JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 3 No 2 – Oktober 2020 | https://s.id/jurnalresistor
DOI : https://doi.org/10.31598
Publishing : LPPM STMIK STIKOM Indonesia

ANALISIS FORENSIK UNTUK MENDETEKSI KEASLIAN CITRA DIGITAL MENGGUNAKAN METODE NIST

Khairunnisak Nur Isnaini[1], Hamid Ashari[2], Adam Prayogo Kuncoro[3]

[1,2,3]Program Studi Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Purwokerto
Jl. Letjend Pol. Soemarto, Watumas, Purwanegara, Purwokerto Utara, Kabupaten Banyumas, Jawa Tengah , Indonesia

e-mail: nisak@amikompurwokerto.ac.id[1], hamidashari743@gmail.com[2], adam@amikompurwokerto.ac.id[3]

Received : Juli, 2020	Accepted : Oktober, 2020	Published : Oktober, 2020

Abstract

*Currently, the changes in image quality resulting a low-resolution images, faded colors, and so on. This condition potentially attract irresponsible parties to take advantage of the situation for certain purposes. Nowadays, it is very easy for people to manipulate, change, or delete the original information from a digital image thus cause the authenticity and integrity of the image to be doubted. This study is conducted in a specific objective to prove the authenticity of a digital evidence for analysis by providing detailed illustrations of the role of Digital Forensics in accordance with applicable legal regulations in Indonesia using the NIST workflow. The research flow begins with uncovering the background of the problem, collecting data, making scenarios, applying the NIST method, and making conclusions. The illustration used in the scenario is a video inserted into a digital evidence. The video used in this research is the Cyanide Coffee Case with the suspect Wayan Mirna Salihin, happened in August 16, 2016 which was uploaded by Kompas TV channel on Youtube. The NIST analysis phases used several tools: Exiftools, Forevid, and Video Cleaner. The result indicates that all phases in the NIST method are correlated to each other. The result is specifically very clear in the collection phase. The discovery of hidden information causes the examination and analysis process to be more complex especially the extraction process of digital evidence in the form of images. Indeed, the use of various tools are more helpful in disclosing the existing information. This information can be seen from the results of metadata, hash value, and image sharpness from the analyzed digital evidence.****Keywords:*** *Video Forensic, Digital Forensic, NIST, Digital Evidence, Metadata*

Abstrak

Saat ini marak terjadi adanya perubahan kualitas citra yang dihasilkan dari citra yang beresolusi rendah, warna yang pudar, dan lain sebagainya. Kondisi ini memungkinkan pihak yang tidak bertanggungjawab memanfaatkan situasi tersebut untuk kepentingan tertentu. Mudahnya seseorang untuk memanipulasi, merubah, maupun menghapus informasi asli dari sebuah citra digital menyebabkan kualitas citra yang digunakan diragukan keaslian dan integritasnya. Penelitian ini memiliki tujuan khusus untuk membuktikan keaslian sebuah bukti digital untuk di analisa dengan memberikan ilustrasi secara detail peran Digital Forensik dalam mengungkap hasilnya sesuai dengan aturan hukum yang berlaku di Indonesia menggunakan alur kerja NIST. Alur penelitian diawali dari mengungkap latar belakang masalh, pengumpulan data, membuat skenario, menerapkan metode NIST, dan membuat kesimpulan. Ilustrasi yang digunakan pada skenario adalah video yang dimasukkan ke dalam sebuah bukti digital. Video yang digunakan adalah video Kasus Kopi Sianida dengan tersangka Wayan Mirna Salihin tertanggal 16 Agustus 2016 yang diupload oleh Kompas TV dilaman Youtube. Analisis pada tahapan NIST menggunakan

beberapa tools yaitu Exiftools, Forevid, dan Video Cleaner. Hasil yang diperoleh menunjukkan bahwa semua tahap yang ada pada metode NIST merupakan tahap yang saling terkait satu dengan yang lainnya. Hasil sangat terlihat jelas pada tahap koleksi, penemuan informasi yang disembunyikan menyebabkan cara pemeriksaan dan analisis tentu menjadi lebih kompleks yaitu proses ekstraksi dari bukti digital berupa gambar. Tentunya tools yang beragam sangat membantu pengungkapan informasi yang ada. Informasi tersebut terlihat dari hasil metadata, nilai hash, dan ketajaman citra dari bukti digital yang dianalisis.

