Analisis Forensik Rekayasa Dokumen PDF dengan Metode NIST

Arizona Firdonsyah*, Danur Wijayanto**
* Program Studi Teknologi Informasi, Universitas 'Aisyiyah Yogyakarta
** Program Studi Teknologi Informasi, Universitas 'Aisyiyah Yogyakarta
*arizona@unisayogya.ac.id, **danurwijayanto@unisayogya.ac.id

ABSTRACT

Digital Forensics is one of the technological fields contained many sub-fields that can assist technically in collecting digital evidence to be presented in a trial in accordance with applicable law. The example of digital forensics sub-field is Image Forensics, which aims to digitally collect and look for evidentiary facts in determining the authenticity of an image or document that contained images. Various criminal and pornographic cases involving image files are still happening nowadays, therefore forensics on images as evidence is an important key to assist the court in making decisions. This research examines the authenticity of documents in the form of digital letters using National Institute of Standard and Technology (NIST) method by applying the forensic ELA (Error Level Analysis). Several previous researches have proven that the forensic ELA is able to detect modifications that have been made to images. Differences with previous researches and this research are the authors also checked the metadata of the images before performing the ELA examination using Fotoforensics. The results of the analysis shows a high level of consistency in the images and writings due to the accumulation of white dots in several places such as in headers, logos, header's writings, text contents, footnotes, and signatures, and based on the conducted analysis and investigation, Fotoforensics shows 100% result on finding every anomaly on digital evidence provided.

Keyword: forensics, document, images, NIST, ELA

1. Pendahuluan

Perkembangan teknologi citra digital yang semakin maju membuat mudahnya merubah atau memodifikasi foto sehingga pemalsuan citra semakin sering terjadi. Teknik manipulasi citra yang semakin berkembang membuat orang yang melihat merasa kesulitan untuk membedakan foto asli dan manipulasi [1]. Kegiatan manipulasi citra sering kali dilakukan sebelum citra tersebut dipublikasi. Manipulasi citra memiliki tujuan seperti memperbaiki background dan memanipulasi bagian tertentu [2]. Manipulasi citra juga bisa digunakan untuk melakukan hal-hal yang negatif seperti menyindir atau menjatuhkan orang lain dan menyebarkan berita palsu (hoax).

Kemajuan teknologi dalam bidang informasi, komunikasi dan media telah mengubah pola pikir dan perilaku masyarakat. Hal tersebut menyebabkan perubahan budaya, ekonomi dan sosial secara signifikan [3]. Teknologi informasi saat ini bisa dikatakan sebagai pedang bermata dua, karena selain dapat memberi dampak negatif juga memberi dampak positif. Dampak positif yang ditimbulkan adalah munculnya kemudahan-kemudahan dalam pencarian informasi, namun diimbangi juga dengan dampak negatif dengan munculnya berbagai aksi kejahatan yang menggunakan teknologi informasi dan internet sebagai medianya, yang disebut dengan istilah cybercrime [4].

Forensik digital dapat membantu secara teknis pada pengumpulan bukti-bukti secara digital untuk disajikan dalam suatu persidangan yang sesuai dengan hukum yang berlaku. Salah satu contoh bidang ilmu digital forensics adalah image forensics yang bertujuan untuk pengumpulan dan mencari fakta-fakta pembuktian dalam menentukan keaslian citra atau gambar [5]. Kasus-kasus kriminal dan pornografi yang melibatkan file gambar masih sering terjadi, oleh karena itu forensik terhadap gambar sebagai barang bukti menjadi kunci penting untuk membantu pengadilan dalam mengambil keputusan.

Penelitian yang dilakukan akan menguji keaslian dokumen berupa surat digital menggunakan motode National Institute of Standard and Technology (NIST) dengan menerapkan forensik ELA (Error Level Analisis). Penelitian sejenis pernah dilakukan oleh peneliti – peneliti sebelumnya antara lain penelitian yang dilakukan Ananga Thapaliya et al. [6] membahas pengenalan dan jenis-jenis manipulasi citra digital (*digital image forgery*) dan teknik-teknik yang digunakan untuk mendeteksi manipulasi citra digital, hasil dari penelitian ini adalah terdapat banyak cara jalur yang berbeda untuk memodifikasi citra digital, misalnya, *copy-*

move, *splicing*, dan *resampling*. Penelitian yang dilakukan oleh Thapaliya ini berfokus pada dua jenis pendeteksian pemalsuan citra digital yaitu *copy move* dan *image splicing*.

