

Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (*National Institute of Standards Technology*)

Desti Mualfah¹, Rizdqi Akbar Ramadhan²

Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau¹

Jurusan Teknik Informatika, Fakultas Teknik, Universitas Islam Riau²

destimualfah@umri.ac.id, rizdqiramadhan@eng.uir.ac.id

Article Info

History :

Dikirim 25 Oktober 2020

Direvisi 29 Oktober 2020

Diterima 14 November 2020

Kata Kunci :

Kamera CCTV

NIST

Metadata

Chain of Custody

Abstrak

Kejahatan konvensional yang terekam kamera CCTV (*Closed Circuit Television*) semakin meningkat, setiap pelaku kejahatan yang terbukti melakukan tindak pidana tertentu akan dihukum sesuai dengan peraturan perundang-undangan. Permasalahannya, adalah bagaimana sebuah kasus yang terekam pada kamera CCTV dapat dijadikan sebagai alat bukti digital. Bukti digital berkaitan erat dalam memastikan keamanan, privasi dan integritas data saat mengikuti tahapan proses identifikasi digital forensik. Tahap identifikasi menggunakan metode NIST (*National Institute of Standards Technology*) digunakan untuk investigasi dalam mencari informasi terkait metadata pada rekaman kamera CCTV agar dapat memberikan informasi terstruktur, menggambarkan serta mengolah sebuah informasi yang didapat dari sumber investigasi digital forensik dapat di implementasikan kedalam 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.

© This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Koresponden:

Desti Mualfah

Program Studi Teknik Informatika, Fakultas Ilmu Komputer

Universitas Muhammadiyah Riau

Jl. Tuanku Tambusai, Pekanbaru, Indonesia,

Email : destimualfah@umri.ac.id

1. PENDAHULUAN

Saat ini peran kamera CCTV (*Closed Circuit Television*) sangat dibutuhkan sebagai sistem pengamanan dalam kehidupan sehari-hari, penggunaan kamera CCTV dinilai sangat efisien sebagai mekanisme pengamanan yang diminati saat ini karena kemampuan yang dimiliki untuk

mengantisipasi terjadinya kejahatan dalam lingkungan masyarakat. Kondisi ini sangat di harapkan oleh masyarakat agar terhindar dari berbagai tindak kriminal [1], dengan demikian peran dan fungsi kamera CCTV saat ini tidak hanya sebagai alat untuk memantau lingkungan disekitar.

Kamera CCTV memiliki kemampuan untuk merekam keadaan sekitar secara *realtime* [2], pada saat tertentu kamera CCTV dijadikan sebagai barang bukti terkait tindak kasus pidana. Akan tetapi barang bukti kamera CCTV memiliki teknik khusus dalam menanganinya karena sifat barang bukti yang didapat dari rekaman kamera bersifat *vollatile* [3] atau mudah berubah, sangat rentan untuk dimodifikasi dan dihilangkan, mudah terkontaminasi oleh data baru, dan sensitif terhadap waktu. Untuk menjaga keutuhan dan keaslian barang bukti di perlukan penerapan ilmu digital forensik [4] dalam investigasi suatu perkara.

Ilmu digital forensik yang digunakan untuk praktik pembedahan perangkat digital dalam mencari fakta yang diperlukan untuk kepentingan hukum. Dalam hal ini bukti digital terdapat dua istilah yang hampir sama yaitu bukti elektronik dan bukti digital[5]. Alat bukti elektronik berbentuk fisik dan dapat dikenali secara visual, seperti komputer, *handphone*, kamera, CD, *hard disk*, dll., Sedangkan alat bukti digital berupa alat bukti yang diekstrak atau diperoleh kembali dari alat bukti elektronik, bukti tersebut dapat berupa *file*, *email*, pesan, gambar, video, *log* maupun teks [6].

