ANALISIS DIGITAL IMAGE FORENSIK TERHADAP KEASLIAN FILE IMAGE MELALUI WHATSAPP DENGAN METODE NIST

Hafil Rizkyawan, Didi Juardi, Jajam Haerul Jaman
Teknik Informatika, Universitas Singaperbangsa Karawang
Jl. HS.Ronggo Waluyo, Puseurjaya, Kec. Telukjambe Tim., Kabupaten Karawang
hafil.rizkyawan19081@student.unsika.ac.id

ABSTRAK

Dalam era globalisasi sekarang banyak perkembangan yang sangat pesat dalam berbagai sektor bidang, contoh nya dalam bidang kesehatan, militer, keamanan, pemerintahan, pendidikan, dan lain-lainnya. Dengan banyak nya kemudahan dalam perkembangan teknologi informasi dan komunikasi sehingga banyak orang menyalahgunakan fungsi dari banyaknya fitur yang diberikan. Faktanya bahwa perkembangan teknologi informasi dan komunikasi yang semakin pesat, khususnya dalam bentuk aplikasi chat dan media sosial, seperti *WhatsApp*. Penelitian ini bertujuan untuk menganalisis keaslian file gambar yang dikirim melalui *WhatsApp* menggunakan metode *National Institute of Standards and Technology (NIST).* Dalam penelitian ini, lima kasus pemalsuan file gambar dianalisis dengan bantuan *ExifTool* dan *Forensically Beta*. Metode *NIST* digunakan untuk mengidentifikasi manipulasi pada metadata dan struktur gambar yang dikirim melalui *WhatsApp*. Hasil penelitian menunjukkan bahwa metode *NIST* efektif dalam memverifikasi keaslian file gambar. Dari lima kasus yang dianalisis, hanya satu file gambar yang terbukti asli setelah penelitian mendalam terhadap metadata, warna, tekstur, dan gradasi gambar.

Kata kunci : *digital image forensic, whatsapp, NIST, exiftool, forensically*

1. PENDAHULUAN

Abad ke-21 merupakan abad yang paling cemerlang dan inovatif dalam berbagai penemuan dan perkembangan nya. Dalam era globalisasi sekarang banyak perkembangan yang sangat pesat dalam berbagai sektor bidang, contoh nya dalam bidang kesehatan, militer, keamanan, pemerintahan, pendidikan, dan lain-lainnya. Dalam semua perkembangan nya yang paling signifikan terlihat adalah dalam sektor teknologi, yang mana hampir dalam setiap bidang pasti menggunakan teknologi dalam menjalankan segala kegiatannya. Bukan tanpa alasan teknologi berkembang karena sangat membantu dan memudahkan umat manusia dalam menjalankan setiap kegiatan, dan juga teknologi sangat efektif dan efisien dalam mengerjakan setiap kegiatan di tiap bidang nya.

Teknologi digital adalah teknologi informasi yang mengutamakan kegiatan yang dilakukan dengan menggunakan komputer/digital daripada menggunakan tenaga manusia.

Namun, cenderung menjadi sistem operasi yang sepenuhnya otomatis dan kompleks dengan sistem/format terkomputerisasi yang dapat dibaca oleh komputer. [1] Kemajuan teknologi ada dalam banyak bidang dan spesifikasi nya. Internet merupakan salah satu hal yang menunjang dalam kemajuan teknologi, dan juga internet merupakan salah satu penemuan dan perkembangan dalam dunia informasi dan komunikasi.

Tercatat dalam Statistik Telekomunikasi Indonesia 2020 yang mengacu pada Badan Pusat Statistik bahwa pengguna internet paling pesat perkembangan nya berasal dari rumah tangga yang mana memiliki angka 78,18%. Perkembangan ini diikuti juga oleh kenaikan pertumbuhan penduduk dalam kurun waktu 5 tahun 2016-2020 yang semula pada tahun 2016 pengguna internet sekitar 25,37% dan pada 2020 menjadi 53,73%. Dan sekarang semua tergantung pada internet dan gadget dalam kehidupan sehari-hari.

Dengan banyak nya kemudahan dalam perkembangan teknologi informasi dan komunikasi sehingga banyak orang menyalahgunakan fungsi dari banyaknya fitur yang diberikan. Dengan kemajuan teknologi yang semakin pesat, sistem keamanan juga semakin ditingkatkan untuk mengatasi tindakan kejahatan dunia maya yang meningkat secara signifikan. Akibatnya, pelaku kejahatan dunia maya menjadi semakin aktif dan dengan cepat mencapai kemajuan baru dalam sistem keamanan yang diterapkan dalam memerangi kejahatan dunia maya. [2].

