DOI: https://doi.org/10.51903/elkom.v17i1.1563

JURNAL ILMIAH ELEKTRONIKA DAN KOMPUTER, Vol.17, No.1, Juli 2024, pp.88-95
p-ISSN : 1907-0012 (print)
e-ISSN : 2714-5417 (online)
http://journal.stekom.ac.id/index.php/elkom · page 88

Analisis Rekaman Video CCTV Dengan Teknik Enhancement Menggunakan Metode National Institute Of Justice (NIJ)

Erick Irawadi Alwi[1], Siska Anraeni[2]
[1,2]Program Studi teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia
Jl. Urip Sumoharjo Km. 5 Gedung Menara UMI lantai 3, (0411)428075, e-mail: erick.alwi@umi.ac.id, siska.anraeni@umi.ac.id

ARTICLE INFO

Article history:

Received September 29, 2023
Received in form 2 Oktober 2023
Accepted 7 Desember 2023
Available online 1 Juli 2024

ABSTRACT

Crime and criminality are increasing by utilizing electronic and digital devices, such as CCTV (closed circuit television) security devices, smartphones, and other electronic devices that have video features, record and store perpetrator data. CCTV recording files are sometimes unclear, so video forensic software is needed to clarify the object so that it can be used as evidence in court. The method used in this research is the National Institute of Justice (NIJ) method and enhancement techniques to clarify the image frame objects of CCTV video recordings using Amped Five forensic image and video tools. The results of the analysis of the evidence concluded that they had succeeded in identifying the vehicle number plate of the alleged perpetrator by carrying out an enhancement process (improving the quality) of the image object. The enhancement process is carried out by utilizing the optical debluring feature of the amped five forensic video software, in settings by increasing the size from 1 to 2 and increasing the noise value from 0.0100 to 0.6310 so it looks clearer than before.

Keywords: *Video, Forensic, CCTV, Enhancement, National Institute of Justice (NIJ)*

1. Introduction

Keamanan merupakan salah satu aspek yang harus dijaga dalam kehidupan masyarakat saat ini, semakin meningkatnya kasus kriminal seperti pencurian, perampokan baik dilingkungan rumah, toko maupun perkantoran diperlukan mekanisme untuk meningkatkan keamanan. Berbagai cara dapat dilakukan untuk meningkatkan keamanan, salah satunya dengan memasang kamera pemantau atau yang biasa disebut CCTV (Closed Circuit Televison) yang digunakan sebagai alat kamera pengawas. CCTV terdapat sebuah file rekaman video yang dapat digunakan sebagai alat bukti digital dalam pengungkapan suatu perkara peradilan [1], untuk itu diperlukan perlakuan khusus dalam memperoleh rekaman video tersebut agar terjaga keutuhan dan keasliannya [2], untuk menjaga keutuhan dan keaslihan barang bukti di perlukan penerapan ilmu digital forensik dalam investasi kejadian suatu perkara. Ilmu digital forensik merupakan praktik pembedahan perangkat digital untuk mencari fakta yang diperlukan untuk kepentingan hukum, berbeda dengan ilmu forensik lainnya yang lebih banyak berkaitan dengan pembedahan dan pencarian artefak pada makhluk hidup [3]. Digital forensic memiliki dua kategori alat bukti berupa bukti fisik dan bukti digital. Istilah lain bukti fisik dan bukti digital disebut sebagai bukti elektronik dan bukti digital,

Received September 29, 2023; Received Oktober 2, 2023; Accepted December 8, 2023

dimana alat bukti elektronik memiliki bentuk fisik dan bentuk yang dapat dilihat visual, seperti personal komputer, smartphone, kamera, hard disk dan lain-lain [4][5], sedangkan alat bukti berupa digital merupakan alat bukti yang diekstrak atau diperoleh kembali dari alat bukti elektronik bisa berupa file, email, pesan, gambar, video, log maupun teks [6].
Terkadang alat bukti berupa rekaman CCTV di beberapa frame kurang jelas atau blur sehingga menyulitkan penegak hukum untuk mengidentifikasi rekaman video gambar yang tidak jelas atau tidak fokus karena buruknya kualitas rekaman tersebut. Contoh kasus digital forensik yang menyulitkan penegak hukum mengidentifikasi seperti kasus kamera CCTV pada kasus novel baswedan penyiraman air keras dikarenakan buruknya kualitas rekaman video CCTV yang berada di sekitar TKP. Dengan permasalahan tersebut peneliti akan melakukan analisis video rekaman CCTV yang kurang jelas atau blur dengan teknik video forensik menggunakan metode National Institute of Justice (NIJ).