Penelitian yang dilakukan oleh Irwansyah et al., Shaweta et al., dan Firdonsyah, menunjukkan bahwa dalam melakukan investigasi Computer Forensics seperti pemalsuan gambar dapat menggunakan beberapa alat perangkat lunak dan perangkat keras sesuai dengan kebutuhan [7][8][9]. Kombinasi dari performa perangkat lunak dan perangkat keras forensik yang digunakan dapat memberikan hasil yang lebih maksimal dan akurasi yang lebih tinggi dibandingkan dengan penggunaan perangkat forensik tunggal (*standalone forensic tool*)

Penelitian lain yang berhubungan dengan gambar dilakukan oleh Harahap [10]. Harahap meneliti mengenai Fotoforensic dan menyimpulkan bahwa fitur dari www.fotoforensics.com dapat digunakan sebagai deteksi keaslian citra atau gambar yang tepat. Fasilitas yang disediakan dari fotoforensics.com dapat digunakan dan sangat efisien untuk mendeteksi keaslian foto terutama pada fitur ELA (Error Level Analysis). Penelitian tersebut hanya menunjukkan bagian foto yang pernah dimanipulasi dengan menampilkan perbedaan dan membandingkan gradien warna pada foto asli dan manipulasi.

Penelitian yang dilakukan Sulistyo et al. melakukan deteksi keaslian citra dengan menggunakan metode ELA dan Principal Component Analysis (PCA) dengan menggunakan alat Forensically Beta. Metode yang digunakan pada penelitian ini berhasil mendeteksi keaslian citra berdasarkan komponen warnanya. Gambar yang termanipulasi memiliki kontras warna yang jauh lebih tajam apabila dibandingkan dengan gambar asli yang berlaku untuk metode ELA dan PCA [11].

Penelitian selanjutnya dilakukan oleh Irwansyah & Yudiastuti yang menggunakan metode ELA serta alat Forensically Beta terhadap rekayasa Image splicing, Copy – Move dan Retouching Images menunjukkan dapat mendeteksi perbedaan pada kedua objek gambar yang diteliti [12]. Analisis forensik image menggunakan aplikasi JPEGSnoop juga menampilkan hasil yang jelas terhadap perbedaan antara gambar yang asli dengan gambar yang telah direkayasa.

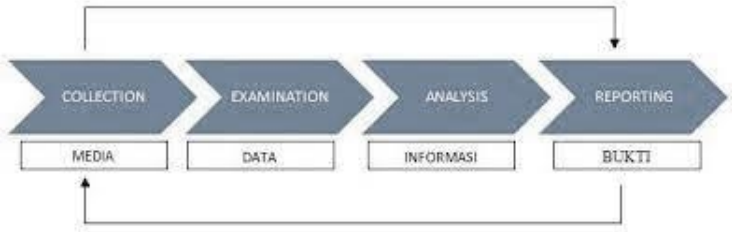
Penelitian yang dilakukan oleh Yuwono & Wijaya [13] meneliti mengenai perbandingan File Carving dengan menggunakan metode NIST. Penelitian ini menunjukkan bahwa dengan menggunakan metode NIST, dapat membantu menganalisis dan mendapatkan informasi dari bukti digital.

Penelitian sebelumnya telah ada yang membuktikan bahwa forensik ELA dapat mendeteksi modifikasi yang telah dilakukan pada gambar. Perbedaan dengan penelitian sebelumnya adalah, penelitian ini melakukan pemeriksaan metadata dari gambar sebelum melakukan pemeriksaan forensik ELA dengan menggunakan perangkat lunak Fotoforensics [14].

2. Metode Penelitian

3.1 Metode Penelitian

Metode yang digunakan dalam penelitian ini merupakan kerangka kerja yang disusun oleh National Institute of Standard and Technology (NIST) Tahapan metode NIST dapat dilihat pada Gambar 1.



