Vol. 5, No. 3, Desember 2024, hal. 502-509

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Analisis Data Forensik Pada Rekaman CCTV Menggunakan Metode *National Institute Of Standard Technology* (NIST)

Ilham Asy'ari[*1], Yuhandri[2], Sumijan[3]
Email: [1]iamasyari@gmail.com, [2]yuyu@upiyptk.ac.id, [3]sumijan@upiyptk.ac.id

[123]Magister Teknik Informatika, Fakultas Ilmu Komputer, Universitas Putra Indonesia YPTK Padang

Diterima: 03 September 2024 | Direvisi: - | Disetujui: 10 November 2024

Abstrak

Rekaman CCTV (Closed-Circuit Television) telah menjadi salah satu instrumen penting dalam pengawasan dan pengamanan berbagai tempat seperti perusahaan, bangunan komersial, institusi publik, dan rumah tangga. Rekaman CCTV seringkali menjadi bukti vital dalam investigasi kejahatan, kecelakaan, atau insiden lainnya. Namun selain konten visual yang tersimpan dalam rekaman CCTV, metadata juga memiliki peran penting dalam analisis forensik dan rekonstruksi kejadian. Metode NIST telah mengembangkan beberapa metode dan pedoman untuk analisis forensik metadata pada rekaman CCTV. Penelitian ini bertujuan untuk menjelajahi dan menerapkan metode analisis forensik metadata yang disarankan oleh NIST (*National Institute Of Standard Technology*) dalam konteks rekaman CCTV. Dengan melibatkan teknik-teknik analisis data forensik dan prinsip-prinsip keamanan informasi, penelitian ini akan menggali potensi analisis metadata dalam mendukung investigasi kejahatan, rekonstruksi kejadian, dan pemenuhan standar keamanan yang telah ditetapkan oleh NIST. Penelitian ini menjadi penting dalam konteks keamanan digital dan investigasi forensik modern. Hasil dari penerapan metode NIST pada analisa data forensik rekaman CCTV yaitu menyusun sebuah laporan resmi yang dibuat dari hasil tahapan-tahapan yang ada pada metode NIST sehingga laporan tersebut dapat dijadikan rujukan dalam pengadilan dan barang bukti digital dapat dinyatakan keasliannya. Dengan penerapan metode NIST dalam analisa data forensik rekaman CCTV membuat proses penanganan kasus berjalan dengan terstruktur dan sesuai prosesdur dengan hasil laporan yang valid sehingga barang bukti digital terjaga keasliannya.

Kata kunci: *Rekaman CCTV, Digital Forensik, Metode NIST, Metadata, Bukti Digital.*

Forensic Data Analysis On CCTV Footage Using National Institute Of Standard Technology (NIST) Method.

Abstract

CCTV (Closed-Circuit Television) recordings have become one of the important instruments in monitoring and securing various places such as companies, commercial buildings, public institutions, and households. CCTV recordings are often vital evidence in investigating crimes, accidents, or other incidents. However, in addition to the visual content stored in CCTV recordings, metadata also plays an essential role in forensic analysis and event reconstruction. The NIST method has developed several techniques and guidelines for forensic metadata analysis on CCTV recordings. This research aims to explore and apply the forensic metadata analysis methods recommended by NIST (National Institute of Standards and Technology) in the context of CCTV recordings. By involving forensic data analysis techniques and information security principles, this study will delve into the potential of metadata analysis in supporting criminal investigations, event reconstructions, and meeting the security standards established by NIST. This research is crucial in the context of digital security and modern forensic investigations. The outcome of applying the NIST methods in forensic data analysis of CCTV recordings is the preparation of an official report derived from the stages outlined in the NIST method, so that the report can serve as a reference in court, and the authenticity of the digital evidence can be validated. By applying the NIST method in forensic data analysis of CCTV recordings, the case handling process becomes structured and adheres to procedures, with a valid report ensuring the integrity of the digital evidence.