Kata Kunci: *Video Forensic, Digital Forensic, NIST, Bukti Digital, Metadata*

1. PENDAHULUAN

Citra digital adalah salah satu jenis *digital evidence* yang memiliki risiko perubahan hingga menyebabkan adanya kerusakan dan kehilangan informasi yang sangat tinggi [1] Citra digital adalah sebuah representasi objek yang diolah di dalam perangkat komputer yang diperoleh dari beragam peranglkat digital[2]. Data pada citra digital berisi beragam informasi sehingga di dalam persidangan dan ranah digital forensik, citra digital digunakan sebagai barang bukti.

Perkembangan teknologi saat ini berpengaruh terhadap perkembangan dunia citra digital. Saat ini marak terjadi adanya perubahan kualitas citra yang dihasilkan dari citra yang beresolusi rendah, warna yang pudar, dan lain sebagainya. Kondisi ini memungkinkan pihak yang tidak bertanggungjawab memanfaatkan situasi tersebut untuk kepentingan tertentu. Pembuktian perubahan yang terjadi di dalam sebuah citra digital dapat dilakukan dengan cara penyamaan isi menggunakan pendekatan metadata. Pendekatan metadata ini dimaksudkan untuk mengetahui adanya perbedaan di antara kedua citra yang terlihat sama[2].

Metadata merupakan informasi tambahan yang menyertai dan mendeskripsikan tentang sebuah data tertentu. Sebagai contoh, sebuah video yang memiliki metadata dapat memberi informasi besarnya ukuran file video, kedalaman warnanya, resolusinya, waktu pembuatan, dan yang lainnya. Pada penelitian [3] terdapat perbandingan dua video asli dan editan untuk mengetahui hasil rekaman metadata yang terjadi menggunakan *Exiftools*.

Mudahnya seseorang untuk memanipulasi, merubah, maupun menghapus informasi asli dari sebuah citra digital menyebabkan kualitas citra yang digunakan diragukan keaslian dan integritasnya. Selain itu, saat ini juga telah berkembang banyaknya aplikasi untuk memanipulasi sebuah citra digital dengan mudah tanpa meninggalkan jejak[4]. Namun hal tersebut dapat dibantu oleh ilmu digital forensik.

Digital forensik adalah salah satu cabang ilmu yang bertujuan untuk memproleh informasi dan menyelidiki barang bukti digital agar bisa dipertanggungjawabkan di pengadilan sebagai barang bukti yang sah di mata hukum. Barang bukti digital sendiri berarti hasil dari barang bukti elektronik yang berasal dari *personal computer, mobile phone, notebook, server*, maupun alat bantu teknologi yang dapat dikategorikan sebagai media penyimpanan dan dan dapat dianalaisa sebagai sebuah barang bukti [5]. Bukti Digital yang tersebar luas di media sosial tentunya dapat diindikasikan atau dicurigai dan diragukan keasliannya sebagai bukti digital yang sah di mata hukum perundang-undangan di Indonesia karena terdapat kemungkinan telah dimodifikasi baik isi maupun format lainnya.

Adanya penerapan ilmu digital forensik kepolisian dapat mengidentifikasi, menguji bukti digital tersebut untuk mendukung sebuah kasus di tahap penyelidikan [6]. Setiap kali video dijadikan sebagai barang bukti dalam persidangan pengadilan, tentu harus melalui proses autentifikasi video sebelum menjadi sebuah barang bukti, karena itu video sangat penting untuk dijadikan sebagai sumber utama sebuah informasi. Berbagai jenis perangkat lunak untuk editing video yang saat ini semakin berkembang pesat menyebabkan seseorang atau sebagian orang sulit untuk membedakan antara video asli dan video palsu[7].

Information gathering pada ilustrasi kasus yang akan diangkat penting untuk dilakukan sebagai salah satu langkah dalam menemukan

keaslian dari bukti digital yang ada. *Information gathering* yang perlu dilakukan adalah mendapatkan metadata file, mengetahui hasil video asli setelah mendapat perlakuan seperti menggunakan metode *low light enchancement*, dan informasi yang diperoleh dari *frame by frame video* yang ada. Beberapa *tools* akan digunakan untuk mendukung analisis keaslian bukti digital seperti Exiftool, Forevid, dan Video Cleaner.