Dengan WhatsApp Messenger mempunyai keistimewaan yaitu dapat melakukan chatting online berupa bertukar teks, berbagi file mp3, file mp4, bertukar foto, video, voice note, peta lokasi dan masih banyak lagi. Dengan fitur ini, pengguna akan lebih mudah berkomunikasi satu sama lain menggunakan WhatsApp Messenger. Oleh karena itu, tidak menutup kemungkinan orang yang hendak melakukan kejahatan akan bertukar informasi atau perintah melakukan kejahatan menggunakan WhatsApp Messenger dengan informasi dalam bentuk teks atau file. [3]

Tingginya angka kejahatan penipuan dan platform *Whatsapp* sebagai sarana melakukan kejahatan sebanding dengan tingkat pengguna internet, aktivitas media sosial dan *Whatsapp* sebagai media sosial populer di Indonesia. Berdasarkan

permasalahan tersebut, perlu dilakukan upaya untuk melacak kejahatan yang dilakukan para pelaku. [4]

Digital Forensik merupakan salah satu cabang ilmu forensik yang digunakan untuk penyelidikan dan penyidikan dalam pemeriksaan bahan (data) dan penemuan isi perangkat digital. Para ahli mengatakan forensik digital adalah seperangkat teknik dan prosedur pencarian dan pengumpulan bukti berdasarkan unit dan perangkat digital sebagai alat bukti yang efektif di pengadilan. [5]

Salah satu metode yang digunakan *dalam Digital Image Forensik* adalah metode *NIST (National Institute of Standards and Technology)*. Metode ini sangat efektif dalam mengidentifikasi apakah sebuah file image telah mengalami perubahan atau tidak. Institut Standar dan Teknologi Nasional *(NIST)* adalah metode yang digunakan untuk mengumpulkan bukti digital dan mencakup tahap pengumpulan, pengujian, analisis, dan pelaporan forensik. [6]

Keberadaan teknologi forensik digital menjadi semakin penting dalam menghadapi kasus-kasus hukum yang melibatkan bukti digital, termasuk dalam kasus kejahatan cyber. Pesatnya perkembangan teknologi dan gaya hidup masyarakat menyebabkan perubahan kebutuhan teknologi yang cepat, dimana teknologi digital menjadi pilihan utama di sini. [1]

2. TINJAUAN PUSTAKA

2.1. Digital Forensik

Digital forensik telah mengalami evolusi yang signifikan selama beberapa dekade terakhir. Investigasi forensik digital mengacu pada proses ilmiah dan hukum dalam menyelidiki kejahatan dunia maya dan media atau objek digital untuk mengumpulkan bukti. Bukti digital harus membuktikan bahwa kejahatan telah dilakukan atau digunakan untuk mendapatkan akses tidak sah. [7]

Contoh subbidang forensik digital adalah forensik gambar yang bertujuan untuk mengumpulkan dan mencari bukti digital kejadian untuk mengetahui keaslian suatu gambar atau dokumen yang mengandung gambar. Berbagai kasus kejahatan dan pornografi yang melibatkan file gambar masih terjadi hingga saat ini. Oleh karena itu, analisis forensik terhadap gambar sebagai bukti menjadi kunci penting untuk membantu pengadilan mengambil keputusan. [8]

2.2. File Image

File gambar adalah sebuah jenis file yang berisi data citra atau gambar yang telah diubah menjadi format digital. File gambar ini dapat berupa berbagai jenis format file seperti JPG, PNG, GIF, dan TIFF. Saat memverifikasi keaslian suatu file foto, beberapa teknik forensik digunakan untuk membuktikan dan memeriksa foto tersebut, menggunakan perangkat lunak yang digunakan untuk memeriksa data sensitif yang terkandung dalam foto tersebut menggunakan alat dan teknik fotografi. [9]

2.3. Bukti Digital

Bukti digital adalah informasi yang disimpan dalam format digital dan digunakan sebagai bukti dalam proses investigasi atau persidangan. Bukti digital sangat berharga dan dapat digunakan pada tahap investigasi dan pengadilan. Banyak kasus penjahat siber yang menggunakan file foto masih sering terjadi, sehingga analisis forensik terhadap foto atau gambar menjadi kunci utama penyelesaian kasus. [10]