Menurut [7], beberapa kasus yang menggunakan kamera CCTV masih terdapat ketidakpastian terhadap penggunaan CCTV apakah CCTV tersebut dapat dijadikan sebagai alat bukti atau sebagai barang bukti. 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 merupakan alat bukti digital yang sah dan memiliki sebuah file rekaman yang memberikan sebuah informasi berupa data atau yang biasa dikenal dengan istilah metadata[8], dimana metadata dapat direkam komputer secara otomatis saat sebuah file dibuat, sehingga bisa diketahui kapan file dibuat, siapa user pembuatnya, berapa ukuran filenya, dan juga ekstensinya. Informasi metadata berfungsi untuk menyimpan, menjaga[9], 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* [10] merupakan upaya untuk menjaga dan memastikan integritas dalam bukti digital dan prosedur pendokumentasian bukti secara kronologis sejak pertama ditemukan di tempat kejadian perkara (TKP) untuk menjelaskan 5 karakteristik (4W dan 1 H) *Chain of Custody*, yaitu *fingerpint of evidences (why)*, *digital signing (who)*, *time stamping (when)*, *geo location (where)* dan *procedures (how)*.

Selanjutnya, dalam mencari 5 karakteristik *Chain of Custody* pada rekaman kamera CCTV diperlukan sebuah metode investigasi NIST (*National Institute of Standards Technology*) [11] yang digunakan untuk mengumpulkan barang bukti digital untuk merekonstruksi suatu tindak kejadian perkara agar dapat mendapatkan informasi terstruktur dari rekaman kamera CCTV, dengan demikian metode investigasi digital forensik dapat memberikan informasi yang terstruktur untuk menggambarkan, menjelaskan, menggunakan dan menempatkan sebuah informasi forensik metadata rekaman kamera CCTV untuk digunakan dalam pembuktian di persidangan.

2. METODE PENELITIAN

Pada penelitian ini, metode penelitian akan dilakukan akuisi berdasarkan pedoman dan persyaratan dalam Standar Nasional Indonesia (SNI) 27037:2014[12]. Beberapa penelitian sebelumnya telah menggunakan prosedur akuisisi sesuai dengan SNI 27037:2014 dengan metode proses investigasi NIST (*National Institute of Standards Technology*) yang digunakan untuk menganalisis metadata rekaman kamera CCTV sebagai alat bukti digital. Gambar 1 merupakan tahapan pemeriksaan dan analisis yang akan dilakukan.

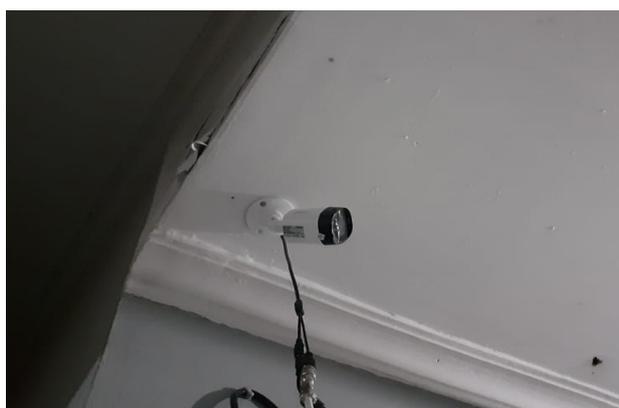


Gambar 1. Alur Proses NIST

Proses NIST yang terdiri dari beberapa tahapan yaitu tahap *collection* (pelabelan) atau 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, *examination* (pengolahan data) atau 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, untuk itu pada file digital perlu dilakukan identifikasi dan validasi file dengan teknik *hashing*, pada proses *examination* ini dilakukan pengujian dengan menggunakan *tools* forensik yaitu MediaInfo dan Exif tool yang digunakan untuk mencari informasi metadata kamera CCTV. Selanjutnya tahap *analysis* (analisis hasil pemeriksaan) atau tahap meneliti ini 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 dipertanggung jawabkan secara ilmiah dan secara hukum., dan *reporting* (pelaporan) atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis hasil dari kasus yang sedang diselidiki yang digunakan sebagai barang bukti yang sah.