Keywords: *CCTV Record, Digital Forensic, NIST Method, Metadata, Digital Evidence.*

1. PENDAHULUAN

Pada era digital yang terus berkembang, rekaman CCTV (*Closed-Circuit Television*) telah menjadi salah satu instrumen penting dalam pengawasan dan pengamanan berbagai tempat seperti perusahaan, bangunan komersial, institusi publik, dan rumah tangga [1]. Rekaman CCTV seringkali menjadi bukti vital dalam investigasi kejahatan, kecelakaan, atau insiden lainnya. Namun selain konten visual yang tersimpan dalam rekaman CCTV, metadata juga memiliki peran penting dalam analisis forensik dan rekonstruksi kejadian. Metadata pada rekaman CCTV meliputi informasi seperti waktu dan tanggal rekaman, lokasi kamera, durasi rekaman, dan informasi teknis lainnya [2]. Maka dari itu dibutuhkan bidang ilmu digital forensik yang merupakan penanganan bukti digital untuk dapat dijadikan sebagai bukti yang sah di pengadilan [3]. Analisis forensik metadata pada rekaman CCTV menjadi semakin penting karena metadata dapat memberikan wawasan tambahan, mengonfirmasi kejadian, atau bahkan mengungkapkan manipulasi atau keaslian rekaman. Pada konteks ini, *National Institute of Standard Technology* (NIST) telah mengembangkan beberapa metode dan pedoman untuk analisis forensik metadata pada rekaman CCTV. Metode NIST dalam analisis forensik digital menawarkan pendekatan terstruktur untuk memeriksa dan menganalisis bukti digital dengan langkah-langkah yang terukur dan dapat direplikasi. Dengan menggunakan metodologi ini, investigator dapat memastikan bahwa analisis yang dilakukan konsisten dan hasilnya dapat diandalkan untuk keperluan hukum [4]. Penelitian ini bertujuan untuk menjelajahi dan menerapkan metode analisis forensik metadata yang disarankan oleh NIST yang berawal dari tahapan *collection, examination, analysis* sampai degan *reporting* dalam konteks rekaman CCTV [5].

Terdapat penelitian sebelumnya yang dilakukan oleh Hendita dkk dengan judul Analisa Digital Forensik Rekaman Video CCTV dengan Menggunakan *Metadata* dan *Hash* pada hasil penelitian yang didapatkan disebutkan bahwa Pemanfaatan teknologi CCTV dalam investigasi hukum menuntut pengembangan metode analisis forensik digital yang komprehensif, termasuk analisis metadata, bingkai, dan hash video, untuk mengungkap bukti digital yang akurat dan dapat dipertanggungjawabkan [6].

Kemudian Mualfah dkk. dalam penelitiannya menjelaskan peningkatan pemanfaatan rekaman CCTV sebagai alat bukti digital dalam investigasi kejahatan menuntut pengembangan metode forensik digital yang komprehensif, khususnya dalam analisis bukti digital dan metadata, untuk memastikan integritas dan keakuratan bukti yang dapat dipertanggungjawabkan di persidangan [7]. Penelitian Ramadhan dkk. menyatakan bahwa peningkatan pemanfaatan rekaman CCTV sebagai alat bukti digital dalam investigasi kejahatan menuntut pengembangan metode forensik digital yang komprehensif. Penelitian ini bertujuan untuk menganalisis karakteristik bukti digital dan metadata rekaman CCTV menggunakan metode NIST, serta merumuskan acuan pengelolaan informasi hasil investigasi forensik yang dapat dipertanggungjawabkan di persidangan [8].

Selanjutnya penelitian Kustian dan Adil menyebutkan dalam bidang forensik digital, analisis nilai hash, metadata, dan magic number merupakan teknik krusial untuk memverifikasi keaslian suatu berkas. Penelitian ini memanfaatkan tiga perangkat lunak, yaitu *Forevid* untuk analisis keaslian video dan metadata, *ExifTool* untuk analisis metadata gambar, dan *WinHex* untuk identifikasi *magic number* atau ekstensi asli berkas. Melalui eksperimen perbandingan antara berkas asli dan berkas yang telah dimodifikasi, penelitian ini menunjukkan bahwa ketiga perangkat lunak tersebut efektif dalam mengidentifikasi karakteristik berkas yang relevan dalam proses forensik, seperti nilai *hash, metadata*, dan *magic number* [9].

Penelitian Andria dkk. Forensik metadata foto merupakan pendekatan ilmiah dalam menggali informasi tersembunyi pada sebuah foto. Perkembangan teknologi fotografi dan perangkat lunak pengeditan foto telah meningkatkan risiko manipulasi foto, yang dapat dimanfaatkan dalam kejahatan siber seperti penyebaran berita bohong. Metadata, sebagai informasi terstruktur yang mendeskripsikan suatu berkas, memiliki peran penting dalam forensik digital, yaitu cabang ilmu forensik yang berfokus pada penyelidikan dan pengumpulan bukti digital. Penelitian ini bertujuan untuk menganalisis metadata foto menggunakan *Exiftool*, sebuah perangkat lunak forensik, untuk mengidentifikasi informasi yang dapat digunakan sebagai alat bukti dalam proses hukum [10].