2. Research Method

Pada penelitian ini mengadaptasi dan mengimplementasikan metode analisa forensik dari National Institute of Justice (NIJ). Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Menurut Anggara disebutkan melakukan teknik forensik dan analisa forensik berdasarkan metode yang benar akan memiliki keberhasilan mendekati 100% dalam mengumpulkan data forensik [7]. Tahapan pada penelitian ini dapat digambarkan seperti pada Gambar 1

Gambar 1. Tahapan Metode National Institute of Justice (NIJ)

Tahapan metode dari National Institute of Justice (NIJ) ini terbagi menjadi lima tahapan yakni Identification, Collection, Examination, Analysis, dan Reporting [8], adapun penjelasan tahapannya sebagai berikut:

1. Identification

Tahap identifikasi merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses identifikasi, pelabelan, perekaman, untuk menjaga keutuhan barang bukti.

2. Collection

Tahap pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan.

3. Examination

Tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa file tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada file digital perlu dilakukan identifikasi dan validasi file dengan teknik hashing.

4. Analysis

Tahapan Analisis dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut.

Hasil analisis terhadap data digital selanjutnya disebut digunakan sebagai barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

5. Reporting

Tahapan pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tool, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, tool, atau aspek pendukung lainnya pada proses tindakan digital forensik.

3. Results and Analysis

3.1. Simulasi kasus

Simulasi kasus dalam penelitian ini berupa kasus pencurian dimana plat motor terduga pelaku terekam CCTV disekitar TKP hanya saja rekamannya yang diperoleh tidak jelas atau blur sehingga sulit mengidentifikasi plat kendaraan bermotor terduga pelaku.

Alat yang dibutuhkan dalam penelitian ini yaitu terdiri dari perangkat lunak dan perangkat keras untuk memperoleh alat bukti digital seperti pada Tabel 1 dibawah ini.

Tabel 1. Perangkat keras dan Perangkat Lunak

No	Alat Penelitian	Deskripsi
1	Wifi CCTV	EZVIZ Model CS-H8c (1080P)
2	Laptop	AMD Ryzen 5 4600H with Radeon Graphics, 16 GB RAM
3	Amped FIVE	Software image and video forensic
4	Hash Generator	Software hashing
5	HashMyFile	Software hashing
6	FTK Imager	Software akusisi
7	EZGIF.COM	Tools extrac video menjadi frame online
8	Flash Disk 16 GB	Media Penyimpanan

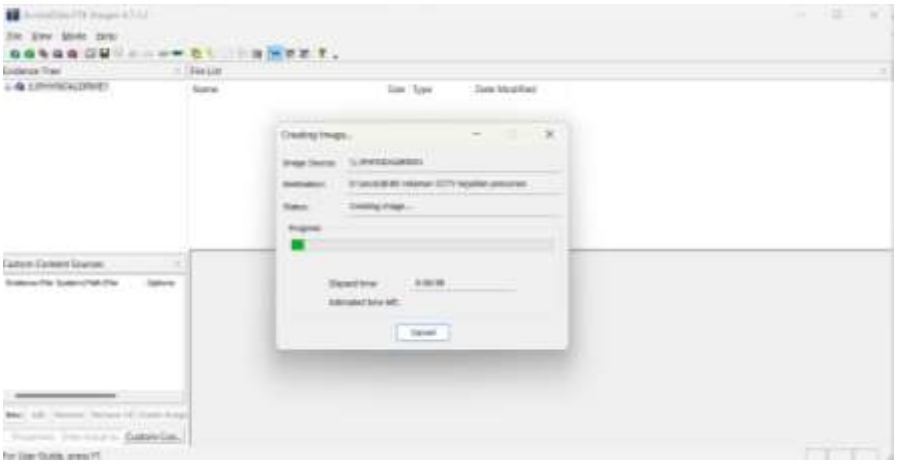
3.2. Identification

Tahapan idenfikasi pada penelitan yaitu pencarian barang bukti apa yang berada di TKP dan sekitarnya yang dapat menjadi petunjuk bagi penegak hukum. Penegak hukum akan mengidentikasi barang bukti berupa kamera cctv di TKP, media penyimpanan cctv berupa micro sd dan format file rekaman tersebut sebelum dilanjutkan pada proses collection atau tahap pengumpulan barang bukti