Penelitian ini memiliki tujuan khusus untuk membuktikan ketajaman *tools forensic* dalam mengungkap keaslian sebuah bukti digital untuk di analisa dengan memberikan ilustrasi secara detail peran Digital Forensik dalam mengungkap hasilnya sesuai dengan aturan hukum yang berlaku di Indonesia. Tentunya dalam membuktikan keaslian bukti digital tersebut diperlukan metode atau acuan yang tepat agar mendapat hasil yang sesuai dan tepat. NIST (*National Institute of Standards Technology* adalah metode yang seringkali digunakan untuk melakukan analisis untuk mendapatkan informasi terhadap bukti digital [8] zamroni. Tahapan metode NIST antara lain *Collection, Examination, Analysis*, dan *Reporting*. NIST [9] adalah serangkaian panduan yang bertanggungjawab untuk mengembangkan standar dan pedoman untuk memberikan keamanan informasi yang memadai untuk semua operasi dan aset perusahaan.

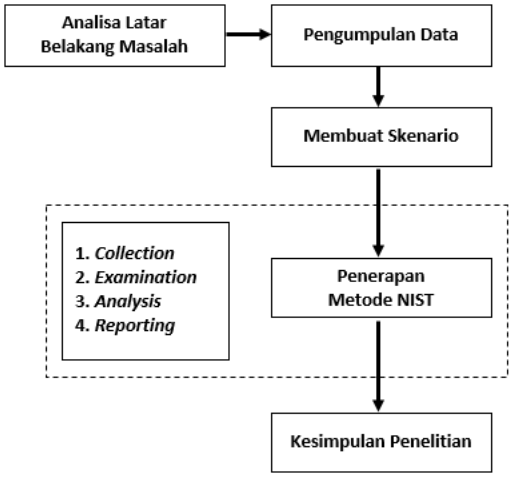
Beberapa penelitian yang terkait antara lain;

1. Penelitian [6] Forensik digital perlu digunakan untuk mendukung penyelidikan dan mencari bukti, menganalisa keaslian barang bukti digital dengan beragam teknik salah satunya dengan metadata dan nilai hash yang dianalisis untuk menghasilkan jawaban yang diungkap di meja persidangan.
2. Penelitian [10] mengungkap bahwa *tools Forevid* dan *Video Cleaner* dapat digunakan untuk menganalisis bukti digital berupa video. Dari kedua *tools* tersebut hasil yang diperoleh adalah nilai hash, hasil metadata, dan citra video *frame by frame* yang dianalisis menggunakan *forensic filter* dari *video cleaner*.
3. Penelitian [11] mengungkap pada penelitiannya menganalisis Aplikasi BeeTalk menggunakan metode NIST. Tools yang digunakan adalah bantuan *tools* MOBILEdit dan OXYGEN *forensic* yaitu *backup* data pada *smartphone* dan bukti *chat*.
4. Penelitian [12] mengungkap hasil yang diperoleh yaitu *smartphone* merk tertentu menjadi dasar analisis pada tahap *collection* dan pada tahap *examination* menggunakan bantuan *tools* untuk *rooting* isi *smartphone* dan OXYGEN *forensic* yaitu *audio*, gambar, dan video.
5. Penelitian [13] mengungkapkan bahwa metode NIST digunakan untuk membandingkan beberapa *tools* untuk kasus *Carving File*. *Tools Scalpel* dianggap lebih baik di antara tools yang lain yaitu *Foremost* dan *Autospy* dalam hal pengembalian *file-file* terhapus, tersembunyi, dan terformat.
6. Pada penelitian yang dilakukan oleh [14] metode NIST digunakan untuk komparasi analisa bukti digital pada *Smartphone* Android dengan mengalisa data kontak, log panggilan, data pesan yang telah di hapus. *Tools* yang digunakan adalah *Wondershare* dan *Oxygen Forensic*.

Pada penelitian sebelumnya hanya membahas perbandingan *tools* untuk membandingkan hasil analisis berupa metadata *file* dan analisis nilai hash, sedang penelitian ini akan membahas penilaian bukti digital berupa video yang dianalisis dari metadata *file*, nilai hash, hasil citra melalui *frame by frame* dan pengaturan kontras gambar untuk membuktikan ada atau tidaknya *tampering file.*

2. METODE PENELITIAN

Metode pelaksanaan penelitian tertuang pada alur penelitian yang tertuang pada gambar 1.



Gambar 2.1. Alur Penelitian

Keterangan pada Gambar 2.1 dijelaskan sebagai berikut.

