

Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital

Desti Mualfah¹, Rizdqi Akbar Ramadhan²

¹Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Muhammadiyah Riau

²Program Studi Teknik Informatika Fakultas Teknik Universitas Islam Riau

¹Jl. Tuanku Tambusai, Pekanbaru, Riau, telp. (0761) 35008

²Jl. Kaharudin Nst No 113, Bukit Raya, Pekanbaru, Riau, telp. (0761) 678267

e-mail: ¹destimualfah@umri.ac.id, ²rizdqiramadhan@eng.uir.ac.id

Abstrak

Kejahatan konvensional yang terekam kamera CCTV (Closed Circuit Television) semakin banyak ditemukan di masyarakat, setiap pelaku kejahatan yang terbukti melakukan tindak pidana tertentu akan dihukum sesuai dengan peraturan perundang-undangan. Kamera CCTV memiliki peran penting dalam keamanan, banyak diantaranya hasil tangkapan rekaman kamera CCTV dijadikan sebagai alat bukti digital. Tantangannya adalah bagaimana teknik yang diperlukan untuk penanganan khusus investigasi digital forensik dalam mencari bukti digital rekaman kamera CCTV menggunakan metode live forensik, yaitu ketika barang bukti dalam keadaan aktif berdasarkan pedoman SNI 27037:2014 sesuai acuan kerangka kerja Common Phases of Computer Forensics Investigation Models untuk di implementasikan ke dalam dokumen Chain of Custody. Hasil penelitian ini berupa hasil analisis video rekaman kamera CCTV tentang karakteristik bukti digital dan informasi metadata yang digunakan untuk memberikan penjelasan komprehensif secara terstruktur serta acuan pengelolaan informasi data yang didapat dari hasil investigasi digital forensik yang dapat dipertanggungjawabkan dalam persidangan.

Kata kunci: Bukti Digital, Live Forensik, Metadata, Kamera CCTV, Chain of Custody.

Abstract

Conventional crimes that are recorded on CCTV (Closed Circuit Television) cameras are increasingly being found in society, every crime that commits certain crimes will be in accordance with statutory regulations. CCTV cameras have an important role in security, many of which are recorded by CCTV cameras used as digital evidence. The challenge is how the techniques required for special handling, digital forensics in searching for digital evidence of CCTV camera footage using the live forensic method, namely when the evidence is in an active state based on the latest SNI 27037: 2014 according to the framework reference Common Phases of Computer Forensics Investigation Models for in implement it into the Chain of Custody document. These results of this research are in the form of analysis of CCTV camera video recordings about the characteristics of digital evidence and metadata information used to provide a structured comprehensive explanation and reference data management information obtained from the results of digital forensic investigations that can be accounted for in court.

Keywords: Digital Evidence, Live Forensic, Metadata, CCTV Camera, Chain of Custody.

1. Pendahuluan

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 Television) 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 keaslian 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, dimana alat bukti elektronik memiliki bentuk fisik dan bentuk yang dapat dilihat visual, seperti *personal computer*, *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].

Menurut [7], beberapa kasus yang menggunakan kamera CCTV terdapat beberapa asumsi terhadap penggunaan rekaman kamera CCTV yang ditemukan dapat dijadikan sebagai barang bukti atau alat bukti dalam bentuk digital. Merujuk pada Undang-Undang No. 19 Tahun 2016 Pasal 5 Ayat 1 (satu) dan Ayat 2 (dua) tentang informasi dan transaksi elektronik dikatakan bahwa informasi elektronik dan atau dokumen elektronik dan atau hasil cetaknya merupakan alat bukti hukum yang sah, dimana hal tersebut merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Dalam hal ini, kamera CCTV menjadi sebuah alat bukti digital [8] yang valid dan mempunyai sebuah file rekaman yang memberikan sebuah informasi berupa data atau yang biasa dikenal dengan istilah metadata [9], dimana metadata dapat direkam oleh komputer dengan otomatis ketika suatu *file* dibuat, sehingga dapat diketahui kapan *file* tersebut dibuat, siapa user pembuatnya, berapa ukuran *file* nya dan ekstensi yang dihasilkan. Informasi metadata berfungsi untuk menyimpan, menjaga, dan mengelola sumber agar tetap terjaga integritas dan keutuhan *file* yang di dapat dari kamera CCTV. Selain metadata dalam penanganan barang bukti digital kamera CCTV terdapat hal esensial yang disebut *Chain of Custody*. *Chain of custody* merupakan upaya untuk menjaga dan memastikan integritas dalam bukti digital dan prosedur pendokumentasian bukti secara kronologis untuk menjelaskan 5 karakteristik (4W dan 1 H) *Chain of Custody*, yaitu *fingerprint of evidences (why)*, *digital signing (who)*, *time stamping (when)*, *geo location (where)* dan *procedures (how)* [10].