Gambar 2. CCTV EZVIZ H8c

3.3. Collection

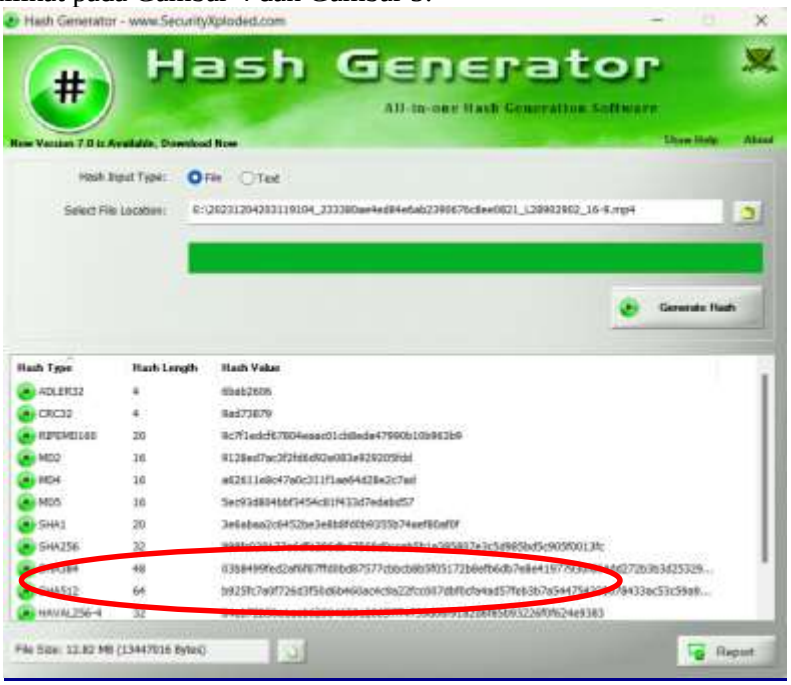
Collection merupakan proses pengumpulan barang bukti yang relevan untuk mendukung penyidikan. Tahapan colectioan biasanya dilakukan proses akusisi dalam hal ini melakukan penggandaan atau imaging terhadap sumber data (penyimpanan data cctv) dengan mengcopy secara presisi satu banding satu atau bit by bit copy menggunakan FTK imager.



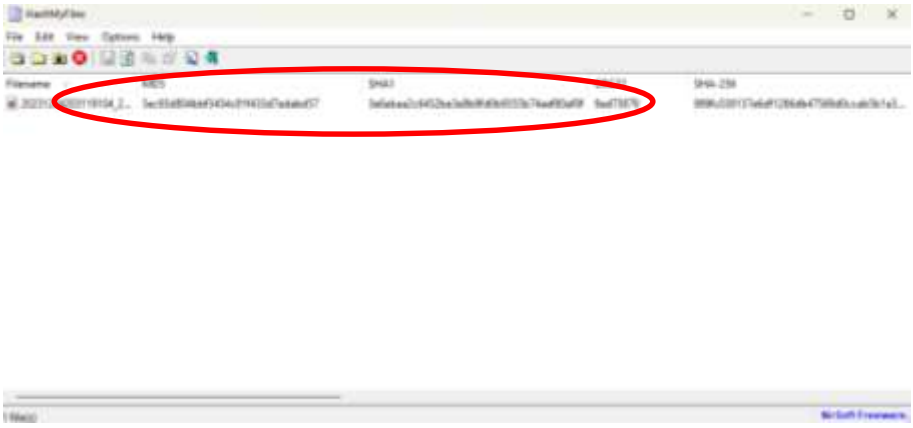
Gambar 3. Proses Akusisi Bukti rekaman CCTV oleh tool FTK Imager

3.4. Examination

Pada tahapan examination, hasil cloning atau penggandaan barang bukti file digital akan dilakukan pemeriksaan keaslian file rekaman cctv tersebut yang diperoleh dari TKP. Pemeriksaan keaslian file rekaman menggunakan teknik hashing. Fungsi mengetahui nilai hash diimplementasikan untuk kepentingan identifikasi dan otentifikasi bukti digital. Fungsi hash digunakan untuk menjaga integrity karena perubahan pada file 1 (satu) bit saja akan mengubah nilai hashnya. Nilai hash file rekaman CCTV kejadian pencurian di uji menggunakan 2 tools hashing yaitu Hash Generator HashMyFile dan menghasilkan nilai MD5 dan SHA yang sama. Adapun nilai hash dari 2 tools tersebut dapat dilihat pada Gambar 4 dan Gambar 5.