2.1. Mengungkap Latar Belakang Masalah

Bukti Digital yang tersebar luas di media sosial yang dapat diindikasikan atau dicurigai dan diragukan keasliannya sebagai bukti digital yang sah di mata hukum perundang-undangan Indonesia karena terdapat kemungkinan telah dimodifikasi baik isi maupun format lainnya. Selain itu memberikan ilustrasi secara detail peran Digital Forensik dalam mengungkap hasilnya sesuai dengan aturan hukum yang berlaku di Indonesia menggunakan tools dan teknik-teknik video forensik.

2.2. Pengumpulan data

Pada tahap ini peneliti mengumpulkan beberapa paper baik dari jurnal, prosiding, buku maupun sumber data lainnya terkait metode, *tools*, maupun teknik-teknik video forensik yang diterapkan pada bukti digital. Dan membuat roadmap penelitian dari studi kasus sejenis.

Data yang digunakan adalah data sekunder dikarenakan pada penelitian ini akan menggunakan sebuah ilustrasi pada skenario yang telah dirancang sebelumnya. Data yang menjadi ilutrasi pada skenario adalah video Kasus Kopi Sianida dengan tersangka Wayan Mirna Salihin tertanggal 16 Agustus 2016 yang diupload oleh Kompas TV dilaman Youtube dengan tautan sebagai berikut : https://www.youtube.com/watch?v=HBElNG46RJs

2.3. Membuat Skenario

Peneliti membuat skenario kasus untuk membuktikan keaslian bukti digital berupa video yang disematkan pada sebuah gambar dengan teknik-teknik dan tools forensik yang ada.

2.4. Menerapkan metode NIST

a. Collection

Tahap ini merupakan proses identifikasi, pelabelan, perekaman dan pengambilan data dari sumber data yaitu video yang tersebar dengan barang bukti berupa *flashdisk*.

b. Examination

Tahap examination adalah tahap pemrosesan data yang dikumpulkan secara digital forensik menggunakan kombinasi dari berbagai skenario, baik otomatis maupun manual. Pada tahap ini akan dilakukan pengecekan isian dari barang bukti digital berupa video di dalam gambar dari tool yang disediakan yaitu Exiftools serta menilai proses hashing dari barang bukti tersebut. Exiftools digunakan untuk mengetahui hasil metadata secara umum dan nilai hash.

c. Analysis

Tahap ini dilakukan proses analisis dari hasil pemeriksaan bukti digital berupa video dari hasil yang sudah diketahui seperti metadata dan nilai hash. Pada tahap ini tool yang digunakan adalah Forevid dan Video Cleaner. Forevid digunakan untuk mengetahui hasil metadata khusunya dari file yang berbetuk video dan Video Cleaner digunakan untuk mengetahui adanya tidaknya tampering file yang dinilai dari kontras, kecerahan, dan lain sebagainya.

d. Reporting

Tahap ini melakukan bentuk pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan yaitu analisis menggunakan metode NIST, penjelasan mengenai alat dan prosedur yang dipilih, memberikan rekomendasi untuk perbaikan kebijakan, prosedur, alat, dan aspek lain dari proses digital forensik.

2.5. Membuat Kesimpulan

Membuat kesimpulan secara lengkap dari uraian tahapan-tahapan NIST yang telah diterapkan untuk analisis video forensik guna membuktikan keabsahan bukti digital.

3. HASIL DAN PEMBAHASAN

3.1 Membuat Skenario

Skenario dibuat dengan tujuan untuk mengetahui ketajaman *tools forensic* dalam menganalisa sebuah barang bukti digital. Langkah-langkah tersebut terdiri dari:

a. Menyediakan sebuah bukti digital berupa gambar yang berisi video.
b. Gambar tersebut di analisis menggunakan tools *image forensic*.
c. Di dalam gambar tersebut terdapat sebuah informasi yang mengarah pada isian gambar berupa video.
d. Video yang terdapat pada gambar akan dianalisa keasliannya menggunakan tools *forensic video*.
e. Membuat kesimpulan terhadap manfaat dari tools yang digunakan berdasarkan hasil analisa skenario kasus.