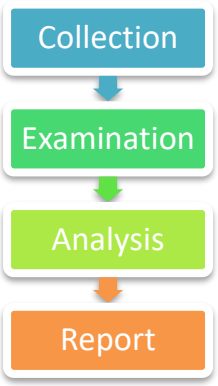
Selanjutnya pada penelitian Sukamto dkk. hasil yang didapatkan bagaimana membuat rekaman video yang dapat dianalisis sebagai data forensik untuk membuktikan kebenaran video tersebut. Dengan forensik, rekaman video dapat digunakan sebagai bukti jika mengandung data yang tidak benar atau data yang berpotensi terkait tindak kejahatan. Metode yang digunakan dalam penelitian ini adalah studi literatur dengan mengkaji berbagai penelitian sebelumnya dari jurnal dan buku yang relevan, untuk mengembangkan permasalahan yang ada serta menemukan kebaruan dalam penelitian ini. Permasalahan yang diangkat adalah bagaimana membuat video dari CCTV yang dapat dibuktikan kebenarannya dengan metode tertentu sehingga dapat dijadikan data forensik yang dapat digunakan sebagai bukti [11].

Penelitian Imam Riadi dkk. dari hasil penelitian ini didapatkan informasi proses pengujian data dengan menggunakan *framework Generic Computer Forensic Investigation Model* (GCFIM) dan untuk proses analisa metadata menggunakan dua *tools* yakni *exiftool dan mediainfo*. Pengujian dilakukan pada video asli dan video tempering. Mengenai metadata video asli dan video tempering yakni adanya perbedaan yang sangat signifikan pada *size* video asli 4.6Mb sedangkan video tempering 4.2Mb. Dapat disimpulkan bahwa *exiftool* dan *mediainfo* dapat dimanfaatkan untuk memperoleh informasi metadata dari suatu data,dengan tujuan untuk memperkuat alat bukti digital pada saat persidangan mengenai keabsahan data tersebut [12]. Berdasarkan beberapa penelitian terdahulu diatas maka pada penelitian ini berusaha mengembangkan proses pemeriksaan dan analisa forensik dengan

menggunakan tiga *tool forensics* untuk menghasilkan informasi yang akurat sehingga bukti digital dapat dijadikan barang bukti yang sah dipengadilan.

2. METODE PENELITIAN

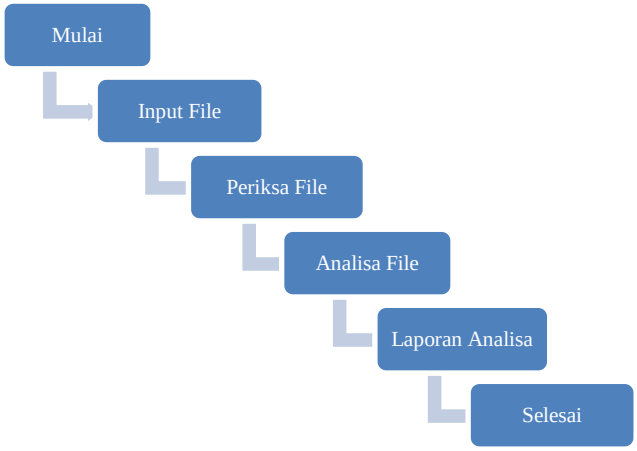
Metodologi penelitian pada penelitian ini menggunakan metode National Institute Of Standard Technology (NIST) yang menngurai tahapan demi tahapan dalam penanganan bukti digital seperti terlihat pada Gambar 1.



Gambar 1. Alur Metode NIST

Alur pada metode NIST seperti terlihat pada Gambar 6 diatas merupakan tahapan-tahapan yang dilakukan sebagai prosedur dalam menangani barang bukti digital. Tahapan tersebut diawali dengan *Collection* yang mengumpulkan barang bukti kemudian *Examination* untuk memeriksa metadata, *Analysis* menganalisa dan *Report* laporan dari hasil tahapan tersebut.