Selanjutnya, dalam mencari 5 karakteristik *Chain of Custody* pada rekaman kamera CCTV diperlukan sebuah kerangka kerja *Common Phases of Computer Forensics Investigation Models* [11] dengan metodologi *live forensic* [5] dalam mengambil objek komponen dari artefak bukti digital dalam keadaan aktif. Teknik yang diperlukan dalam menganalisis hasil rekaman kamera CCTV, informasi metadata dan *Hash* suatu *file* yang terkandung dalam video memerlukan prinsip ilmu digital forensik, karena alat bukti digital pada dasarnya memiliki ciri yang mudah digandakan dan ditransmisi sehingga sangat rentan dilakukan modifikasi dan menghilangkan data yang ada serta mudah dikontaminasi oleh data yang baru dan sensitif terhadap waktu sehingga dibutuhkan sebuah kerangka kerja ilmiah untuk proses investigasi. Hasil penelitian ini berupa alat bukti digital kamera CCTV yang memiliki *file* rekaman video dan metadata yang merepresentasikan informasi terkait yang didapat dari rekaman kamera CCTV sebagai alat bukti digital yang sah dalam persidangan, dengan menerapkan ilmu digital forensik investigasi analisis rekaman kamera CCTV dapat dijaga integritasnya dari sejak pertama ditemukan hingga dijadikan alat bukti digital yang dapat dipertanggungjawabkan dalam persidangan.

2. Metode Penelitian

Tahapan penelitian yang dilakukan adalah menggunakan pendekatan metodologi teknik *live forensic*, metodologi *live forensic* merupakan pengambilan (*capturing*) terhadap objek komponen komputasi guna eksplorasi bukti digital dan artefak lainnya dalam keadaan pemrosesan aktif pada bukti digital rekaman kamera CCTV dengan berdasarkan pedoman dan

persyaratan dalam Standar Nasional Indonesia (SNI) 27037:2014 [12] menggunakan acuan kerangka kerja *Common Phases of Computer Forensics Investigation Models*.

2.1. Common Phases of Computer Forensics Investigation Models

Common Phases of Computer Forensics Investigation Models merupakan kerangka kerja ilmiah yang memiliki dasar dan terbukti untuk proses investigasi digital forensik yang meliputi *Acquisition*, *Identification*, *Evaluation* dan *Admission* dari bukti yang berasal dari sumber digital dari tempat perkara dan alat yang telah dilakukannya simulasi skenario rekaman kamera CCTV pada suatu peristiwa kasus yang melanggar hukum teknologi informasi dan mengandung pidana, atau membantu untuk mengantisipasi tindakan yang merusak keaslian barang bukti sehingga membuat barang bukti yang telah didapatkan menjadi tidak sah di mata hukum. Kerangka [13] kerja *Common Phases of Computer Forensics Investigation Models* yang dipakai dalam penelitian dapat dilihat pada gambar dibawah ini:



Gambar 1. Alur Tahap Kerangka Kerja

Secara lengkap dipaparkan sebagai berikut: Tahap *Acquisition* merupakan proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktifitas yang dilakukan dari bukti yang berasal dari sumber digital dari tempat perkara. Tahap *Identification* melibatkan proses mencari bukti potensial dari perangkat digital dan media penyimpanan digital. Tahap *Evaluaiton* dilakukan untuk menentukan alat bukti yang sedang diidentifikasi relevan dengan kasus yang sedang diselidiki dengan meneliti yang 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. Tahap *Admission* ini menyajikan laporan yang di ekstrak secara detail saat penyelidikan dengan bukti yang telah dianalisis.

2.2. Simulasi Kasus

Merupakan tahap dilakukannya simulasi kasus yang ditangkap oleh kamrea CCTV. Simulasi kasus bertujuan untuk melakukan pengujian hasil rekaman kamera CCTV untuk mendapatkan hasil metada rekaman CCTV. Pada simulasi ini dilakukan skenario pada sebuah rumah yang dipasangkan kamera CCTV dengan sudut titik rumah bagian belakang. Pada gambar 2 terlihat letak sudut pemasangan kamera CCTV yang dipasang untuk melakukan skenario simulasi kasus.