Skenario dibuat seolah-olah seorang informan (anonim) akan memberikan informasi valid dan rahasia kepada pihak kepolisian sehingga diperlukan teknik khusus untuk membuat informasi tersebut agar terlihat biasa melalui bukti digital (gambar) yang ditemukan. Barang bukti digital tersebut tersimpan di dalam sebuah *flashdisk* yang dikirim ke kantor polisi. Perlunya penyampaian informasi dengan cara tersebut untuk menjaga kualitas keaslian dari banyaknya informasi hoax yang beredar melalui dunia maya seperti sosial media terkait isu yang sedang berkembang dan mengungkap pelaku kejahatan yang terdapat pada isian informasi tersebut. Sehingga diperlukan *forensic analysis* untuk membuka informasi utama tersebut.

3.2 *Applying NIST Method*

a. Proses Koleksi / *Collection*

Barang bukti terdapat dalam flashdisk dalam bentuk *imaging file*.

Gambar 3.1. Indikasi Barang Bukti Digital

Ekstensi yang digunakan dari barang bukti yang ditemukan adalah ".jpg" selanjutnya adalah melakukan penilaian hash yang dapat dilhat pada gambar 3.1.

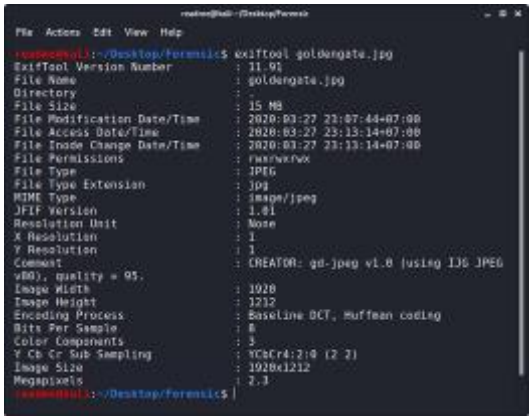
Name	goldengate.jpg
Size	15475451 bytes (14 MiB)
CRC32	31983B04
CRC64	C7629A1D824E0A0F
SHA256	F7BDEF268469DCD7D75F809DEFCC414AA10ABA9A0EA19ECEF374050B8085976B
SHA1	C05854FF965EEB24E220033B8CBC77C29CB348DC
BLAKE2sp	9C6279DCDC73FBB3F2CC2EC5FA520ADC6780D64ECC5F4F81593B9552E95E723A

Gambar 3.2. Nilai Hash

Proses hashing dilakukan untuk menerima masukan string yang panjangnya sembarang dan konversi string yang dihasilkan memiliki panjang yang tetap. Algoritma yang digunakan pada kasus ini adalah CRC32, CRC64, SHA256, SHA1, dan BLAKE2sp sesuai pada gambar 3.2.

b. Proses Pemeriksaan

Tahap ini dilakukan pemeriksaan *Image File* dengan maksud mendapatkan data yang mendukung. Data yang dimaksud adalah semua komponen yang ada di dalam *Image File* yang diberi nama "goldengate" yang berekstensi ".jpg" menggunakan aplikasi *Exiftool* dan pembacaan strings.



Gambar 3.3. Hasil Pembacaan dari Aplikasi *Exiftools*

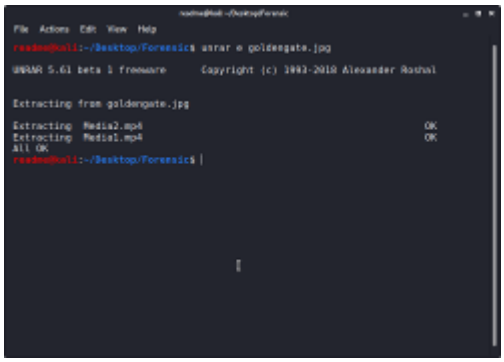
Gambar 3.4. Hasil Pembacaan dari *Strings*

Hasil pemeriksaan dengan menggunakan *Exiftool* dan pembacaan strings ditemukan beberapa kejanggalan dimana ukuran file yang terlalu besar yaitu 15 MB dengan ukuran image 1920x1212 dan informasi file yang terkandung di dalamnya berekstensi .mp4. Pada gambar 3.3 dan 3.4 dapat dilihat hasil pembacaan dari aplikasi Exiftools dan pembacaan strings.

c. Proses Analisis

Dari hasil yang didapat pada pemeriksaan, tahap selanjutnya dilakukan ekstraksi *file* yang terkandung didalam *image file*. Saat melakukan ekstraksi, tidak ada *file* yang terenkripsi sehingga *file* yang ditemukan sebelumnya dapat dipisahkan dengan mudah.