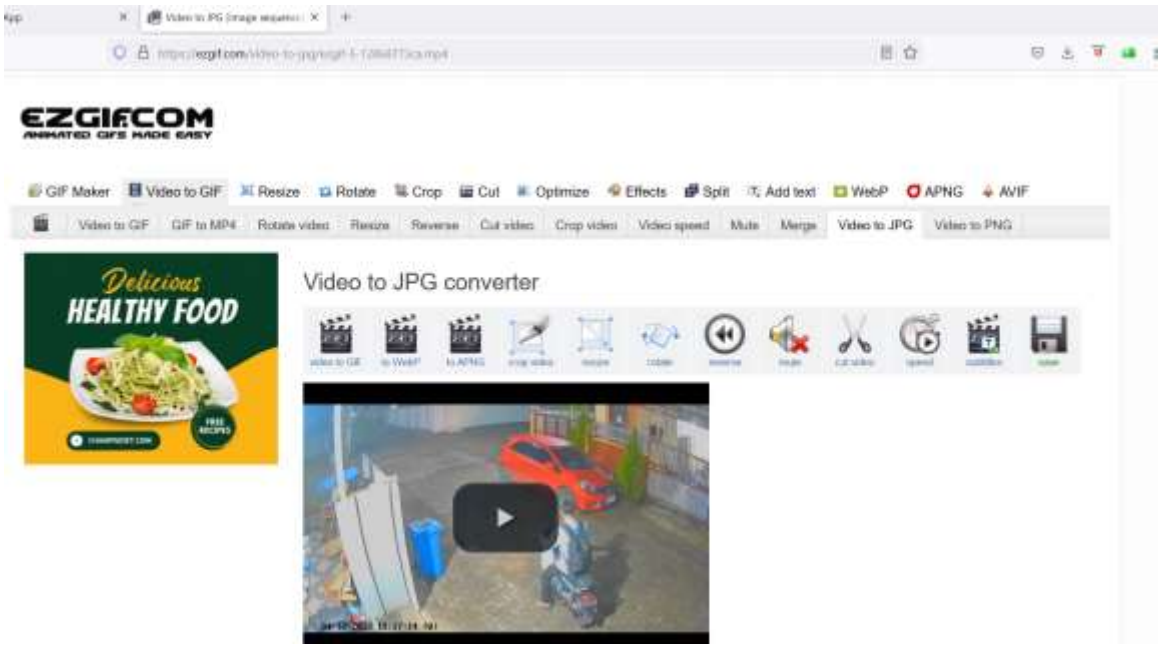
Gambar 4. Nilai Hash MD5 dan SHA1 dari Hash Generator



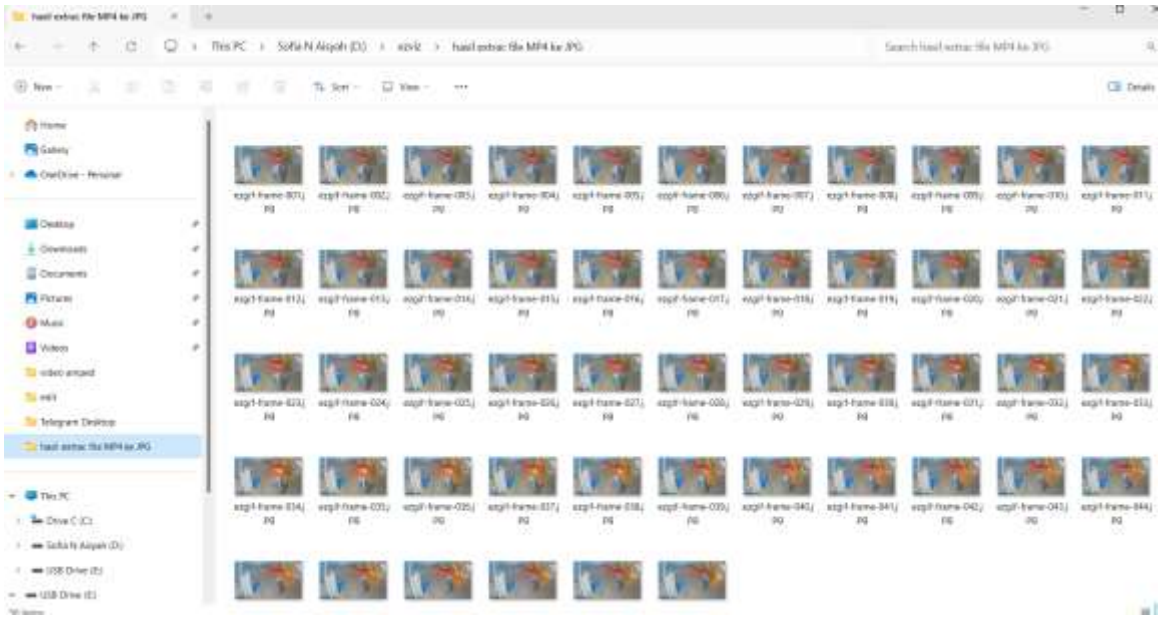
Gambar 5. Nilai Hash MD5 dan SHA1 dari HashMyFiles