Gambar 1. Skema Metode NIST

Penjelasan dari tahapan metode NIST adalah sebagai berikut :

3.1.1. Collection/ Preservation

Tahap ini disebut juga tahap preservasi. Tahap ini merupakan proses koleksi, identifikasi, pelabelan, perekaman, dan pengambilan barang bukti berupa perangkat keras yang akan diambil datanya untuk digunakan sebagai bukti digital dari suatu kasus kejahatan digital. Proses ini dilakukan dengan mengikuti prosedur penjagaan integritas data. Penjagaan integritas data dapat dilakukan dengan teknik isolasi barang bukti fisik dan pembuatan cadangan dokumen asli berupa *cloning* atau *image file* dari barang bukti fisik tersebut. Penelitian ini menggunakan barang bukti fisik berupa dokumen PDF yang didapatkan dari komputer korban, kemudian dilakukan *cloning* barang bukti fisik sehingga didapatkan hasil bukti digital siap pakai seperti pada Gambar 2 (nama korban disamarkan untuk menjaga integritas dan kerahasiaan kasus sesuai prinsip CIA (Confidentiality, Integrity, Availability).

Gambar 2. Barang Bukti berupa Dokumen PDF

3.1.2. Examination

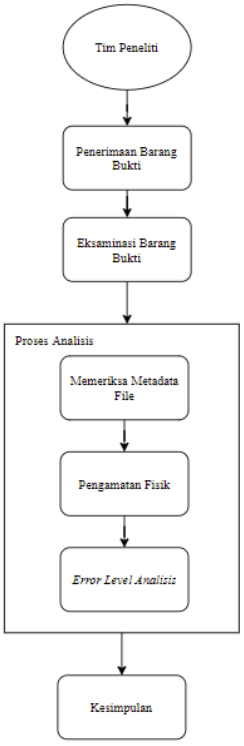
Proses eksaminasi dilakukan untuk pemrosesan data yang dikumpulkan secara forensik menggunakan kombinasi dari berbagai skenario, baik otomatis maupun manual, serta menilai dan mengeluarkan data sesuai dengan kebutuhan dengan tetap mempertahankan integritas data. Proses eksaminasi pada penelitian ini dilakukan dengan dengan memisahkan dan membuat *softcopy* barang bukti berupa tujuh file surat berformat pdf dan analisis dilakukan menggunakan *softcopy* barang bukti supaya integritas barang bukti tetap terjaga dan dapat digunakan kembagi apabila dibutuhkan.

3.1.3. Analysis

Proses analisis dilakukan untuk memeriksa hasil dari proses examination dengan menggunakan metode yang dibenarkan secara teknik dan hukum guna mendapatkan informasi yang dapat digunakan untuk menjawab pertayaan-pertayaan yang menjadi pendorong dalam melakukan pemeriksaan. Analisis yang dilakukan pada penelitian ini adalah:

i. Memeriksa metadata file yang akan diuji keasliannya. Analisa metadata ini dilakukan di awal untuk mengetahui detail sumber file. Poin yang diamati adalah MAC (Modification Time, Access Time, and Creation Time).
ii. Melakukan pengamatan fisik dan melakukan penilaian awal temuan kejanggalan pada bagian surat.
iii. Melakukan ELA untuk mengetahui apakah ada manipulasi digital di dalam file.

Tahapan proses analisis secara detail ditunjukkan pada Gambar 3.



Gambar 3. Tahapan Proses Analisis

3.1.4. Reporting

Tahap *reporting*/pelaporan merupakan proses pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai alat dan prosedur yang dipilih, penentuan tindakan lain yang perlu dilakukan (misalnya, pemeriksaan forensik dari sumber data tambahan, mengamankan celah yang teridentifikasi, atau meningkatkan kontrol keamanan yang ada), dan memberikan rekomendasi untuk perbaikan kebijakan, prosedur, alat, dan aspek lain dari proses forensik [15].

3.2 Alat Penelitian

Perangkat lunak forensik yang digunakan pada penelitian ini adalah seperti dijelaskan pada tabel 1.

Tabel 1. Perangkat Lunak Forensik

No	Perangkat Lunak Forensik	Deskripsi
1	Foxit PDF	Perangkat lunak pembaca dokumen PDF yang dapat digunakan untuk melakukan observasi fisik terhadap dokumen PDF
2	Metadata2Go	Perangkat lunak daring berlisensi gratis yang dapat memberikan akses pada metadata tersembunyi
2	FotoForensics	Perangkat lunak yang digunakan pada ranah digital forensik untuk melakukan analisis terhadap gambar dan dokumen

3. Hasil dan Pembahasan

4.1 Collection

Pada tahap ini, peneliti melakukan proses koleksi berkas barang bukti yang dianalisa berupa satu file PDF yang mempunyai empat halaman.