Gambar 2. Letak Posisi Kamera CCTV

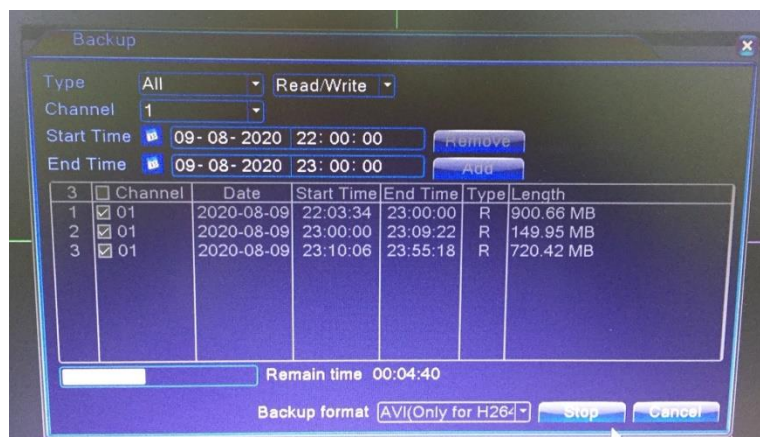
3. Hasil dan Pembahasan

3.1 Hasil

3.1.1 Acquisition

Proses akuisisi (*Acquisition*) melibatkan pembuatan salinan bukti digital dan mendokumentasikan metode live forensik setelah melakukan skenario kasus yang digunakan dan aktivitas yang dilakukan dengan cara *logical aquisition*, yaitu hanya menargetkan tipe data tertentu, direktori atau lokasi yang diinginkan untuk memperoleh informasi dari alat digital dan

media peralatan. Seperti pada gambar 3 proses akusisi rekaman kamera CCTV dilakukan setelah melakukan skenario dengan mengcopy file tipe data [14] yang sudah ditentukan.



Gambar 3. Proses Acquisition

3.1.2 Identification

Investigasi forensik pada tahap identifikasi dimulai dengan pencarian bukti seputar alat rekam yang ada pada kamera CCTV yang difungsikan untuk menyimpan tangkapan gambar yang berasal dari kamera CCTV tersebut dengan mengetahui posisi kamera dan tipe kamera yang dipakai dengan mencantumkan label pada alat bukti digital. Label alat bukti digital diperoleh sebuah rekaman kamera CCTV dengan jenis kamera yang digunakan berupa alat rekam berjenis *Stand Alone* dengan serial number yang didapat pada tabel 1 tipe kamer.

Tabel 1. Tipe Kamera CCTV

Tipe	Keterangan
Jenis	Stand Alone DVR
Merek	HD Hybrid AHD DVR
Serial Number	221C10F3087C1924

Dari tabel diatas kamera CCTV memiliki model *Stand Alone* DVR yang merupakan jenis alat elektronik untuk merekam sebuah video kedalam bentuk format digital dengan media penyimpanan berupa HDD, USB *FlashDisk*, SSD maupun kartu memori SD. Jenis DVR *Stand Alone* merupakan jenis DVR yang dapat berdiri sendiri tanpa menggunakan PC (*Personal Computer*). Pada kamera CCTV DVR biasanya memiliki kemampuan dalam merekam dengan format beresolusi Half D1, CIF, D1, dan 960H dengan ukuran resolusi pada tabel 2 dibawah ini:

Tabel 2. Resolusi Kamera DVR

Ukuran	Resolusi (NTSC)	Resolusi (PAL)
QCIF	176x120	176x144
CIF	352x240	352x288
Half D1	352x480	352x576
D1/4CIF	704x480	704x576
960H	928x480	960x576

Kamera CCTV tipe DVR, yang memiliki fungsi utama alat perekam dengan bantuan kamera sebagai objek rekam dapat dipakai sebagai komputer server, *smartphone* maupun laptop untuk dapat mengakses kamera CCTV untuk dapat melihat hasil rekaman. Dengan demikian DVR memiliki sebuah *MAC Address* khusus [15] beberapa port ethernet agar dapat dikoneksikan ke dalam infrastruktur *network*.

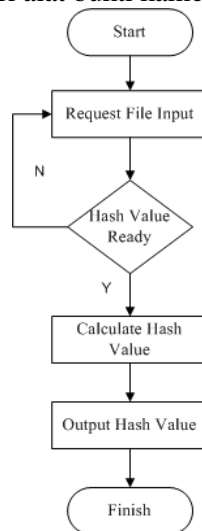
3.1.3 Evaluation

Proses evaluation dilakukan untuk menentukan alat bukti yang sedang diidentifikasi relevan dengan kasus yang sedang diselidiki. Forensik digital yang merupakan proses penyelidikan untuk mencari penemuan, mengumpulkan dan menganalisis bukti digital. Dalam

hal ini bukti digital dalam bentuk rekaman video kamera CCTV. Rekaman tersebut diperiksa sehubungan dengan kegiatan pelaku tindak kejahatan [16] yang telah direkam dalam kamera pengawas pada sebuah rumah. Rekaman tersebut kemudian dilakukan proses tempering video forensik yang digunakan untuk mendapatkan informasi yang dicari.