1. *Collection*
   Tahap *collection* merupakan tahapan proses identifikasi, pelabelan, perekamandan pengambilan data dari sumber data. Data yang digunakan pada penelitian ini merupakan data bukti digital dari kasus yang pernah ditangani oleh Bidang Laboraturium Forensik Polda Riau, data bukti digital yang digunakan berupa data rekaman CCTV dari kasus tersebut. Data bukti digital yang diperoleh oleh kepolisian tersebut kemudian akan dideteksi keasliannya sebagai barang bukti digital dalam analisis forensik menggunakan tools forensik.
2. *Examination*
   Tahap *examination* adalah tahap pemeriksaan dan analisis bukti digital denganmenggunakan teknik dan alat forensik yang terstandarisasi, termasuk pengambilangambar forensik, analisis file dan metadata, serta pemulihan data yang hilang.Eksaminasi pada tahap ini akan dilakukan dengan pengecekan metadata bukti digital berupa file video menggunakan *tool* forensik *MediaInfo*,*ExifTool* dan *MD5 File Checksum*. Detail informasi metadata yang didapat dari file rekaman CCTV, berupa tanggal dan waktu gambar diambil, jenis kamera yang digunakan, exif foto dan apakah terdapat software editing yang digunakan, serta informasi metadata lainnya. Beberapa karakteristik metadata yang ditampilkan dalam tahapan ini yaitu dibagi menjadi empat kategori:
   a. Metadata Checksum yaitu Nilai MD5 dan SHA-256. Merupakan proses menampilkan nilai hash dari file rekaman CCTV dengan menggunakan generator MD5 dan SHA-256 secara online melalui website https://emn178.github.io/online-tools/md5_checksum.html dengan cara menginputkan file video yang ingin dicek.
   b. Metadata MediaInfo General yaitu merupakan proses menamplikan metada umum dari file rekaman CCTV seperti *complete file name*, *format*, *file size*, *duration*, *overall bit rate*, *frame rate*, *file extension*.
   c. Metadata MediaInfo Detail yaitu proses menampilkan metadata detail dari file video rekaman CCTV yang berisi *id*, *format*, *format/info*, *format profile*, *duration*, *width*, *height*, *display aspec ratio*, *frame rate*, *color space*, *chrome subsampling*, *dit depth*, *color range*, *color primaries*, *transfer characteristics*, *matrix coefficients*.
   d. Metadata ExifTool yaitu proses menampilkan informasi stempel waktu pada file video rekaman CCTV yang berisi *file modification date/time*, *file access date/time* dan *file creation date/time*.
3. *Analysis*
   Analysis dalam metode NIST adalah suatu tahapan yang dilakukan oleh pihak Laboraturium Forensik dalam untuk menganalisa suatu kejadian dari bukti digital yang telah didapat melalui tahapan sebelumnya yaitu tahap *Collection*. Tahapan *Analysis* ini bertujuan untuk memastikan keaslian dan kebenaran suatu rekaman CCTV. Adapun *tool forensics* yang digunakan dalam tahapan ini sama dengan *tool* yang digunakan pada tahap *Examination*. Berikut ini merupakan alur dari proses *Analysis* seperti pada Gambar 2 berikut.



Gambar 2. Flowchart Analysis

Gambar 2 merupakan alur dari proses analisa dimana file diinputkan ke *tool forensic* terlebih dahulu. Kemudian diperiksa dan dianalisa. Hasil periksa dan analisa dibuat dalam bentuk laporan. Setelah itu laporan tersebut akan dijadikan rujukan dalam kasus yang sedang diselidiki.

4. *Report*

Tahapan selanjutnya dalam metode NIST setelah berhasil melakukan *Collection*, *Examination* dan *Analysis* terhadap barang bukti digital yaitu tahap membuat laporan atau *Report*. Tahapan ini merupakan dimana dikumpulkannya semua bentuk informasi yang diperoleh dari tahapan sebelumnya sehingga menjadi sebuah laporan resmi yang dapat diajukan atau diserahkan kepada pihak yang berwenang untuk dijadikan rujukan dalam pengadilan.