3.5. Analysis

Pada tahap ini setelah dilakukan penggandaan barang bukti dan pemeriksaan keaslian barang bukti pada tahap sebelumnya, selanjutnya dilakukan analisis terhadap file rekaman video yang kurang jelas atau blur dengan cara terlebih dahulu rekaman video diekstraksi frame-frame dari rekaman tersebut menjadi gambar – gambar berformat jpg dengan tools online ezgif.com dapat dilihat pada Gambar 5 dan Gambar 6, kemudian gambar- gambar tersebut diseleksi untuk mencari gambar yang mana yang menunjukkan kualitas objek yg paling baik dibandingkan gambar lainnya. Apabila gambar yang diperoleh belum memuaskan, maka objek gambar tersebut di tingkatkan terlebih dahulu kualitasnya (Enhancement) dengan tools image dan video forensic Amped memanfaatkan fitur optical debluring seperti terlihat pada Gambar 7.



Gambar 6. Proses Convert dari rekaman CCTV ke Gambar format jpg



Gambar 7. Hasil ektraksi dari video ke gambar berformat jpg

Gambar 8. Hasil ektraksi dari video ke gambar berformat jpg

3.5. Reporting

Setelah melakukan analisis terhadap barang bukti disimpulkan bahwa telah berhasil mengidentifikasi plat nomor kendaraan terduga pelaku dengan dilakukan enhancement (peningkatan kualitas) objek gambar. Proses enhancement dilakukan dengan memanfaatkan fitur optical debluring dari software video forensik Amped FIVE, pada settingan dengan menaikkan size dari 1 ke 2 dan menaikkan nilai noise dari 0.0100 ke 0.6310 untuk memperjelas objek yang tidak jelas (blur).

Sebelum proses Enhancement	Sesudah proses Enhancement

Gambar 9. Hasil dari proses enhancement menggunakan tool Amped FIVE

Gambar 10. Plat Nomor Kendaraan teridenfikasi setelah dilakukan enhancement

4. Conclusion

Penelitian ini berhasil menganalisis bukti rekaman cctv yang tidak jelas (blur) menjadi tampak jelas untuk dapat mengidentifikasi plat kendaraan bermotor dari terduga pelaku dengan mengikuti metode analisis National Institute of Justice (NIJ) dalam pemeriksaan barang bukti digital. Analisis gambar yang tidak jelas menggunakan filter optical debluring tools amped five dengan dengan menaikkan size dari 1 ke 2 dan menaikkan nilai noise dari 0.0100 ke 0.6310 sehingga tampak lebih jelas dari sebelumnya.

References

[1] G. Hendita, A. Kusuma, and I. N. Prawiranegara, "Analisa Digital Forensik Rekaman Video CCTV dengan Menggunakan Metadata dan Hash," Pros. Semin. Nas. Sist. Inf. dan Teknol., vol. 3, no. 1, pp. 223–227, 2019.

[2] E. Casey, "Interrelations between digital investigation and forensic science," Digit. Investig., vol. 28, pp. A1–A2, 2019, doi: 10.1016/j.diin.2019.03.008.

[3] M. N. Al Azhar, Praktical Guidlines for Computer Investigation. 2529.

[4] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, "Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid state Drive (SSD)," Teknomatika, vol. 9, no. 2, pp. 1–13, 2017, [Online]. Available: http://teknomatika.stmikayani.ac.id/wp-content/uploads/2017/07/1.pdf.

[5] W. Pranoto, I. RIadi, and Y. Prayudi, "Live forensics method for acquisition on the solid state Drive (SSD) NVMe TRIM function," Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control, vol. 5, no. 2, pp. 129–138, 2020, doi: 10.22219/kinetik. v5i2.1032.

[6] Mualfah and I. Riadi, "Network Forensics for Detecting Flooding Attack On Web Server," IJCSIS) Int. J. Comput. Sci. Inf. Secur., vol. 15, no. 2, 2017.

[7] Faiz, M. N., Umar, R., & Yudhana, A. Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. JISKa, 1 February 2017, 108–114. https://doi.org/10.14421/jiska.2017.13-02

[8] M. Harbawi and A. Varol, "An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I," Int. Symp. Digit. Forensic Secur, pp. 1– 6, 2017.