Selanjutnya file rekaman akan dicari nilai hash verification yang terdapat dalam metadata rekaman CCTV. Hasil nilai hash dapat menjelaskan karakteristik metadata dari hasil rekaman video CCTV untuk membuktikan tingkat keasliannya [17], nilai hash menggunakan algoritma tertentu contohnya SHA1, SHA256, MD5 dan lainnya sehingga dihasilkan suatu deret nilai yang unik yang berbeda dengan yang lain.

Keutuhan barang bukti video rekaman CCTV didapatkan dari nilai hash yang berfungsi menjelaskan originalitas barang bukti sebagai langkah awal untuk memverifikasi kesesuaian *file* yang asli dengan *file* yang dianalisis. Pada gambar 4 merupakan langkah untuk mendapatkan nilai *Hash* investigasi digital forensik dari alat bukti kamera CCTV.



Gambar 4. *Authentication Hash Value*

Dari *file* rekaman di dapat nilai *Hash* dengan ekstensi MD5 (*Message Digest algorithm 5*) dengan panjang 32 karakter, dibawah ini merupakan gambar 5 hasil nilai *Hash* video kamera CCTV.

db3197120b42015f157a40a7601c62a9

Gambar 5. *Hash Value*

Setelah mendapatkan nilai *hash* selanjutnya ialah melakukan analisis terhadap *file* rekaman kamera CCTV, pada rekaman kamera CCTV didapatkan informasi seputaran alat rekam dan jenis DVR yang digunakan adalah jenis *Stand Alone* dengan versi alat rekam pada tabel 3.

Tabel 3. Informasi Alat Rekam

Info	Versi
System	V4.03.R11E4831191.10001.231900.00000
Device Info	00009.00000.0000000000
Build Date	19-11-2018 16:41:05
Mac Address	0012414bd237
Serial Number	221C10F2087C1924
Record Channel	4
Status	3
Nat Status	Probing DNS
Nat Status Code	0:/0/+000

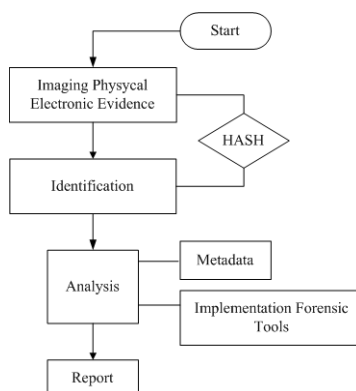
Informasi alat rekam dengan jenis *Stand Alone* DVR merupakan jenis perangkat dalam bentuk elektronik yang memiliki tugas untuk merekam video dalam mengubah format digital ke media penyimpanan berupa HDD. Setelah mendapatkan informasi identifikasi tipe kamera selanjutnya mencari informasi terkait fitur CCTV yang terpasang pada DVR seperti multiplexer, network capabilities dan fitur atau alat lainnya yang disandingkan dengan DVR. Berikut adalah tabel 4 yang menjelaskan fitur CCTV.

Tabel 4. Informasi Fitur CCTV

Fitur	Keterangan
Multiplexer	4 Channel
Network Terhubung	Tidak Terhubung
Transactional Data	USB
Penyimpanan	HDD 500 GB

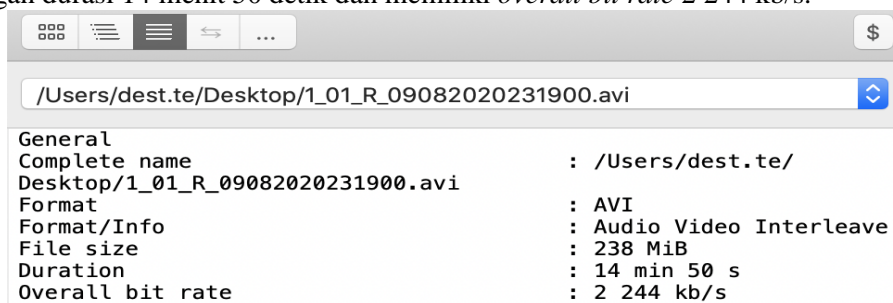
Selanjutnya, setelah identifikasi informasi seputar alat rekam ialah dengan menganalisis *file* rekaman yang didapat dari kamera CCTV, pada *file* kamera CCTV terdapat sebuah metadata yang menjelaskan gambaran suatu informasi terstruktur yang dihasilkan dari data rekaman kamera untuk menjelaskan dan menempatkan serta mengelola sebuah sumber data agar dapat dipahami informasi yang terdapat pada file rekaman.