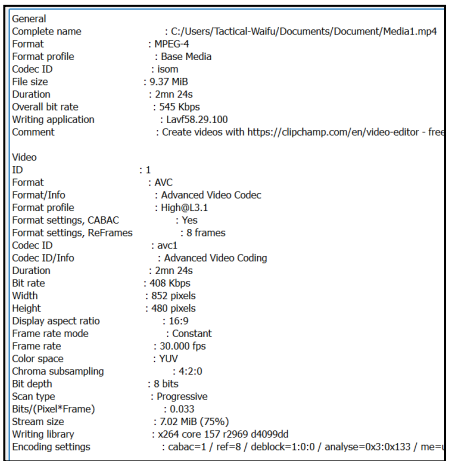
Dilanjutkan dengan melakukan analisa pada *file* .mp4 yang ditemukan untuk mencari data-data yang mendukung sebagaimana terlampir pada gambar 3.5.



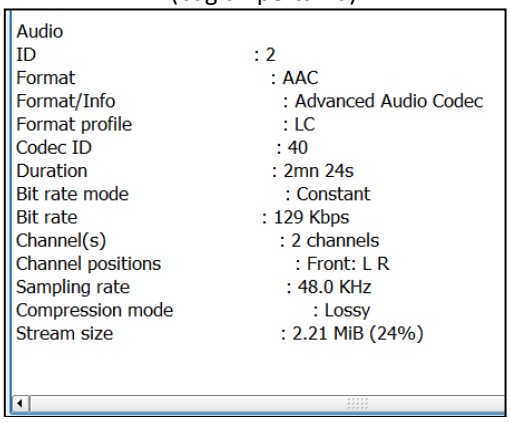
Gambar 3.5. Proses Ekstraksi File

Menurut hasil pemeriksaan diindikasikan bahwa di dalam file gambar terdapat file lain sehingga harus diekstraksi dan menghasilkan file ber-ekstensi ".mp4" yang tersaji pada gambar 3.5. pada gambar 3.5 hasil ekstraksi menunjukkan adanya 2 file video yaitu media1.mp4 dan media2.mp4.

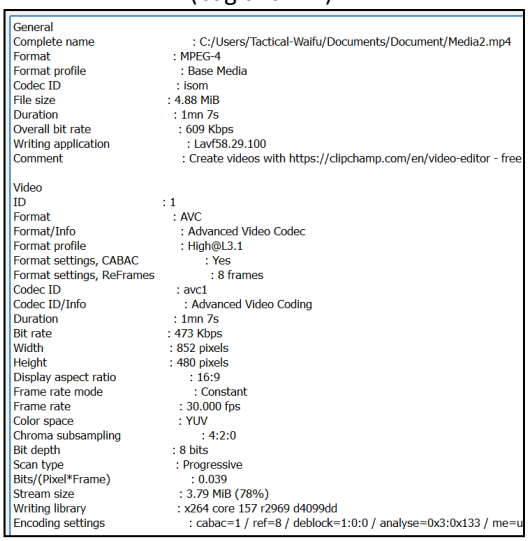
Tahapan selanjutnya adalah analisis metadata file yang telah ditemukan. Metadata merupakan informasi terstruktur agar mudah untuk dibaca. Hasil metadata tersebut terdapat pada gambar 3.6 hingga 3.9.



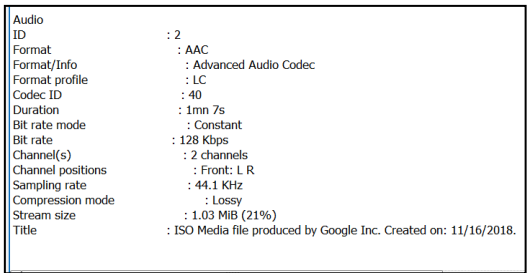
Gambar 3.6. Hasil Metadata pada media1 (bagian pertama)



Gambar 3.7. Hasil Metadata pada media1 (bagianakhir)



Gambar 3.8. Hasil Metadata pada media2 (bagian pertama)



```
Audio
ID                                       : 2
Format                                   : AAC
Format/Info                              : Advanced Audio Codec
Format profile                           : LC
Codec ID                                 : 40
Duration                                 : 1mn 7s
Bit rate mode                            : Constant
Bit rate                                 : 128 Kbps
Channel(s)                               : 2 channels
Channel positions                        : Front: L R
Sampling rate                            : 44.1 KHz
Compression mode                         : Lossy
Stream size                              : 1.03 MiB (21%)
Title                                    : ISO Media file produced by Google Inc. Created on: 11/16/2018.
```