Bukti digital pada dasarnya sangat rapuh dan pada saat yang sama disimpan dalam jangka waktu yang lama. Konten dan lokasi dapat diubah dengan mudah dan cepat. Pada saat yang sama, selama kondisi dan lokasinya tetap sama seperti saat disita, mereka dapat memberikan informasi pembuktian penting dengan jelas dan tidak dapat disangkal. [11]

2.4. *Cybercrime*

Perkembangan penggunaan media sosial yang pesat ini tidak hanya memberikan dampak positif, namun juga menimbulkan dampak negatif, seperti kejahatan (cybercrime). [12] Kejahatan dengan menggunakan teknologi digital mudah dilakukan dengan menggunakan komputer. Oleh karena itu, tidak mengherankan jika kasus kejahatan siber (cybercrime) semakin banyak terjadi. [9]

2.5. *WhatsApp*

WhatsApp adalah sebuah aplikasi pesan instan yang memungkinkan pengguna untuk bertukar pesan teks, gambar, dan video secara gratis melalui koneksi internet. Aplikasi ini dapat digunakan pada berbagai platform seperti *Android, iOS, dan Windows Phone*. *WhatsApp* pertama kali diluncurkan pada tahun 2009 dan saat ini telah menjadi salah satu aplikasi pesan instan paling populer di seluruh dunia. Aplikasi ini juga sangat mudah digunakan, hanya dengan mendaftarkan nomor telepon, dan mudah dipahami oleh pengguna aplikasi. Maka tidak heran jika aplikasi *WhatsApp* bisa dikembangkan dengan sangat cepat. [6]

2.6. Metode *NIST*

Metode *NIST* adalah salah satu metode yang dapat digunakan dalam analisis *digital image forensik* untuk menentukan keaslian suatu *file image* atau foto. Metode ini dapat membantu dalam menentukan keaslian suatu bukti digital dalam kasus-kasus hukum. NIST adalah metode empat langkah untuk menyelesaikan dan menyelidiki kasus kejahatan dunia maya, langkah pertama adalah pengumpulan (pengumpulan data), pemeriksaan (pemeriksaan bukti), analisis dan terakhir pelaporan pelaporan (menghasilkan laporan berdasarkan hasil analisis). [13]

2.7. *Metadata*

Metadata adalah data yang memberikan informasi tentang data lainnya. *Metadata* berfungsi

untuk memberikan konteks dan informasi tambahan tentang data yang diterapkan pada berbagai jenis data seperti teks, gambar, video, atau audio. Sistem ini menggunakan metadata atau data tentang aset digital untuk memungkinkan penemuan, identifikasi, dan pengiriman sumber daya kepada pengguna. Metadata juga membantu inventaris, pelacakan, dan manajemen internal lainnya dari aktivitas. [14]

2.8. *Exiftool*

ExifTool adalah perangkat lunak berbasis baris perintah yang digunakan untuk membaca, menulis, dan mengedit metadata (informasi tentang informasi) dalam berbagai jenis file, termasuk file gambar, audio, dan video. Secara umum, sebagian besar pengguna alat ini sering mengidentifikasi gambar berdasarkan informasi metadata gambar terperinci. Penggunaan tool ini sangat mudah, cukup drag file yang dipilih ke dalam *tool Exiftool*. [15]

2.9. *Forensically*

Forensik mengacu pada metode dan sumber daya internet yang digunakan untuk analisis citra digital, khususnya dalam konteks analisis forensik digital. Pengguna dapat mengunggah suatu gambar dan memeriksanya menggunakan berbagai fitur dan metode di sisi kanan tampilan Forensik. Forensically menawarkan berbagai pilihan metode pendeteksian mulai dari clone, ELA, noise, scanning, metadata, jpeg analysis dan lain-lain. [16]

3. METODE PENELITIAN

3.1. Objek Penelitian

Objek penelitian dari judul diatas adalah *WhatsApp* yang mana *file image* akan dikirimkan melalui aplikasi *WhatsApp*. Penelitian ini akan mengambil sampel file image dari percakapan yang terjadi diaplikasi *WhatsApp* antara teman ke penulis yang memberikan *file image* yang diduga telah diedit dan penulis akan melakukan analisis digital image forensik untuk memverifikasi keaslian file image tersebut.