Pengujian file rekaman dilakukan dengan menggunakan *tool* forensik MediaInfo dan Exif *tool* dengan tujuan untuk mendapatkan informasi data yang didapat dari *header*, isi dan *footer* [16]. *Header* berada pada banyak *byte* pertama sebelum informasi isi *file*, sedangkan *footer* berada pada beberapa *byte* yang teletak terakhir sebelum adanya isi informasi. Metadata pada bagian *header* video kamera CCTV berisikan *file signature* data yang digunakan untuk mengidentifikasi memverivikasi isi dari sebuah file yang berisikan metadata tentang informasi umum, *codec* video dan *codec* audio. Gambar 6 menjelaskan tentang alur pengujian metadata rekaman kamera CCTV untuk memperoleh info terkait integritas alat bukti rekaman video CCTV.



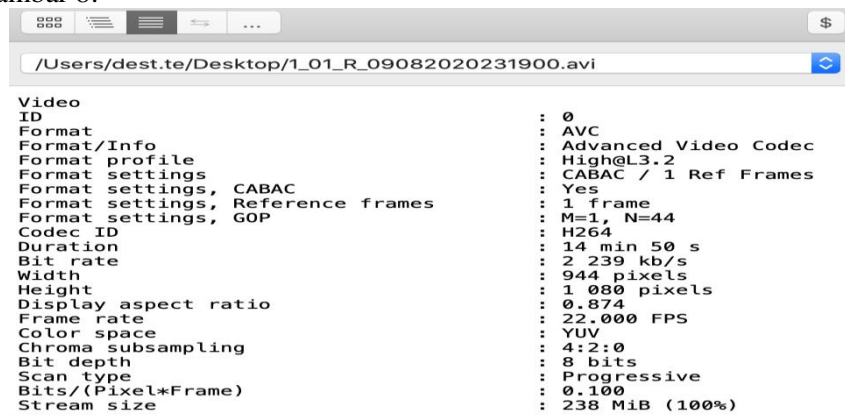
Gambar 6. Core Acquisition

Hasil ekstraksi pengujian metadata menggunakan *tool* forensik MediaInfo mendapatkan informasi umum terkait data-data pada gambar 7 tentang *file* nama dengan hasil 1_01_R_09082020231900.avi dengan format .AVI (*Audio Video Interleave*), berukuran file 238 MiB dengan durasi 14 menit 50 detik dan memiliki *overall bit rate* 2 244 kb/s.



Gambar 7. Informasi Header Metadata

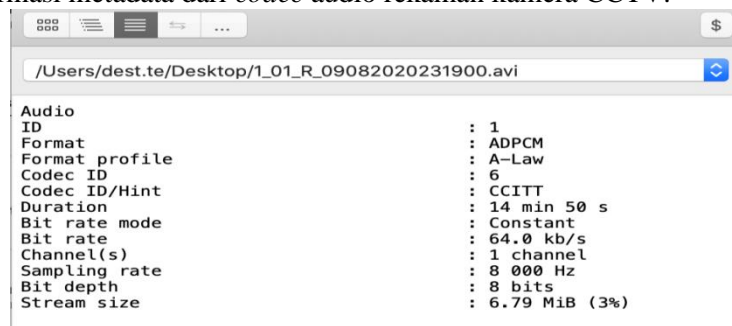
Setelah didapat tentang informasi umum selanjutnya mendapatkan kompresi video berisikan *codec* dengan format AVC serta panjangnya video x lebar video yang beresolusi 944 pixels yang memiliki *frame rate* 22.000 FPS dan ukuran *stream* yang didapat berupa informasi isi dalam gambar 8:



Gambar 8. Informasi Isi Metadata

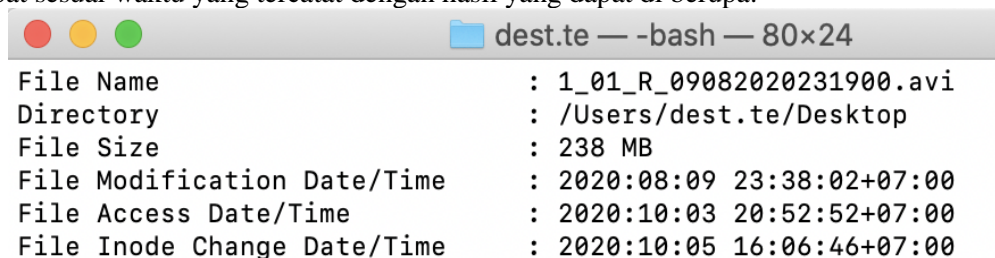
Forensik rekaman kamera CCTV didapatkan informasi dari gambar 7 tentang *codec* audio yang berisikan format *codec* yang menerjemakan biner kedalam pixel untuk menerjemahkan data visual berupa format AVC (*advanced Video Codec*).

Setelah mendapatkan informasi metadata terkait *codec* video ialah tentang *codec* audio yang berisi format *codec* (*compression/decompression*), yaitu *channel* yang dapat menentukan mono maupun stereo untuk rekaman jenis audio dan ukuran *stream*. Ekstraksi ini mendapkan informasi audio dengan format ADPCM (*Adaptive differential pulse-code modulation*) yang menjelaskan langkah kualitas data yang diperlukan untuk rasio sinyal terhadap noise atau sinyal-sinyal yang tidak diinginkan dalam suatu sistem informasi. Gambar 9 dibawah ini merupakan informasi metadata dari *codec* audio rekaman kamera CCTV.