Gambar 3.9. Hasil Metadata pada media2 (bagian kedua)

Lampiran gambar 3.6, gambar 3.7, gambar 3.8, gambar 3.9 merupakan hasil dari analisis barang bukti yang ditemukan menunjukan adanya perubahan. Hal tersebut ditunjukan dengan adanya sebuah komentar bertuliskan "https://clipchamp.com/" yang merupakan penyedia layanan editor video berbasis *online*. Analisis ini dilakukan menggunakan program Forevid.

Tahap analisis selanjutnya menggunakan tools *Video Cleaner* dengan tujuan untuk peningkatan kualitas video. *Sample video* yang dipakai adalah video yang berisi tulisan namun memiliki pencahayaan yang sangat buruk, sehingga perlu dilakukan peningkatan kualitas video untuk mendapatkan informasi dari video tersebut. Langkah analisis diawali dengan membuka video tersebut ke *video cleaner*. Selanjutnya menghidupkan *"apply TOOLS settings"* agar semua perubahan yang dilakukan dapat terlihat hasilnya. Langkah selanjutnya yaitu menghidupkan pengaturan "Histogram" agar warna video tampak lebih cerah. Setelah itu, menajamkan detail *per frame* agar terlihat sedikit lebih natural.

Pada video cleaner diaktifkan mode metode *low light enchanment*.

Gambar 3.10. Frame 405 pada Media2 sebelum diubah

Gambar 3.11. Frame 405 pada media2 setelah diubah

Pada gambar 3.10 merupakan gambar sebelum diberikan metode metode *low light enchanment*. Pada tahap ini diterapkan metode tersebut yang didapat darii *frame by frame video* yang ditemukan menggunakan tools *Video Cleaner* yang dapat dilihat pada gambar 3.10. Perbedaannya pun dapat dilhat pada gambar 3.11.

Langkah berikutnya yaitu menambahkan kontras.

Gambar 3.1. Media1 Frame 4274

Gambar 3.23. Frame 4274 sebelum diubah

Gambar 3.14. Tools yang diaktifkan pada Video Cleaner

Pengaturan kontras pada gambar 3.13 bertujuan untuk mengetahui perbedaan warna gelap dan warna cerah lebih dapat terlihat. Sehingga terdapat perbedaan yang cukup jelas pada frame 4274 yang dapat dilihat gambar 3.12. Dan secara umum pengaturan pencahayaan pada Video Cleaner terlihat apda gambar pada gambar 3.14.

Pada tahap analisis selanjutnya yaitu menghidupkan fitur "apply FORENSIC settings" dan menambahkan "sobel edge" .

Gambar 3.15. Hasil Perubahan menggunakan SobelEdge

Gambar 3.16. Pengaturan Sobel Edge pada Video Cleaner

Pengaturan "apply forensic settings" dan pengaturan sobel edge bertujuan untuk membuat hasil gambar menjadi lebih halus, namun warna menjadi hijau dengan tujuan untuk dapat menganalisa kejanggalan pada *image* atau citra digital secara "*per frame*". Dan hasil pengaturan tersebut terlihat pada gambar 3.15 Pengaturan sobel edge dapat dilihat pada gambar 3.16.

d. Reporting

Berdasarkan apa yang telah dilakukan pada image file dengan nama "goldengate" yang berekstensi ".jpg" memiliki file lain yang sehingga perlu diekstraksi untuk menemukan file yang ada di dalamnya. Terdapat dua file tambahan yang tersimpan yaitu "Media1.mp4" dan "Media2.mp4" yang merupakan sebuah video yang sudah mengalami perubahan didalamnya berdasarkan metadata yang ditemukan yaitu sebuah komen yang menunjuk kepada alamat website "https://clipchamp.com/" dan *watermark* yang dapat mudah ditemukan menggunakan *low light enchanment* bertuliskan "clideo.com".