2.1. Persiapan Sistem

Merupakan tahap pemasangan alat dan implementasi kamera CCTV yang akan digunakan sebagai objek penelitian. Kamera CCTV menggunakan Merek Dahua, dengan 4 *Channel* dan selanjutnya akan di pasang pada sebuah rumah dibagian belakang. Pada gambar 1 merupakan titik lokasi kamera CCTV yang digunakan untuk simulasi kasus.



Gambar 1. Titik Kamera CCTV

2.2. Simulasi Kasus

Merupakan tahap dilakukannya simulasi kasus yang ditangkap oleh kamera CCTV. Simulasi kasus bertujuan untuk melakukan pengujian hasil rekaman kamera CCTV untuk mendapatkan hasil metadata rekaman CCTV.

2.3. Pengumpulan Data

Tahap pengumpulan data yang akan dilakukan analisis digital forensik terkait rekaman kamera CCTV terbagi dalam beberapa langkah, yaitu:

2.3.1. Dokumentasi

Dokumentasi dilakukan untuk mencatat temuan yang diperoleh selama proses pengumpulan barang bukti berupa time display atau catatan waktu tertampil dalam rekaman untuk memastikan waktu kejadian yang bersangkutan dapat dilihat pada tabel 1:

Time Display	Keterangan
Waktu Kejadian	09/08/2020
Pukul	23:19 WIB

2.3.2. Informasi Seputar Alat Rekam

Pada informasi seputar alat rekam pada penelitian ini menggunakan jenis kamera *stand alone* dengan jenis DVR, pada jenis DVR [13] terpasang sebuah PC1 DVR card yang mampu dipasang kamera berdasarkan dari jumlah *channel* yang tersedia umumnya berjumlah 4 *channel* hingga 32 *channel* dan memiliki *motherboard*, *network card*, *VGA card*, *CPU*, *hard drive* dan *memory*. Tabel 2 merupakan informasi seputar alat rekam yang digunakan untuk simulasi kasus pada penelitian ini.

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

3. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan dengan menggunakan metode NIST dalam melakukan investigasi rekaman kamera CCTV. Berdasarkan simulasi kasus yang terekam kamera CCTV, investigator melakukan tahap NIST dengan transformasi pertama kali dilakukan simulasi kasus, kemudian mengumpulkan data yang akan diperiksa, selanjutnya akan di ekstrak data dari media kamera CCTV dengan mengubahnya menjadi format yang dapat di proses oleh alat forensik yang terbagi menjadi 4 tahapan.

3.1. Collection

Tahap collection merupakan tahap mengidentifikasi, pelabelan, rekaman serta pengambilan data dari sumber data yang relevan secara prosedural agar tetap terjaga integritas dari data yang di dapat dari rekaman kamera. Pelabelan alat bukti pada penelitian ini didapat dari jenis kamera CCTV stand alone jenis DVR yang merupakan jenis perangkat elektronik perekam video menjadi format digital ke dalam media seperti HDD, USB Flash Disk, SSD maupun CD [14] [15].



Gambar 2. Kamera CCTV yang digunakan

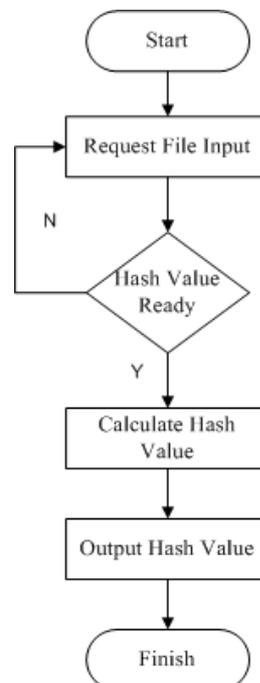
Pada gambar 2 merupakan kamera CCTV yang digunakan dalam penelitian ini dengan tipe jenis kamera yang dapat dilihat pada tabel 3 berikut:

Tabel 3. Jenis Kamera CCTV

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

3.2. Examination

Setelah mengidentifikasi dan pelabelan barang bukti hal paling utama ialah melakukan *hashing*. Dimana *hashing* dilakukan untuk menjaga integritas data dari data yang berasal dari bukti digital. *Hashing* [17] pada bagian ini merupakan teknik algoritma yang digunakan pada bagian data untuk menciptakan sebuah data yang unik dengan ketentuan panjang variabel yang tetap. Pada gambar 3 merupakan langkah untuk mendapatkan nilai *Hash* investigasi digital forensik dari alat bukti kamera CCTV.