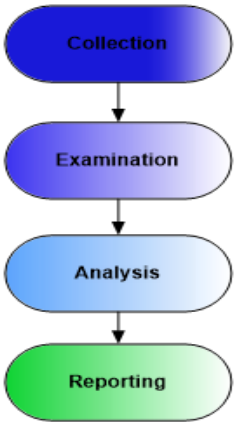
3.2. Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Pengambilan sampel file image dari percakapan di aplikasi *WhatsApp*.
2. Analisis metadata dari *file image* untuk mendapatkan informasi mengenai kamera yang digunakan untuk mengambil foto, waktu dan lokasi pengambilan foto, dan informasi teknis lainnya menggunakan *exiftool*.
3. Analisis *Noise Analysis* untuk mendeteksi perbedaan dari file gambar melalui *forensically*.
4. Analisis *Principal Component Analysis* seberapa terlihat perbedaan yang ada melalui *forensically*.
5. Analisis menggunakan metode *NIST* untuk membuktikan *file image* asli atau telah melalui proses editing, yang dikirimkan melalui aplikasi *WhatsApp*.
6. Pembuatan laporan hasil analisis.

3.3. Metode NIST

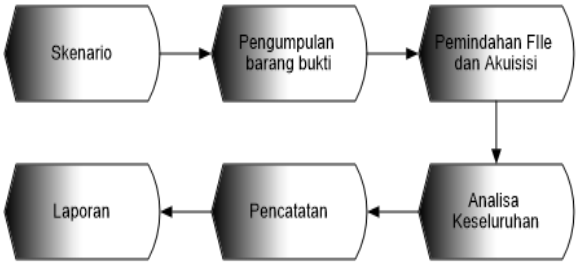
Metode ini didasarkan pada analisis statistik dan matematis pada ciri-ciri yang unik dari *file image*, seperti *noise*, kecerahan, dan kontras. Metode ini memiliki beberapa langkah, yaitu :



Gambar 1. Tahapan Metode NIST

Pada gambar 1 terlihat ada beberapa tahapan dari metode *NIST*. Dimulai dari *Collection* (pengumpulan) yang mana semua barang bukti yang berupa foto-foto yang akan dicek dikumpulkan semuanya. Lalu, dilanjut ketahap *Examination* (pemeriksaan) dengan menggunakan *exiftool* untuk mendapati informasi metadata dari masing-masing foto. Lalu, dilanjut ketahap ketiga yaitu, tahap *Analysis* (analisis) pada tahap ini dilakukan pengecekan secara mendalam dengan menggunakan *tool forensically* untuk mencari perbedaan dari segi warna, gradasi, tekstur serta kontur. Lalu, ditahap terakhir adalah tahap *Reporting* (laporan) yaitu penulisan hasil akhir dari semua foto yang telah dicek dengan beberapa *tools* yang telah disebutkan.

3.4. Rancangan Penelitian



Gambar 2. Tahapan Penelitian

Pada gambar 2 terlihat gambaran bagaimana alur dari penelitian ini berjalan serta terdapat skenario yang akan di jelaskan dalam penelitian ini, sebagai berikut :

Dalam tahapan awal ini akan ada seseorang yang berwirausaha sebuah makanan namun orang yang bersangkutan memiliki kekurangan dalam bidang

pembayaran yang mana orang ini tidak memiliki *M-Banking* sehingga tidak bisa mengecek bukti pembayaran yang sudah masuk atau belum dan hanya menerima bukti pembayaran *via whatsapp*. Orang yang bersangkutan ini merasa ada yang janggal karena merasa banyak transferan yang masuk tetapi seperti sudah melewati tahap edit dan ketika ia melakukan pengecekan ke *ATM*, saldo nya hanya bertambah sedikit, lalu ia tidak yakin bukti foto transferan mana yang sudah melewati tahap edit, sehingga ia meminta bantuan seorang teman untuk membantunya dalam mengecek keaslian dari bukti-bukti foto yang ia terima dari para konsumen nya.

3.5. Alat dan Bahan Penelitian

Tabel 1. Alat dan Bahan Penelitian

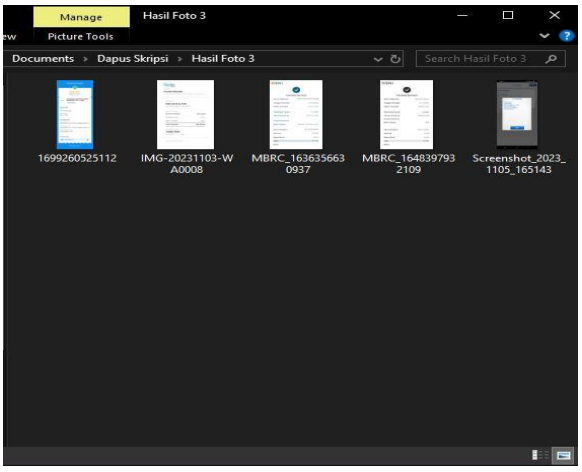
No	Kategori	Spesifikasi
1.	Perangkat Keras	Laptop Lenovo B490
		Handphone Asus Max Pro M1
2.	Perangkat Lunak	Exiftools
		Forensically
		PhotoScapeX
		WhatsApp Web