Sehingga dapat menjadi pembuktian bahwa terdapat proses editing pada file bukti digital yang dalam penelitian ini adalah file berjenis video dengan format mp4. *Tools* forensic yang digunakan berhasil membantu proses identifikasi terhadap file video tersebut terutama untuk mengungkap detail isian file dengan nilai hash dan metadata serta mengungkap lebih jelas isi bukti digital sesungguhnya yang di analisis dengan mengaktifkan *forensic tools* di dalam Video Cleaner terutama untuk mengidentifikasi adanya indikasi perubahan dengan metode *frame by frame.*

4. KESIMPULAN

Kesimpulan yang dapat diperoleh dari hasil penelitian ini adalah bahwa *tools* yang digunakan dalam proses identifikasi forensic terhadap file video (analisis citra digital) terbukti efektif digunakan. Bahkan penerapan metode NIST pun dapat diterapkan sebagai salah satu acuan standar dalam proses pembuktian sebuah file elektronik yang terindikasi sebagai bukti digital. Hal tersebut dapat terlihat pada tahapan metode NIST terutama pada tahap pemeriksaan dan analisis.

Peneliti memberikan saran untuk penelitian berikutnya yaitu penerapan metode video forensik selain NIST serta aplikasi pendukung pembuktian bukti digital masih memungkinkan untuk diimplementasikan. Sehingga dapat diperoleh keragaman cara pencarian bukti digital pada artefak data.

PERNYATAAN PENGHARGAAN

Peneliti menghaturkan ucapan terima kasih kepada kampus Universitas AMIKOM Purwokerto dan lembaga LPPM, yang menjadi sponsor sehingga penelitian ini terealisasi.

DAFTAR PUSTAKA

[1] H. Wijayanto, I. A. Prabowo, and P. Harsadi, "Optimalisasi Penyusutan Exif Metadata Dengan Teknik Substitusi Null Value Pada Kasus Keamanan Citra Digital," *J. Ilm. SINUS*, vol. 16, no. 1, p. 1, 2018.

[2] A. Apriliani and K. Hijjayanti, "Menggunakan Exif Metadata," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 5, no. 1, 2020.

[3] A. I. Putra, R. Umar, and A. Fadlil, "Analisis Forensik Deteksi Keaslian Metadata Video Menggunakan Exiftool," in *Seminar Nasional Informatika*, 2018, vol. 1, no. 1, pp. 21–25.

[4] W. Yuli Sulistyo, I. Riadi, A. Yudhana, A. Dahlan, P. Studi Teknik Elektro, and U. Ahmad Dahlan Jalan Soepomo, "Analisis Deteksi Keaslian Citra Menggunakan Teknik Error Level Analysis Dengan Forensicallybeta," in *Seminar Nasional Informatika (SEMNASIF)*, 2018, vol. 2018, no. November, pp. 154–159.

[5] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android," *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2018.

[6] G. Hendita, A. Kusuma, and I. N. Prawiranegara, "Analisa Digital Forensik Rekaman Video CCTV dengan Menggunakan Metadata dan Hash," in *Prosiding Seminar Nasional Sistem Informasi dan Teknologi (SISFOTEK)*, 2019, vol. 3, no. 1, pp. 223–227.

[7] C. Feng, Z. Xu, W. Zhang, and Y. Xu, "Automatic location of frame deletion point for digital video forensics," in *IH and MMSec 2014 - Proceedings of the 2014 ACM Information Hiding and Multimedia Security Workshop*, 2014, pp. 171–179.

[8] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 949–955, 2018.

[9] K. Kent, S. Chevalier, T. Grance, and H. Dang, *Guide to Integrating Forensic Techniques into Incident Response*. 2006.

[10] R. Umar, A. Fadlil, and A. I. Putra, "Analisis Forensics Untuk Mendeteksi Pemalsuan Video," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 3, no. 2, p. 193, 2019.

[11] M. I. Syahib, I. Riadi, and R. Umar, "Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan," in *Seminar Nasional Informatika 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 November 2018*, 2018, vol. 2018, no. November, p. 134.

[12] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, p. 13, 2018.

[13] D. T. Yuwono, A. Fadlil, and S. Sunardi, "Performance Comparison of Forensic Software for Carving Files using NIST Method," *J. Teknol. dan Sist. Komput.*, vol. 7, no. 3, p. 89, 2019.

[14] U. S. Rusydi, "METODE NIST UNTUK ANALISIS FORENSIK BUKTI DIGITAL PADA PERANGKAT ANDROID," in

Prosiding SENDI_U 2019, 2019, no. 1998, pp. 978–979.