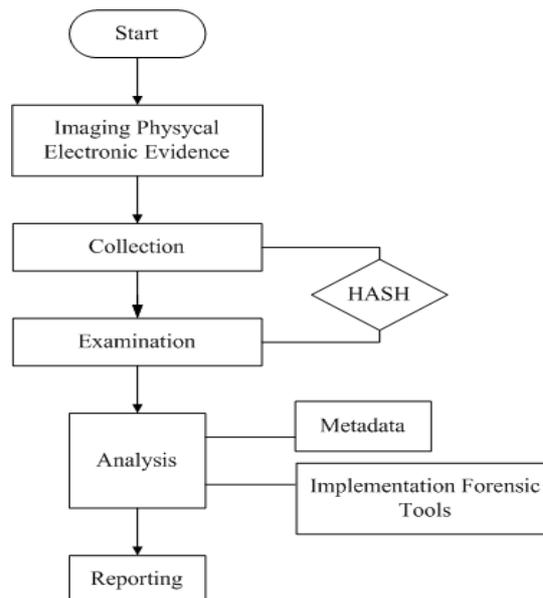
Gambar 3. Autentication Hash Value

Gambar 4 menunjukkan hasil *hashing* dari bukti digital rekaman kamera CCTV didapatkan dengan *file* berekstensi MD5 (*Message Digest algorithm 5*) dengan panjang 32 karakter.

7789fcfbcb0efd516d0297a29a513214

Gambar 4. *Hash Value*

Berikutnya adalah proses examination yang merupakan tahap pengujian dan pengolahan data yang dikumpulkan dengan menggunakan *tools* forensik dari MediaInfo dan ExifToll [16]. Tahapan ini dapat dilihat pada gambar 5 dengan proses akuisisi bukti fisik dari kamera CCTV untuk mendapatkan file video rekaman yang selanjutnya akan dilakukan pengujian terhadap bukti digital.



Gambar 5: *Core Acquisition*

Pengujian pertama untuk mendapatkan sebuah informasi menggunakan *tools* MediaInfo yang dapat dilihat pada gambar 6 dibawah ini:

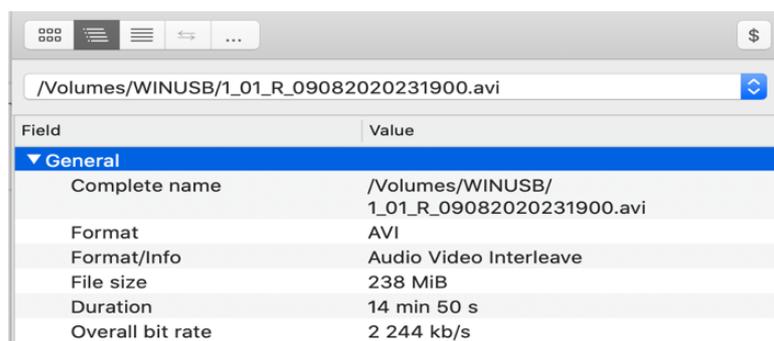


Gambar 6. *Examination Process*

3.3. Analysis

Pada tahap analysis (analisis) dari hasil pemeriksaan dengan menggunakan metode teknis yang nantinya dapat digunakan dalam persidangan adalah proses analisis forensik rekaman kamera CCTV menggunakan *tools* forensik yang pertama menggunakan MediaInfo didapatkan informasi tentang isi kamera CCTV berupa data atau yang sering disebut sebagai metadata yang dapat menjelaskan isi informasi, menggambarkan informasi yang terstruktur dari sumber data agar dapat dipahami informasi tersebut pada file yang diperoleh dari rekaman kamera.

