhir dari analisis metadata. Tabel berikut merangkum temuan utama dari perbandingan file.

Tabel 2. Laporan Hasil Analisa Metadata

Parameter	Gambar Asli	Gambar Manipulasi	Status
MIME Type	image/jpeg	application/x-vnd.corel.zcf.draw.document+zip	Indikasi manipulasi
File Type	JPEG	ZIP	Format tidak lazim
Create Date	2025-05-10	2025-05-12	Waktu manipulasi
Creator Tool	Canva	CorelDRAW	Aplikasi pengeditan
Resolution (DPI)	96	300	Perubahan signifikan

Berdasarkan hasil analisis yang ditampilkan dalam tabel di atas, terdapat sejumlah atribut metadata yang mengalami perubahan signifikan setelah gambar dimanipulasi. Atribut-atribut tersebut antara lain MIME type, Software, Modify Date, dan dimensi gambar (Image Width/Height). Perubahan tersebut menunjukkan adanya aktivitas penyuntingan, serta memungkinkan penelusuran waktu dan alat yang digunakan dalam proses tersebut. Informasi ini penting untuk dituangkan secara sistematis dalam laporan forensik guna mendukung validitas hasil investigasi.

PENUTUP

Simpulan

Penelitian ini menunjukkan bahwa analisis metadata gambar digital berdasarkan kerangka kerja forensik NIST dapat digunakan untuk mendeteksi indikasi manipulasi file gambar. Berdasarkan perbandingan antara metadata gambar asli dan yang telah diedit, ditemukan perbedaan signifikan pada atribut seperti MIME type, resolusi, waktu pembuatan file, serta perangkat lunak yang digunakan. Hasil ini mengindikasikan bahwa metadata dapat menjadi komponen penting dalam mendeteksi perubahan mencurigakan pada file digital, khususnya pada kasus yang melibatkan potensi kebocoran informasi. Namun, perlu ditegaskan bahwa metadata tidak dapat dijadikan sebagai satu-satunya bukti atas tindakan pencurian gambar. Metadata berperan sebagai pendukung dalam rangkaian bukti digital yang lebih luas. Penggunaan alat bantu seperti EXIFTool terbukti efektif dalam mengekstraksi data tersembunyi secara efisien. Dengan demikian, pendekatan ini dapat dimanfaatkan dalam proses investigasi awal dalam ranah forensik digital, khususnya dalam kasus kebocoran informasi perusahaan.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, disarankan agar perusahaan mulai menerapkan kebijakan pengelolaan metadata secara lebih ketat sebagai bagian dari strategi keamanan informasi digital. Kesadaran karyawan juga perlu ditingkatkan melalui edukasi mengenai potensi kebocoran informasi yang dapat terjadi melalui file gambar yang tampak biasa namun menyimpan informasi penting di dalam metadata-nya. Selain itu, pelatihan teknis mengenai penggunaan alat bantu forensik metadata seperti ExifTool

sebaiknya diberikan secara rutin kepada tim keamanan informasi agar mereka memiliki kemampuan untuk mendeteksi manipulasi file secara mandiri. Untuk pengembangan penelitian selanjutnya, disarankan untuk melakukan eksplorasi lanjutan dengan menggabungkan analisis metadata dengan teknik forensik berbasis kecerdasan buatan (AI), seperti klasifikasi manipulasi gambar menggunakan machine learning atau deep learning berbasis pola metadata. Penelitian lanjutan juga dapat menguji efektivitas alat bantu metadata lainnya seperti Metadata++, Exiv2, atau Metadata2Go dalam menangani file dengan format non-standar. Selain itu, sistem analisis metadata dapat dikembangkan ke arah otomatisasi dan real-time monitoring, yang terintegrasi langsung dengan sistem keamanan perusahaan guna memperkuat kemampuan deteksi dini terhadap potensi manipulasi digital dan kebocoran data tersembunyi.

REFERENSI

Afandi, M., Amrulloh, R., Isnaini, K. N., & Suhartono, D. (2024). Analisis Forensik Pemalsuan Dokumen PDF Menggunakan Metode National Institute of Justice (NIJ). *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *7*(3), 162–170. https://doi.org/10.31598/JURNALRESISTOR.V7I3.1460

Apriliani, A., Hijjayanti, K., & Suhairoh, S. (2020). Analisis Keaslian Citra Dengan Menggunakan Exif Metadata. *CESS (Journal of Computer Engineering, System and Science)*, *5*(1), 84–88. https://doi.org/10.24114/CESS.V5I1.15600

Fajar, R., Erick, I. A., & Abdul, R. M. (2024). Deteksi Foto Palsu Menggunakan Tools Forensically. *Literatur Informatika & Komputer*, *1*(3), 277–283. https://doi.org/10.33096/linier.v1i3.2505

Firdonsyah, A., & Wijayanto, D. (2022). Analisis Forensik Rekayasa Dokumen Digital dengan Metode NIST. *INFORMAL: Informatics Journal*, *7*(2), 121. https://doi.org/10.19184/ISJ.V7I2.31198

Fransiskus, M., & P, N. (2024). Analisis Digital Forensik Metadata pada Rekayasa Digital Image sebagai barang bukti Digital. *Infact: International Journal of Computers* , *8*(01), 1–5. https://doi.org/10.61179/JURNALINFACT.V8I01.439

Khairunnisak, K., Ashari, H., & Kuncoro, A. P. (2020). Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *3*(2), 72–81. https://doi.org/10.31598/JURNALRESISTOR.V3I2.634

Mualfah, D., & Ramadhan, R. A. (2021). Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology). *IT Journal Research and Development*, *5*(2), 171–182. https://doi.org/10.25299/ITJRD.2021.VOL5(2).5731

Satria, A. F., Adam, R. I., & Carudin, C. (2021). Analisis Digital Watermarking untuk Otentikasi pada Citra Manipulasi Menggunakan Metode Least Significant Bit. *Edumatic: Jurnal Pendidikan Informatika*, *5*(2), 204–213. https://doi.org/10.29408/edumatic.v5i2.3901

Syafar, Z. J., Salim, Y., & Rachman Manga', A. (2023). Analisis Penerapan Metode Exif Metadata Dan Metode Error Level Analysis Untuk Pengolahan Forensic Digital. Literatur Informatika & Komputer, x, pp xx-xx. https://doi.org/10.33096/linier.vxix.xxxx

Sulistyo, W. Y., Riadi, I., & Yudhana, A. (2020). Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital(Application of SURF Technique in

Image Forensic for Digital Photo Engineering Analysis). *JUITA: Jurnal Informatika*, *8*(2), 179–186. https://doi.org/10.30595/JUITA.V8I2.6602