4.2 Examination

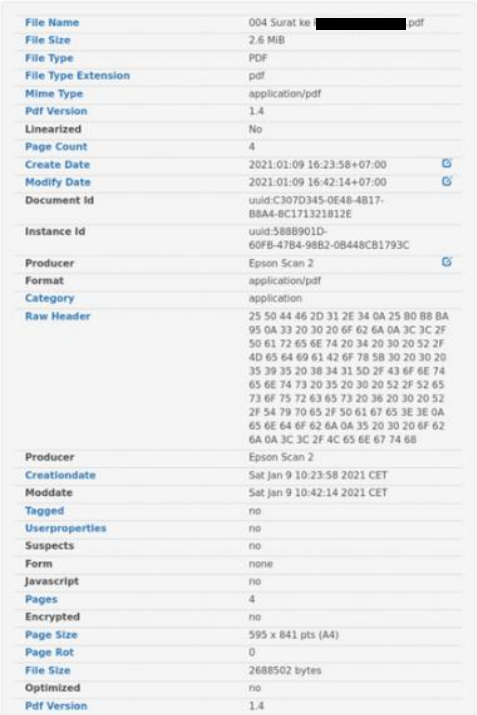
Proses eksaminasi (pemisahan dan penjagaan integritas barang bukti dilakukan dengan memisahkan dan membuat soft copy barang bukti berformat pdf dan analisis dilakukan menggunakan *soft copy* barang bukti supaya integritas barang bukti tetap terjaga dan dapat digunakan kembali apabila dibutuhkan.

4.3 Analysis

Proses analisa dilakukan dalam beberapa tahap yaitu:

4.3.1. Memeriksa metadata

Analisa metadata dilakukan untuk mengetahui detail sumber file khususnya MAC (Modification Time, Access Time, and Creation Time). Contoh hasil pemeriksaan metada ditunjukkan pada Gambar 4.



File Name	004 Surat ke [redacted].pdf
File Size	2.6 MiB
File Type	PDF
File Type Extension	pdf
Mime Type	application/pdf
Pdf Version	1.4
Linearized	No
Page Count	4
Create Date	2021:01:09 16:23:58+07:00
Modify Date	2021:01:09 16:42:14+07:00
Document Id	uuid:C307D345-0E48-4B17-B8A4-BC171321812E
Instance Id	uuid:588B901D-60FB-47B4-98B2-0B448CB1793C
Producer	Epson Scan 2
Format	application/pdf
Category	application
Raw Header	25 50 44 46 2D 31 2E 34 0A 25 B0 B8 BA 95 0A 33 20 30 20 6F 62 6A 0A 3C 3C 2F 50 61 72 65 6E 74 20 34 20 30 20 52 2F 4D 65 64 69 61 42 6F 78 5B 30 20 30 20 35 39 35 20 38 34 31 5D 2F 43 6F 6E 74 65 6E 74 73 20 35 20 30 20 52 2F 52 65 73 6F 75 72 63 65 73 20 36 20 30 20 52 2F 54 79 70 65 2F 50 61 67 65 3E 3E 0A 65 6E 64 6F 62 6A 0A 35 20 30 20 6F 62 6A 0A 3C 3C 2F 4C 65 6E 67 74 68
Producer	Epson Scan 2
Creationdate	Sat Jan 9 10:23:58 2021 CET
Moddate	Sat Jan 9 10:42:14 2021 CET
Tagged	no
Userproperties	no
Suspects	no
Form	none
Javascript	no
Pages	4
Encrypted	no
Page Size	595 x 841 pts (A4)
Page Rot	0
File Size	2688502 bytes
Optimized	no
Pdf Version	1.4

Gambar 4. Hasil Pemeriksaan Metadata

Dari hasil pemeriksaan metadata yang ditunjukkan pada Gambar 3 terdapat bagian – bagian yang perlu dicermati yang ditunjukkan pada Tabel 2.