Gambar 9. Informasi Isi Footer

Selain mendapatkan informasi terkait isi dari metadata video, forensik metadata rekaman kamera CCTV didapatkan informasi *live data* [18] menggunakan *Exif Tool* yang berupa informasi *timestamps* [19] tentang catatan waktu terhadap *file* metadata video kamera CCTV seperti kapan waktu kejadian sebuah *file* tersebut dibuat, kapan waktu terakhir *file* rekaman terjadi proses modifikasi yang terekam pada sistem. Catatan berisikan waktu *file* tersebut didapat sesuai waktu yang tercatat dengan hasil yang dapat di berupa:



Gambar 10. Informasi Timestamps File

Pada gambar 10 diatas didapatkan informasi *created date* 09-08-2020 pukul 09:38:03 dengan keterangan informasi waktu kejadian ketika sebuah *file* pertama dibuat oleh sistem. Selanjutnya didapatkan informasi tentang *modified date* 09-08-2020 pukul 23:38:02+07:00 dengan keterangan waktu berdasarkan *file* tersebut dimodifikasi, dan informasi *access date* 10-08-2020 pukul 13:05:23+07:00 dengan keterangan catatan ketika sebuah *file* dibaca atau diakses didalam sebuah sistem.

Informasi lain dari metadata *file* video hasil rekaman CCTV terlihat oknum saat melakukan kegiatan berupa kronologi isi video yang terekam pada gambar 11 yang tertangkap oleh kamera.



Gambar 11. Isi Kronologi Kejadian

Setelah selesai menguji dan analisis metadata rekaman CCTV teknik investigasi pencarian bukti digital ialah menguji kembali file rekaman untuk memastikan nilainya tidak berubah dari awal di temukan hingga sampai akhir di analisis. Pengujian *Hash* metadata setelah proses analisis investigasi berhasil maka dilakukan langkah *authentication Hash value* dengan langkah pada gambar 4 berupa file rekaman video kamera CCTV setelah dilakukan analisis dan pengujian dapatkan nilai dengan panjang 32 karakter dan berekstensi MD5 dengan nilai db3197120b42015f157a40a7601c62a9 yang menunjukkan nilai *Hash* yang sama dengan pengujian nilai *hash* sebelum dilakukan analisis, dengan demikian alat bukti dari rekaman video kamera CCTV tidak mengalami perubahan dengan file aslinya.

3.1.4 Admission

Tahap ini menyajikan laporan yang di ekstrak secara detail saat penyelidikan dengan bukti yang telah dianalisa dan dapat dipertanggung jawabkan di pengadilan. Dari hasil pengujian dan analisis metadata rekaman CCTV mendapatkan bukti digital informasi terkait metadata yang di dapat dari hasil rekaman video kamera CCTV telah berhasil untuk menjaga dan memastikan integritas bukti digital dan prosedur pendokumentasian bukti secara kronologis dapat dipergunakan didalam persidangan sebagai alat bukti digital yang sah, tabel 5 merupakan hasil laporan catatan analisis metadata pada rekaman CCTV berupa:


Tabel 5. Hasil Analisis Metadata

No.	Identifikasi	Keterangan
1	Seputar Tipe Alat Rekam	CCTV Stand Alone DVR Compresor Name Handler Description
2.	Info File	Waktu keajdian dalam file 2020:08:09 Nama Rekaman 1_01_R09082020239000.avi Format File MP4 Video/x-msvideo Durasi 0:14:50
3.	Serial Number	221C10F2087C1924
4.	Record Channel	Channel 4
5.	Kualitas Video	Default

No.	Identifikasi	Keterangan
6.	Frame Rate	124.5 KB/S
7.	Frame Record Size	Width x Height=944 x 1080
8.	Kapasitas	238 MB
9.	Firmware	Probing DNS code 0:/0/+000
10.	Timestamps	Date/time Actual 09:08:2020 Pukul 23:38:02+07:00

Menuru [20], model pelaku dalam interaksi proses *chain of custody* akan dipengaruhi oleh ketentuan hukum disetiap negara. Namun apapun model yang dibangun harus dapat menjelaskan aktivitas, hubungan dan keterlibatan pelaku pada bukti digital. Sebagai contoh dalam perkara nomor 85/PID/.B/2012/PN.PWT yang dikutip dari penelitian [21] didapat alat bukti elektronik berjenis 3 buah CD pada rekaman kamera CCTV yang tidak memiliki kekuatan hukum disebabkan tidak diajukan atau disertakannya alatu bukti berupa surat yang menyatakan hasil dari proses *hashing* dan penerimaan barang bukti kedalam bentuk dokumen surat sebagai lampiran bentuk keaslian suatu *file* yang sedang di investigasi , hal demikian dapat memberikan petunjuk kepada pihak pengadilan tidak dapat menerima bukti yang diberikan apabila suatu tindak pidana yang terekam oleh kamera tidak dapat menunjukkan dan memastikan bagaimana barang bukti yang sedang ditangani.