Pada tabel 1 tertera beberapa alat dan bahan yang dibutuhkan. Terdapat laptop sebagai alat utama untuk penelitian ini, lalu diikuti oleh *handphone* asus sebagai penunjang utama kedua dalam penelitian ini. Lalu ada beberapa perangkat lunak yang digunakan untuk melakukan pengeditan, pengecekan, serta mengakses file gambar yang nanti nya akan dicek keasliannya.

4. HASIL DAN PEMBAHASAN

4.1. Pengumpulan *(collection)*

Dalam tahap ini akan dilakukan tahapan pengumpulan semua bukti-bukti file foto yang akan di cek keasliannya. Semua bukti dari yang bersangkutan akan dipindahkan ke laptop penguji untuk diteliti lebih dalam lagi.



Gambar 3. File yang telah dikumpulkan

4.2. Pemeriksaan *(examination)*

Pada tahap ini akan dilakukan penelitian atau pemeriksaan terhadap file foto yang telah diambil dari *whatsapp* dan telah dipindahkan ke *device* laptop penguji. Dengan bantuan *tools exiftool* akan memudahkan dalam pengecekan terhadap *file-file* foto tersebut.

Gambar 4. Hasil metadata semua file gambar

Pada gambar 4 merupakan hasil metadata dari semua gambar yang telah dicek menggunakan *tools exiftool.* Berikut rincian dari masing-masing gambar :

1. Pada keterangan *exiftool* 1.1, bahwa penguji mendownload *file* tersebut dari *whatsapp* pada tanggal 6 november 2023 pukul 16.28. Lalu, penguji masuk untuk mengakses foto ini melalui *exiftool* pada tanggal 14 Maret 2024. *File* foto tersebut termasuk foto dengan format *PNG*. Foto tersebut memiliki lebar 1080 dan tinggi 2722.
2. Pada keterangan *exiftool* 2 dan 2.1, foto diambil atau dipindahkan pada tanggal 7 November 2023 dan di akses ke *exiftool* pada tanggal 14 Maret 2024. Foto tersebut termasuk kedalam jenis foto JPG. Lalu bisa dilihat bahwa *file* foto tersebut memiliki banyak jenis warna yang masuk kedalam warna RGB dengan banyak rincian dari *red, green, dan blue*. *File* foto tersebut juga memiliki lebar 474 dan tinggi 761 dengan *megapixels* 0.361.
3. Pada keterangan *exiftool* 3, diperoleh pada tanggal 7 November 2023 dan di akses kedalam exiftool pada tanggal 14 Maret 2024. Dengan memiliki *color type RGB with Alpha*. Dan sudah terlihat jelas bahwa foto tersebut telah melalui *software editing canva* dengan judul *"foto hasil 3-1"* dan telah diedit pada tanggal 6 November 2023.
4. Pada keterangan *exiftool* 4, tidak banyak informasi yang didapat dengan *exiftool* maka apakah file tersebut telah melewati proses edit atau belum nanti akan dilanjut kedalam pengecekan lebih lanjut menggunakan *software forensically*.
5. Pada keterangan *exiftool* 5, bahwa tanggal pengambilan foto pada tanggal 6 November 2023 dan diakses ke *exiftool* pada tanggal 14 Maret 2024. Ada keterangan lebih detail lagi yang mana tanggal asli diterima nya pada tanggal 5 November 2023. File foto tersebut masuk kedalam jenis foto JPG.

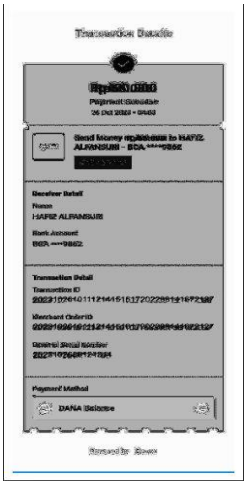
4.3. Analisis *(analysis)*

Pada tahap ini akan dilakukan nya penelitian lebih mendalam karena jika hanya melihat dari segi metadata saja tidak cukup untuk membuktikan file mana yang berisi *editing*. Pada tahap ini peneliti akan menggunakan bantuan dari *Forensically Beta* dan akan berfokus pada *Noise Analysis* dan *Principal Component Analysis.*