3. HASIL DAN PEMBAHASAN

Data yang digunakan pada penelitian ini adalah data yang didapat dari laboraturium forensik polda riau berupa file rekaman CCTV dari tempat kejadian perkara. Setelah seorang karyawan minimarket melaporkan ke kepolisian bahwa telah terjadi aksi pencurian di minimarket tersebut. Setelah dilakukan olah tempat kejadian perkara dan didapat data-data yang dianggap penting untuk diperiksa lebih lanjut. Pemeriksaan dan file rekaman CCTV tersebut menggunakan tiga *tools forensics* untuk menampilkan metadata dari file tersebut menggunakan tahapan metode NIST. Berikut tabel informasi laporan dugaan tindak kejahatan

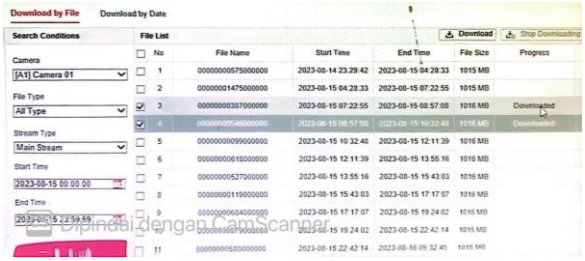
Tabel 1. Rangkuman Laporan Kejadian

No	Informasi	Keterangan
1	Kasus / Topik	Pencurian
2	Petugas	Polsek Tualang
3	Pemeriksa	Investigator Laboraturium Forensik Polda Riau
4	Pelapor	Karyawan Minmarket
5	Alat Bukti Elektornik	DVR CCTV Kamera CCTV
6	Barang Bukti Digital	File Rekaman CCTV

Tabel 1 diatas merupakan rangkuman dari laporan kejadian dan barang bukti yang didapat dari tempat kejadian perkara. Terdapat informasi kasus, petugas, pemeriksa, pelapor alat dan barang bukti digital.

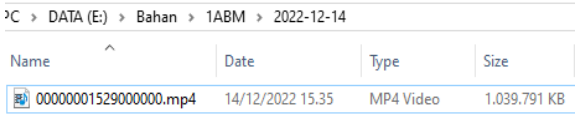
a. Tahap *Collection*

Collection merupakan tahapan pertama pada rangkaian metode NIST. Tahapan ini dilakukan pengumpulan data terhadap barang bukti digital yang akan dilakukan proses pemeriksakan dan dianalisa menggunakan *tool forensics* seperti pada Gambar 3.



Gambar 3. Proses Download File Rekaman CCTV

Gambar 3 terlihat proses download file rekaman CCTV yang dilakukan menggunakan login administrator agar mendapat akses penuh untuk mendownload file rekaman CCTV.

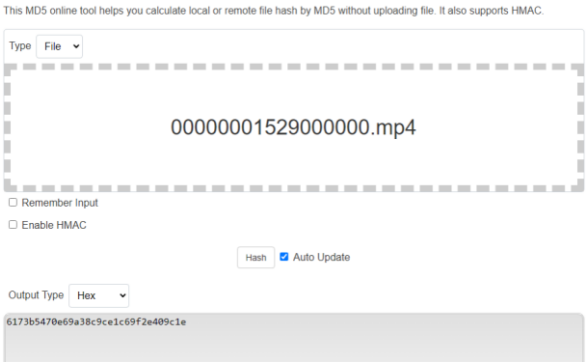


Gambar 4. File Rekaman CCTV

Sedangkan Gambar 4 merupakan keterangan dari file yang sudah berhasil didownload dengan nama file "00000001529000000.mp4" yang berformat MP4 Video dan ukuran 1.039.791 KB atau sekitar 1 GB.

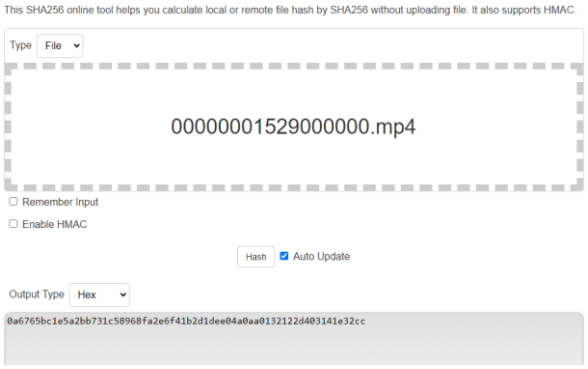
b. Tahap *Examination*

Tahapan berikutnya dalam metode NIST adalah *Examination* yaitu proses pemeriksaan barang bukti digital untuk memastikan dan menjaga keaslian dari barang bukti digital dengan menggunakan *tool forensics* yaitu *MD5* dan *SHA-256* generator, *MediaInfo* dan *ExifTool*. Hasil pemeriksaan dengan *tool forensics* tersebut merupakan metadata yang terdapat pada file rekaman CCTV yang berformat MP4 Video. Adapun hasil dari *Hashing* file video tersebut seperti terlihat pada Gambar 5 dan Gambar 6 berikut.