Dari perkara yang ada *Chain of Custody* digunakan untuk “*A Road Map That Shows how evidence was collected, analyzed and preserved in order to presented as evidence in court*”. Pada gambar 10 menunjukkan formulir *Chain of Custody* yang didapat dari metadata rekaman CCTV dapat digunakan saat persidangan dengan hasil bukti yang diserahkan sudah sesuai dan meluui proses investigasi digital forensik telah terdokumentasi dengan melampirkan bukti tidak adanya unsur barang bukti yang diserahkan telah dimanipulasi. Dengan demikian laporan hasil investigasi metadata kamera CCTV didapatkan pada gambar 10 yang akan digunakan dalam persidangan.



FORM CHAIN OF CUSTODY
INFORMATIC ENGINEERING LABOLATORY
 UNIVERSITAS MUHAMMADIYAH RIAU
 Street Tuanku Tambusai City Pekanbaru

Section 1

CASE INFORMATION			
Case Number	B/198/****		
Date and Time	Selasa / 1 September 2020		
PIHAK PENANGGUNG JAWAB			
Investigator	Desti		
Institution	Universitas Muhammadiyah Riau		
Address	Street Tuanku Tambusai City Pekanbaru		

Section 2

DESCRIPTION OF THE EVIDENCE			
Type of Evidence	USB Flash Disk	Merek	SanDisk
Serial Number	-----	Brand	
Condition	Write Protected	Other Information	Master Evidence

Section 3

TRANSFER OF EVIDENCE			
Date	17 August 2020	Location	Jl. Melati Indah
Submitted by		Received by	
Name	Desti	Name	Nan
Position	Investigator	Position	UMRI Laboratory
Signature	-----	Signature	-----
Information	The Master of Evidence CCTV Recording Comfirmed .avi Hash Number : db3197120b42015f157a40a7601c62a9		

Gambar 10. Dokumen *Chain of Custody*

3.2 Pembahasan

Menangani bukti digital atau bukti elektronik yang terkait dengan kamera CCTV semakin kompleks, oleh karena itu metode yang digunakan dalam menangani CCTV harus sesuai dengan keadaan dimana alat bukti tersebut didapatkan, pada penelitian sebelumnya telah membahas *framework* akuisisi terkait jenis kamera CCTV berupa tipe Analog DVR (*Digital Video*

Recorder), tipe NVR (*Network Video Recorder*) dan NVR Based on Cloud Computing, akan tetapi dalam penelitian [22] metode akuisisi yang dilakukan belum mengkaji status *live* atau *static* forensik, dimana *live* forensik mengambil (*capturing*) terhadap objek komponen komputasi guna eksplorasi bukti digital dan artefak lainnya dalam keadaan pemrosesan aktif pada bukti digital, sedangkan pada *static* forensik bukti digital yang akan *diekslore* diambil dalam keadaan komputer mati dan bisa diartikan investigator melakukan *capturing* pada komponen penyimpanan secara tidak langsung, hal yang potensial terjadi pada metode *static* forensik adalah manipulasi data hasil akuisisi, hal ini dibenarkan pada perspektif investigator dalam rangka membuktikan artefak-artefak yang perlu diperjelas secara mekanisme dan fakta.

Pada penelitian ini bukti digital yang di *capture* dilakukan secara *realtime* yang mengindikasikan penelitian ini menggunakan *live* forensik. Barang bukti pada penelitian ini dapat dipastikan tidak terdapat manipulasi dan terbukti dari nilai *Hash* yang identik pada saat perhitungannya dalam dua garis waktu yang berbeda (alat bukti sebelum dianalisis dan yang sudah dianalisis). Pada gambar 11 ditampilkan secara visual hasil dari analisis metadata oleh sistem yang menjadi tantangan bagi investigator dalam melakukan analisa khususnya dalam karakteristik barang bukti fisik (kamera CCTV) serta bukti digital berupa rekaman video masih terjaga integritasnya dengan membuktikan jumlah *frame* dan durasi waktu yang sama seperti saat dilakukan pengujian, yaitu selama 14 menit 50 detik.