Pada tahap ini akan dilakukan pengujian menggunakan *tools forensically* akan digunakan cara *noise analysis* dan *principal component analysis* sebagai berikut :

Gambar 5. Foto pertama dengan *noise analysis*

Pada gambar 5, bahwa dalam menu *Noise Analysis* peneliti membuat skala *noise amplitude* menjadi 75, lalu menceklis *equalize* membuat skala *opacity* 0,95. Karena dengan memilih opsi demikian peneliti dapat dengan mudah melihat perbedaan dari foto tersebut. Setiap gambar mempunyai opsi yang berbeda-beda sampai terlihat perubahannya. Lalu dari hasil nya dilihat bahwa ada perubahan, ada bagian yang mempunyai gradasi warna hitam dan memiliki tingkat tekstur berbeda juga dari daerah lainnya.



Gambar 6. Foto pertama dengan *principal component analysis*

Dengan melihat gambar 6, hasil foto pertama melalui *principal component analysis* bahwa banyak terdapat bayangan dari deret angka yang berada di bagian bawah dari foto. Dan juga banyak terdapat titik buram dari beberapa kata atau angka, sehingga bisa disimpulkan bahwa foto pertama telah diedit.

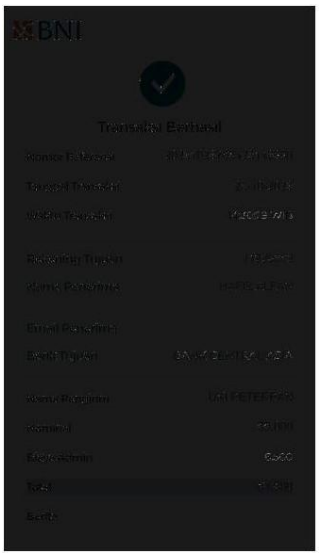
Gambar 7. Foto kedua dengan *noise analysis*

Gambar 7 diatas menggunakan skala *noise amplitude 60* dan *opacity* 0.40 untuk melihat perbedaan dalam foto tersebut, karena perbedaannya baru akan signifikan terlihat dengan skala tersebut. Terlihat bahwa dalam foto ada kata yang masih bagus dan masih dapat dibaca di bagian nama penerima dan nama pengirim. Ada indikasi bahwa file foto ini adalah foto dari transferan orang lain yang diedit nama penerima dan nama pengirimnya.

Gambar 8. Foto kedua dengan *principal component analysis*

Pada gambar 8 merupakan foto kedua yang mana bahwa memang nama pengirim dan nama penerima tetap jelas terbaca disaat yang lainnya *blur*, dikarenakan telah diedit. Dan terlihat juga bahwa total transaksi nya telah diedit karena masih jelas terbaca sama seperti nama pengirim dan nama penerima. Jadi

bisa disimpulkan bahwa foto kedua pun telah melalui tahap *editing.*



Gambar 9. Foto ketiga dengan *noise analysis*

Pada gambar 9, menggunakan skala *noise amplitude* 85 dengan menceklis *equalize histogram* dan dengan *opacity 0.92*, sama seperti lainnya agar perbedaannya terlihat dan lebih jelas. Lalu, terlihat bahwa ada beda ketajaman warna dan tekstur foto di beberapa titik sehingga bisa dilihat sebagai indikasi diedit.

Gambar 10. Foto ketiga dengan *principal component analysis*

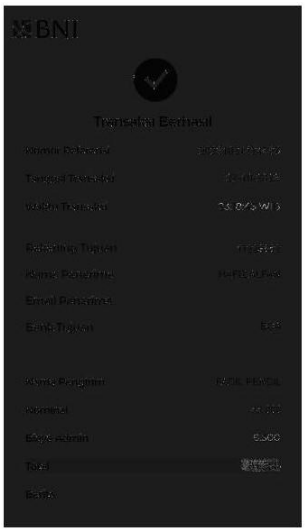
Pada gambar 10, bahwa dalam mode *principal component analysis* ini terdapat banyak warna yang mayoritas dan minoritas. Yang mana warna minoritas nya warna hijau dan hijau nya tidak konsisten melainkan berbeda-beda sehingga bisa disimpulkan bahwa yang berwarna hijau telah diedit. Sehingga foto ketiga ini memang telah melalui tahap edit.