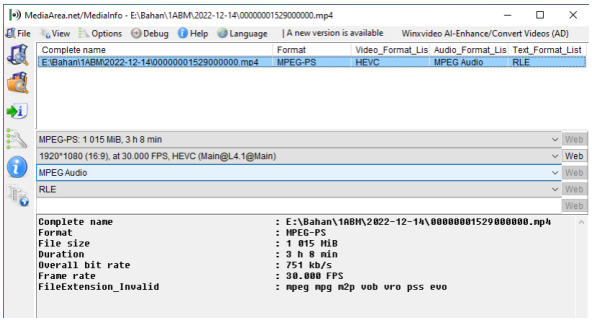
Gambar 5. Metadata MD5 Generator

Gambar 5 terlihat proses pemunculan metadata *MD5 Checksum* dari file video rekaman CCTV dengan nilai *MD5* "6173b5470e69a38c9ce1c69f2e409c1e". Nilai tersebut didapat dari proses *hashing* pada generator online.



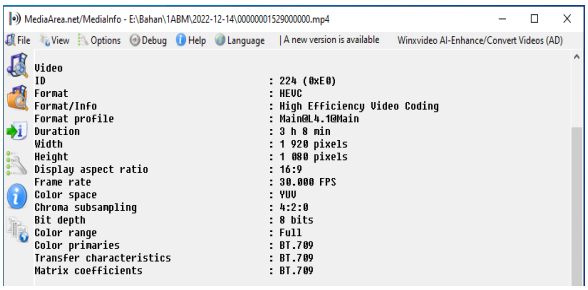
Gambar 6. Metadata SHA-256 Generator

Gambar 6 terlihat proses pemunculan metadata *SHA-256 Checksum* dari file video rekaman CCTV dengan nilai *SHA-256* "0a6765bc1e5a2bb731c58968fa2e6f41b2d1dee04a0aa0132122d403141e32cc". Nilai tersebut didapat dari proses *hashing* pada generator online.



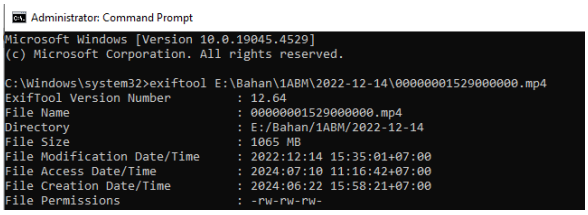
Gambar 7. Metadata MediaInfo General

Gambar 7 merupakan metadata dari aplikasi MediaInfo yang berisikan informasi umum dari file rekaman CCTV yaitu *complete file name, format, file size, duration, overall bit rate, frame rate, file extension*. Metadata general ini merupakan *header* dari file rekaman CCTV. Sedangkan untuk metadata detailnya dapat dilihat seperti yang tertera pada Gambar 8.



Gambar 8. Metadata MediaInfo Detail

Gambar 8 merupakan metadata detail dari aplikasi MediaInfo yang berisikan *id, format, format/info, format profile, duration, width, height, display aspec ratio, frame rate, color space, chrome subsampling, dit depth, colorrange, color primaries, transfer haracteristics, matrix coefficients*.

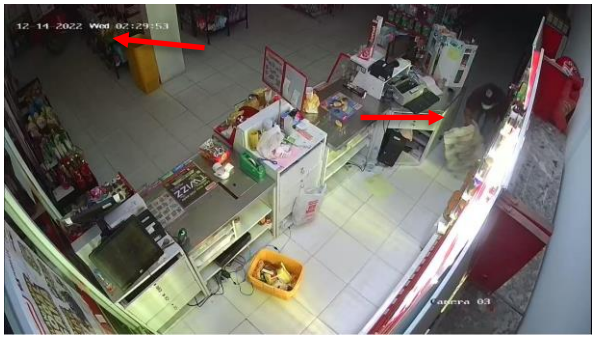


Gambar 9. Metadata ExifTool

Pada Gambar 9 dapat dilihat metadata yang ditampilkan melalui *command exiftool* yang berisikan timestamp dari file rekaman CCTV sehingga dapat diketahui kapan data dibuat dan dimodifikasi.

c. Tahap *Analysis*

Tahap *Analysis* merupakan tahap selanjutnya setelah proses eksaminasi. Pada tahap inilah investigator memberikan penjelasan terhadap video rekaman dan metadata yang telah dieksaminasi seperti terlihat pada Gambar 10 dan Gambar 11 berikut.