Gambar 11. Raw Image

4. Kesimpulan

Tahapan utama akuisisi dalam investigasi dan analisis forensik digital diperlukan integritas keaslian barang bukti dari saat ditemukan, diperoleh, dianalisis hingga tahap pelaporan sesuai dengan prinsip *Chain of Custody*. Secara teknis keutuhan dan keaslian barang bukti dapat dibuktikan dengan menghitung nilai hash, sedangkan dalam hal alat bukti berupa CCTV dibutuhkan kemampuan untuk menggunakan aspek multimedia dalam menganalisis alat bukti digital metadata rekaman kamera CCTV yang digunakan untuk memperkuat alat bukti digital dalam persidangan.

Daftar Pustaka

- [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 Guidelines 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] D. 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] W. Abraham, H. Firmansyah, and W. Abraham, “Analisis Pembuktian Alat Bukti Closed Circuit Television (CCTV) Sebagai Alat Bukti Petunjuk,” no. 11, 2019.
- [8] A. Yudhana, I. Riadi, and I. Zuhriyanto, “Menggunakan Metode Digital Forensics Research Workshop (DFRWS),” vol. 20, no. 2, pp. 125–130, 2019.
- [9] M. Subli, B. Sugiantoro, and Y. Prayudi, “Metadata Forensik untuk Mendukung Proses Investigasi Digital,” *J. Ilm. DASI*, vol. 18, no. 1, pp. 44–50, 2017, doi: 10.13140/RG.2.2.34035.94242.
- [10] M. N. O. Sadiku, A. E. Shadare, and S. M. Musa, “Digital Chain of Custody,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 7, p. 117, 2017, doi: 10.23956/ijaresse.v7i7.109.
- [11] C. Liu, S. G. Li, S. Qin, and S. G. Yang, “Research and application of influences of lateral pressure coefficients on the extension angle of coal cracks,” *Math. Probl. Eng.*, vol. 2016, no. 3, pp. 17–31, 2016, doi: 10.1155/2016/3068347.
- [12] D. M. Suratno, I. Riadi, and Y. Prayudi, “First Respond Framework Untuk Forensik CCTV,” *Hacking Digit. Forensics Expo.*, pp. 13–20, 2018.
- [13] C. Paper, Y. Prayudi, and U. Islam, “(DiFRI) Untuk Mengukur Tingkat Kesiapan Institusi Dalam Menanggulangi Aktifitas Model Digital Forensic Readiness Index (DiFRI),” no. July, 2016.
- [14] A. Putra Justicia, “Analysis of Forensic Video in Storage Data Using Tampering Method,” *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 328–335, 2018, doi: 10.17781/p002471.
- [15] D. Mualfah, Y. Fatma, and R. A. Ramadhan, “Anti-forensics: The image asymmetry key and single layer perceptron for digital data security,” *J. Phys. Conf. Ser.*, vol. 1517, no. 1, 2020, doi: 10.1088/1742-6596/1517/1/012106.
- [16] X. Du, N. A. Le-Khac, and M. Scanlon, “Evaluation of digital forensic process models with respect to digital forensics as a service,” *Eur. Conf. Inf. Warf. Secur. ECCWS*, pp. 573–581, 2017.
- [17] H. A. Rahman, “Otentikasi File Dengan Algoritma Kriptografi SHA-1 Menggunakan Python Dan Pycrypto,” no. January 2013, 2008.
- [18] R. Chowdhry, “FORENSIC SCIENCE PAPER No . 7 : Criminalistics and Crime Scene Investigation MODULE No . 32 : Use of CCTV for Forensic Evidence FORENSIC SCIENCE PAPER No . 7 : Criminalistics and Crime Scene Investigation MODULE No . 32 : Use of CCTV for Forensic Evidence,” no. 7.
- [19] R. Alshalawi and T. Alghamdi, “Forensic tool for wireless surveillance camera,” *Int. Conf. Adv. Commun. Technol. ICACT*, no. January 2017, pp. 536–540, 2017, doi: 10.23919/ICACT.2017.7890148.
- [20] J. Hukum and K. Ummah, “Peran Laboratorium Forensik Polri Sebagai Pendukung Penyidikan Secara Ilmiah Dalam Sistem Peradilan Pidana Di Indonesia Teguh Prihmono * , Umar Ma’ruf ** , Sri Endah Wahyuningsih *** *,” *J. Huk. Khaira Ummah*, vol. 13, no. 1, pp. 273–286, 2018.
- [21] S. Terintegrasi and K. D. A. N. Berkesinambungan, “Linguistik Forensik: Sumbangsih Kajian Bahasa dalam Penegakan HUKUM,” vol. 1, no. 3, pp. 51–60, 2019.
- [22] D. Hariyadi, F. E. Nastiti, and F. N. Aini, “Framework for Acquisition of CCTV Evidence Based on ACPO and SNI ISO / IEC 27037 : 2014,” *Int. Conf. Informatics Dev.*, 2018.