Gambar 11. Foto keempat dengan *noise analysis*

Pada gambar 11 mode *noise analysis* dengan *noise amplitude* skala 85 dan *opacity* di skala 0.67 dengan skala tersebut baru terlihat gradasi dan tekstur dari gambar diatas dan terlihat bahwa file tersebut memiliki tingkat warna yang sama dan gradasi warna yang sama semua, serta memiliki blur yang sama tidak ada perbedaan yang signifikan diantara warna lainnya atau kontur lainnya.

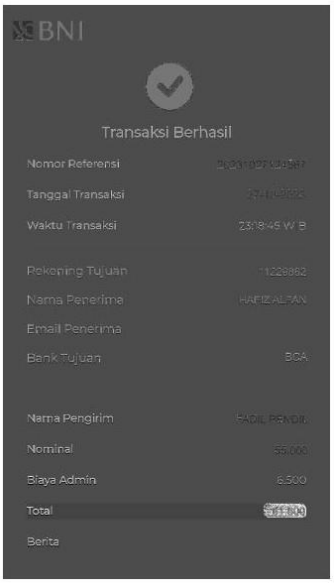
Gambar 12. Foto keempat dengan *principal component analysis*

Pada gambar 12, dengan beberapa opsi yang dipilih, bahwa kontur atau tekstur dari gambar tersebut memiliki tingkat yang rata sama di semua bagian foto. Serta memiliki tingkat blur yang sama pula sehingga bisa diindikasikan bahwa foto ini asli dan tidak ada sentuhan *editing.*



Gambar 13. Foto kelima dengan *noise analysis*

Pada gambar 13, dengan *noise amplitude* 85, tanpa ceklis *equalize histogram*, dan dengan transparansi *(opacity)* 0.93, sehingga dengan skala tersebut perbedaan dari gambar terlihat dan tidak ada ketentuan dari skala-skalanya. Terlihat bahwa ada beberapa titik yang lebih terang, dengan kontur yang berbeda dari lainnya. Dan perbedaan dari gradasi warna lainnya, bisa diindikasi foto kelima ini juga telah diedit.



Gambar 14. Foto kelima dengan *principal component analysis*

Pada gambar 14, bahwa terdapat *editing* dari beda nya gradasi warna pada total transfer yang mana ada blok putih dan juga ada gradasi tidak rata di nama pengirim sehingga bisa disimpulkan bahwa foto kelima ini telah diedit. Lalu pada keterangan total terdapat blok putih yang bertekstur beda dari lainnya yang mana terlihat jelas bahawa ada tahap editing dibagian ini.

4.4. Laporan *(reporting)*

Tabel 2. Laporan hasil penelitian

Keterangan	Metadata	Noise Analysis	Principal Component Analysis	Hasil
Foto Pertama	Non interlace/Deflate	Memiliki bagian yang mempunyai gradasi warna hitam beda dari daerah lainnya	Banyak terdapat bayangandari deret angka yang berada di bagian bawah dari foto	Palsu
Foto Kedua	*JPEG, Baseline DCT, Huffman Coding, sRGB*	Bekas foto transferan orang lain yang diedit nama penerimadan nama pengirim nya	Total transaksi nya telah diedit karena masih jelas terbaca sama seperti nama pengirim	palsu
Foto Ketiga	*PNG, made with canva, deflate*	Ada beda ketajaman warna di beberapa titik sehingga bisa dilihat sebagai indikasi diedi	Adanya ketidakkonsistenan warna dalam satu area yang sama	Palsu
Foto Keempat	*PNG, non interlace, deflate*	Memiliki tingkat warna yang sama, gradasi warna yang sama, serta memiliki blur yang sama	Kontur atau tekstur dari gambar tersebut memiliki tingkat yang rata sama di semua bagian foto.	Asli
Foto Kelima	*JPEG, Baseline DCT, Huffman Coding, Big-Endian*	Ada beberapa titik yang lebih terang dari gradasi warna lainnya	Pada total transfer yang mana ada blok putih dan juga ada gradasi tidak rata di nama pengirim	Palsu

5. KESIMPULAN DAN SARAN

Setelah melakukan penelitian maka dapat disimpulkan bahwa, terdapat file-file yang telah dimanipulasi. Dari 5 file foto yang telah dicek, 4 dari 5 foto tersebut telah melalui pengeditan, dan hanya ada 1 foto yang asli. Lalu, telah ditemukan banyak nya editing foto seperti pengubahan gradasi warna, mengganti kata dengan cara ditiban dan ditutupi, perbedaan dari segi kontur gambar, dan perbedaan ketajaman warna dari beberapa titik bagian foto. Dalam penentuan nilai skala dalam *noise amplitude* dan *equalize histogram* memengaruhi dalam perubahan tingkat ketajaman warna, gradasi warna, tekstur foto serta kualitas foto yang sedang dicek. Jadi sangat membantu penglihatan dalam menentukan adanya bagian-bagian yang telah diedit.