Gambar 10. Awal Aksi Pencurian

Gambar 10 Ditemukan dalam video bahwa memang telah terjadi aksi pencurian pada menit 03:50 sampai menit 21:00 dan waktu nyata di tempat kejadia perkara yaitu terjadi pada 12-14-2022 hari rabu pukul 02:29:53 sampai pukul 02:47:03.

Gambar 11. Akhir Aksi Pencurian

Gambar 11 terlihat pelaku pencurian meninggalkan tempat kejadian perkara. Dapat dilihat kondisi area kasir mini market mengalami perubahan dari sebelumnya yaitu banyaknya barang yang berjatuhan akibat perbuatan pencuri. Tahap *Analysis* juga memastikan bahwa metadata dari file rekaman tidak mengalami perubahan setelah melakukan proses analisa dalam mencari waktu aksi pencurian terjadi. Berikut hasil analisa pada tahap *Analysis* seperti pada Tabel 2.

Tabel 2. Perbandingan Metadata

Metadata Sebelum	Metadata Sedudah
MD5 - 6173b5470e69a38c9ce1c69f2e409c1e	MD5 - 6173b5470e69a38c9ce1c69f2e409c1e
SHA-256 0a6765bc1e5a2bb731c58968fa2e6f41b2d1dee04a0aa0132122d403141e32cc	SHA-256 0a6765bc1e5a2bb731c58968fa2e6f41b2d1dee04a0aa0132122d403141e32cc

Tabel 2 merupakan perbandingan dari metadata dari file rekaman cctv sebelum dianalisa dan sesudah dianalisa. Hasil dari perbandingan tidak ditemukan perbedaan metadata. Itu menunjukkan bahwa tidak ada rekayasa pada file rekaman CCTV.

d. Tahap *Report*

Tahapan selanjutnya dalam metode NIST setelah berhasil melakukan *Collection*, *Examination* dan *Analysis* terhadap barang bukti digital yaitu tahap membuat laporan atau Report. Tahapan ini merupakan dimana dikumpulkannya semua bentuk informasi yang diperoleh dari tahapan sebelumnya sehingga menjadi sebuah laporan resmi yang dapat diajukan atau diserahkan kepada pihak yang berwenang untuk dijadikan rujukan dalam pengadilan. Pada tahapan ini akan ditampilkan sebuah tabel yang berisikan informasi mengenai kasus pencurian disebuah minimarket yang terekam oleh kamera CCTV seperti yang terlihat pada Tabel 3.

Tabel 3 Laporan Hasil Pemeriksaan dan Analisa

Informasi	Barang Bukti	Keterangan
Kamera CCTV	Kamera *Hikvision* 2 MP	Ada
DVR CCTV	DVR *Hikvision* 16 CH	Ada
Harddisk	*Seagate* 1 TB	Ada
Nama File Rekaman	00000001529000000.mp4	Ada
Ukuran File Rekaman	1.039.791 KB	Ada
Durasi Rekaman	3 jam 8 menit 58 detik	Ada
Waktu Kejadian	Rabu 14 Desember 2022	Ada
Tempat Kejadian	Alfamart M.Ali Perawang	Ada
Waktu Aksi Kejahatan	02:29:53 - 02:47:03	Ada
Durasi Aksi Kejahatan	18 menit 50 detik	Ada
Waktu Pemeriksaan	04 Maret 2024	Ada
Tempat Pemeriksaan	Laboraturium Forensik Polda Riau	Ada
Tool Forensik	MediaInfo ExifTool MD5-SHA256 Generator	Ada
Hasil Pemeriksaan	Metadata File Rekaman tidak berubah setelah dianalisa. Status File Rekaman Asli.	Ada
Metadata Asli	MD5 – 6173b5470e69a38c9 ce1c69f2e409c1e SHA-256 – 0a6765bc1e5a2b b731c58968fa2e6f41b2d1dee 04a0aa0132122d403141e32cc	Ada
Metadata Pembanding	MD5 – 6173b5470e69a38c9 ce1c69f2e409c1e SHA-256 – 0a6765bc1e5a2b b731c58968fa2e6f41b2d1dee 04a0aa0132122d403141e32cc	Ada
Hasil	**Rekayasa Pada Video Rekaman**	**Tidak Ada**

Tabel 3 merupakan hasil dari laporan yang dirangkum untuk dijadikan rujukan dipengadilan. Isi dari laporan ini terdiri dari informasi mulai dari waktu kejadian, alat bukti digital, barang bukti digital dan nama file yang diperiksa. Pada bagian hasil dijelaskan bahwa tidak ditemukan rekayasa pada video rekaman CCTV.