Tabel 2. Important Metadata

No	Jenis Metadata	Deskripsi
1	Create Date	9 Januari 2021 16:23:58+07:00
2	Modify Date	9 Januari 2021 16:42:14+07:00
2	Producers	Epson Scan

Berdasarkan metadata pada Gambar 3 dan Tabel II, file yang bersangkutan dibuat pada tanggal 9 Januari 2021 pukul 16:23:58 GMT (Greenwich Mean Time) dan suntingan terakhir pada tanggal 9 Januari 2021 pukul 16:23:58 GMT dan dapat diasumsikan merupakan hasil scan dari printer Epson.

4.3.2.Melakukan pengamatan fisik

Proses ini dilakukan untuk melakukan penilaian awal apabila ditemukan kejanggalan pada bagian surat. Hasil pengamatan fisik berupa temuan kejanggalan barang bukti ditunjukkan pada Tabel 3.

Tabel 3. Hasil Pengamatan Fisik

No	Temuan Awal	Objek Temuan
1	Terdapat pembubuhan paraf pada surat dimaksud yang tidak diketahui pemilik tanda paraf tersebut dan tanda paraf tersebut dimungkinkan hasil penggandaan elektronik bukan dari paraf langsung	Paraf
2	Terdapat pembubuhan paraf pada surat dimaksud yang tidak diketahui pemilik tanda paraf tersebut, terdapat tanda tangan dan tanda paraf yang dimungkinkan hasil penggandaan elektronik bukan dari paraf langsung. Warna stempel biru atau warna cerah, namun pada tampilan terlihat bahwa warna stempel menimpa dan tidak terputus oleh warna tanda tangan yang berwarna hitam dan lebih gelap.	Paraf

4.3.3. Melakukan ELA

File mempunyai 3 halaman yang semuanya dianalisa untuk menemukan apakah ada manipulasi digital di dalam halaman tersebut. Halaman pertama ditunjukkan pada Gambar 5, Halaman kedua ditunjukkan pada Gambar 6 dan Halaman ketiga ditunjukkan pada Gambar 7. Halaman pertama menunjukan tingkat ketidak konsistenan yang tinggi pada gambar dan tulisan. Terlihat banyak penumpukan titik putih tempat-tempat berikut: tulisan pada kop surat, logo kop surat di sebelah kanan, tulisan isi surat, tulisan dan stempel pada tanda tangan, paraf di kanan bawah, dan tulisan di bawah surat. Penumpukan titik putih ini mengindikasikan adanya manipulasi digital yang dilakukan pada file.

Gambar 5. Halaman Pertama


PERSATUAN
PANAHAN INDONESIA
(PERPANI)

INDONESIA ARCHERY
ASSOCIATION

Gambar 6. Halaman Kedua

Halaman kedua menunjukan tingkat ketidak konsistenan yang tinggi pada gambar dan tulisan. Terlihat banyak penumpukan titik putih tempat-tempat berikut: semua logo kop surat, tulisan kop surat, isi tulisan, tulisan kaki surat, dan paraf di bawah kanan. Penumpukan titik putih ini mengindikasikan adanya manipulasi digital yang dilakukan pada file.

Halaman ketiga menunjukan tingkat inkonsistensi yang tinggi pada gambar dan tulisan. Terlihat banyak penumpukan titik putih pada tempat-tempat berikut: semua logo kop surat, tulisan kop surat, isi tulisan, kaki surat, dan paraf di bawah kanan. Penumpukan titik putih ini mengindikasikan adanya manipulasi digital yang dilakukan pada file.


PERSATUAN
PANAHAN INDONESIA
(PERPANI)

INDONESIA ARCHERY
ASSOCIATION

Gambar 7. Halaman Ketiga

4.4 Reporting

Analisis forensik yang telah dilakuan menunjukkan bahwa surat-surat tersebut diduga telah dimanipulasi berdasarkan Proses dan Teknik antara lain pemeriksaan dan pengamatan fisik yang dilakukan dengan menggunakan perangkat lunak Foxit PDF, pemeriksaan dan pengamatan metadata dengan perangkat lunak metadata2go dan pemeriksaan Error Level Analysis dengan menggunakan perangkat lunak Fotoforensics.