Menggunakan metode *NIST* yang sangat membantu dan efektif dalam menjalankannya, karena

dalam pengujian dan penelitiannya alur dari pengujiannya sangat mudah untuk dijalankan dan diaplikasikan nya. 4. Dalam meningkatkan keamanan dan integritas dalam penggunaan *whatsapp* para pengguna harus lebih sensitif dan teliti dalam melihat file-file foto, video, atau dokumen lainnya agar tidak terjadinya sebuah kerugian.

Saran yang diberikan adalah dengan cara mengkaji ulang dan lebih mendalam ketika menerima file-file yang dikirimkan melalui *whatsapp*, jika dirasa ragu akan adanya pemalsuan atau kerugian baiknya bisa untuk dicek menggunakan beberapa software forensik atau dengan pernagkat lunak laiinya untuk meyakinkan keasliannya. Jika tidak paham bisa meminta bantuan kepada teman atau orang lain yang lebih mengerti.

DAFTAR PUSTAKA

[1] M. Danuri, "Development and transformation of digital technology," *Infokam*, vol. XV, no. II, pp. 116–123, 2019.

[2] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[3] N. Anggraini, S. U. Masruroh, and H. Tiaraningtias, "Analisa Forensik Whatsapp Messanger Pada Smartphone Android," *J. Ilm. FIFO*, vol. 12, no. 1, p. 83, 2020, doi: 10.22441/fifo.2020.v12i1.008.

[4] S. D. Utami, C. Carudin, and A. A. Ridha, "Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[5] S. RACHMIE, "Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website," *Litigasi*, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.

[6] S. N. Aniza and I. Riadi, "Mobile Forensic of Facebook Messenger on Cyber Fraud Case using National Institute of Standard Technology Method," *Int. J. Comput. Appl.*, vol. 183, no. 42, pp. 43–49, 2021, doi: 10.5120/ijca2021921825.

[7] O. AY, "Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence," *J. Forensic, Leg. Investig. Sci.*, vol. 6, no. 1, pp. 1–8, 2020, doi: 10.24966/flis-733x/100045.

[8] A. Firdonsyah and D. Wijayanto, "Analisis Forensik Rekayasa Dokumen Digital dengan Metode NIST," *INFORMAL Informatics J.*, vol. 7, no. 2, p. 121, 2022, doi: 10.19184/isj.v7i2.31198.

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

[10] M. R. Al-fajri, Caruddin, and D. Yusup, "Jurnal Sistem dan Teknologi Informasi Analisis Image Forensic Dalam Mendeteksi Rekayasa File Image Dengan Metode Nist," *J. Sist. dan Teknol. Inf.*, vol. 6, no. 2, pp. 84–90, 2021, [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

[11] C. Karagiannis and K. Vergidis, "Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal," *Inf.*, vol. 12, no. 5, pp. 1–16, 2021, doi: 10.3390/info12050181.

[12] D. Mualfah, Muhammad Iqbal Syam, and Baidarus, "Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ)," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 4, no. 1, pp. 283–292, 2023, doi: 10.37859/coscitech.v4i1.4767.

[13] M. Fitriana, K. A. AR, and J. M. Marsya, "Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.

[14] M. E. Phillips, O. L. Zavalina, and H. Tarver, "Using metadata record graphs to understand digital library metadata," *Proc. Int. Conf. Dublin Core Metadata Appl.*, pp. 49–58, 2019.

[15] M. A. Kustian, "Analisis Forensik Penggunaan Fungsi Hash Dalam Menentukan Keaslian Video, Metadata Image Dan Magic Number File," *J. Sains, Nalar, dan Apl. Teknol. Inf.*, vol. 2, no. 2, pp. 10–16, 2023, doi: 10.20885/snati.v2i2.21.

[16] dan L. H. S. Made Hari Kesuma Arta, I Gede Bagati Kusuma, Muhammad Rial Rasyid Askar, Ida Bagus Gde Kurnia Dyatmika, Dinda Riani, "Analisis Citra Digital Dengan Tools Image Forensic Berupa Fotoforensic, Jpegsnoop, Ghiro, Dan Forensically," pp. 1–16, 2019.