4. KESIMPULAN

Berdasarkan penelitian dan implementasi yang telah dilakukan maka dapat disimpulkan bahwa penerapan metode *National Institute Of Standard Technology* (NIST) dalam menangani barang bukti digital berupa video rekaman CCTV memberikan hasil analisa yang terstruktur dan dapat dipertanggung jawabkan setelah melalui tahapan-tahapan yang kongkrit dalam menangani barang bukti digital. Implementasi laporan hasil tahapan-tahapan yang komplit dengan rincian keterangan sehingga laporan dan

barang bukti digital dapan dibawa ke pengadilan sesuai dengan undang-undang yang berlaku.

DAFTAR PUSTAKA

[1] E. I. Alwi and S. Anraeni, "Analisis Rekaman Video CCTV Dengan Teknik Enhancement Menggunakan Metode National Institute Of Justice (NIJ)," vol. 17, no. 1, pp. 88–95, 2024, [Online]. Available: http://journal.stekom.ac.id/index.php/elkom□page88

[2] F. Azhiman, R. N. Dasmen, and A. Apriyanto, "Implementasi Exiftool pada Forensik Metadata Video untuk Antisipasi Berita Hoax," *J. Bina Komput.*, vol. 5, no. 1, pp. 23–28, 2023, doi: 10.33557/jbkom.v5i1.2422.

[3] K. Eka Purnama, C. Rozikin, and A. Ali Ridha, "Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode Nist," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 2, pp. 1100–1107, 2023, doi: 10.36040/jati.v7i2.6660.

[4] J. Saintikom, J. Sains, M. Informatika, K. A. Dahlan, A. Yudhana, and H. Yuliansyah, "Analisis File Carving Solid State Drive Menggunakan Metode National Institute of Standards and Technology," vol. 23, pp. 273–280, 2024.

[5] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying Dengan Metode National Institute of Standard and Technology Sp 800-86," *J. Ilm. Inform.*, vol. 12, no. 01, pp. 68–73, 2024, doi: 10.33884/jif.v12i01.8344.

[6] G. Hendita, A. Kusuma, and I. N. Prawiranegara, "Analisa Digital Forensik Rekaman Video CCTV dengan Menggunakan Metadata dan Hash," *Sisfotek*, vol. 3, no. 1, pp. 223–227, 2019.

[7] D. Mualfah, Y. Rizki, and M. Gea, "Analisis Digital Forensik Keaslian Video Rekaman CCTV Menggunakan Metode Localization Tampering," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 1, pp. 43–51, 2022, doi: 10.37859/coscitech.v3i1.3697.

[8] D. Mualfah and R. A. Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 257–267, 2020, doi: 10.31849/digitalzone.v11i2.5174.

[9] 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.

[10] Andria and Saifulloh, "Forensik Metadata Foto Sebagai Alat Bukti Digital Forensic Photo Metadata As Digital Evidence Tool," *Semin. Nas. Has. Penelit. Pengabdi. Masy. Bid. Ilmu Komput.*, no. April 2021, pp. 8–12, 2022.

[11] P. Sukamto, Ispandi, Arman Syah Putra, Nurul Aisyah, and Rohmat Toufiq, "Forensic Digital Analysis for CCTV Video Recording," *Int. J. Sci. Technol. Manag.*, vol. 3, no. 1, pp. 284–291, 2022, doi: 10.46729/ijstm.v3i1.460.

[12] I. Riadi, A. Yudhana, and R. V. A. Saputra, "Forensik Video Pada CCTV Menggunakan Framework Generic Computer Forensics Investigation Model (GCFIM)," *JURIKOM (Jurnal Ris. Komputer)*, vol. 10, no. 2, p. 540, 2023, doi: 10.30865/jurikom.v10i2.5888.