4. Kesimpulan

Hasil penelitian menunjukkan dengan menggunakan metode National Institute of Standard dan Technology (NIST) dan Error Level Analisis (ELA) dapat digunakan untuk membuktikan keaslian citra atau gambar dan file. Hasil analisa menunjukkan tingkat konsistenan yang tinggi pada gambar dan tulisan dikarenakan terlihat banyak penumpukan titik putih beberapa tempat seperti logo kop surat, tulisan kop surat, isi tulisan, tulisan kaki surat, dan paraf di bawah kanan. Hasil analisis dan investigasi yang dilakukan menunjukkan nilai unjuk kerja dan hasil pengujian yang dilakukan menggunakan Fotoforensic adalah sebesar 100%. Penelitian selanjutnya dapat dikembangkan dengan melakukan perbandingan dengan alat forensik yang lain.

Referensi

[1] A. Y. Wijaya, S. Al Musayyab, and H. Studiawan, "Pengembangan Metode Block Matching Untuk Deteksi Copy-Move Pada Pemalsuan Citra," *JUTI: Jurnal Ilmiah Teknologi Informasi*, vol. 15, no. 1, p. 84, 2017, doi: 10.12962/j24068535.v15i1.a638.

[2] I. Riadi, A. Fadlil, and T. Sari, "Image Forensic for detecting Splicing Image with Distance Function," *International Journal of Computer Applications*, vol. 169, no. 5, pp. 6–10, 2017, doi: 10.5120/ijca2017914729.

[3] M. R. Wijaya and R. Arifin, "Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?," *IJCLS (Indonesian Journal of Criminal Law Studies)*, vol. 5, no. 1, pp. 63–74, 2020, doi: 10.15294/ijcls.v5i1.23273.

[4] A. G. Gani, "Cybercrime (Kejahatan Berbasis Komputer)," *Jurnal sistem Informasi*, vol. 5, no. 1, pp. 16–29, 2018.

[5] R. Umar, A. Fadlil, and A. I. Putra, "Analisis Forensics Untuk Mendeteksi Pemalsuan Video," *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, vol. 3, no. 2, p. 193, 2019, doi: 10.30645/j-sakti.v3i2.140.

[6] A. Thapaliya, D. E. Atonge, M. Mazzara, S. Chakraborty, I. Afanasyev, and M. Ahmad, "Digital Image Forgery," *CEUR Workshop Proceedings*, vol. 2525, no. December 2019, 2019, doi: 10.1201/9781315123905-12.

[7] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Scientific Journal of Informatics*, vol. 5, no. 2, pp. 235–247, 2018, doi: 10.15294/sji.v5i2.16545.

[8] S. Sachdeva, B. L. Raina, and A. Sharma, "Analysis of Digital Forensic Tools," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 6, pp. 2459–2467, 2020, doi: 10.1166/jctn.2020.8916.

[9] A. Firdonsyah, "Comparative Analysis of Forensic Softwares for Android-based Blackberry Messenger Using NIJ Framework and NIST Measurements," vol. 10, no. 2, pp. 78–90, 2021.

[10] F. Harahap, "Deteksi Foto Manipulasi Dengan Tools Forensicallybeta dan Imageforensic . org Dengan Metode Error Level Analysis (ELA)," vol. 2, no. 3, 2021.

[11] W. Y. Sulistyo, I. Riadi, and A. Yudhana, "Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital," *JUITA: Jurnal Informatika*, vol. 8, no. 2, p. 179, 2020, doi: 10.30595/juita.v8i2.6602.

[12] I. Irwansyah and H. Yudiastuti, "Analisis Digital Forensik Rekayasa Image Menggunakan Jpegsnoop Dan Forensically Beta," *Jurnal Ilmiah Matrik*, vol. 21, no. 1, pp. 54–63, 2019, doi: 10.33557/jurnalmatrik.v21i1.518.

[13] D. T. Yuwono and Y. W, "Analisis Perbandingan File Carving Dengan Metode Nist," *Jurnal Sains Komputer dan Teknologi Informasi*, vol. 2, no. 2, pp. 1–6, 2020, doi: 10.33084/jsakti.v2i2.1472.

[14] F. Mahardika, A. D. Khatulistian, and A. P. Kuncoro, "Review Foto Forensic.com dengan Teknik Error Level Analysis dan JPEG untuk mengetahui Citra Asli," *Jurnal Informatika: Jurnal Pengembangan IT Poltek Tegal*, vol. 03, no. 01, pp. 71–75, 2018.

[15] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.