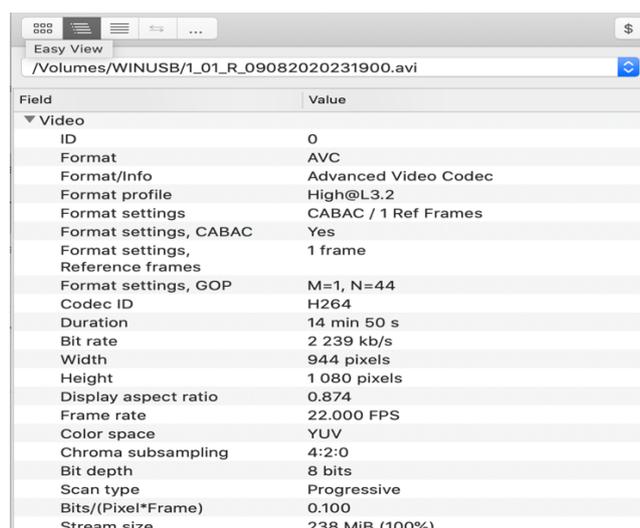
Analisis menggunakan tool forensik yang didapat dari metadata berupa *header*, isi dan *footer*. Pada bagian header terdapat informasi pertama sebelum isi file, sedangkan untuk footer terletak pada akhir sebelum adanya isi informasi. Metadata pada bagian *header* video kamera CCTV berisikan *file signature* data yang digunakan untuk mengidentifikasi dan memverivikasi isi dari sebuah file yang berisikan metadata tentang informasi umum, *codec* video dan *codec* audio[18].



Field	Value
General	
Complete name	/Volumes/WINUSB/ 1_01_R_09082020231900.avi
Format	AVI
Format/Info	Audio Video Interleave
File size	238 MiB
Duration	14 min 50 s
Overall bit rate	2 244 kb/s

Gambar 7. Informasi *Header* Metadata

Gambar 7 diatas merupakan informasi *header* metadata *file* video rekaman kamera yang berisi tentang informasi umum dengan nama file 1_01_R_09082020231900.avi menggunakan format .AVI (*Audio Video Interleave*), berukuran file 238 MiB dengan durasi 14 menit 50 detik dan memiliki *overall bit rate* 2 244 kb/s. Pada informasi isi metadata file di dapat tentang kompresi video yang berisikan *codec* yang menggunakan format AVC serta panjang video x lebar video beresolusi 944 pixels serta memiliki frame rate 22.000 FPS dengan ukuran stream berupa gambar 8 berikut :

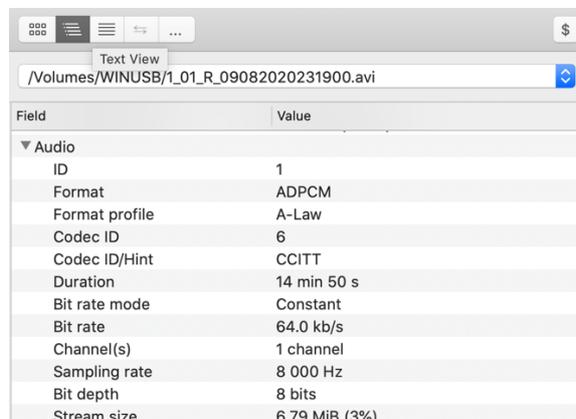


Field	Value
Video	
ID	0
Format	AVC
Format/Info	Advanced Video Codec
Format profile	High@L3.2
Format settings	CABAC / 1 Ref Frames
Format settings, CABAC	Yes
Format settings, Reference frames	1 frame
Format settings, GOP	M=1, N=44
Codec ID	H264
Duration	14 min 50 s
Bit rate	2 239 kb/s
Width	944 pixels
Height	1 080 pixels
Display aspect ratio	0.874
Frame rate	22.000 FPS
Color space	YUV
Chroma subsampling	4:2:0
Bit depth	8 bits
Scan type	Progressive
Bits/(Pixel*Frame)	0.100
Stream size	238 MiB (100%)

Gambar 8. Informasi Isi Metadata

Forensik rekaman kamera CCTV diperlihatkan dari hasil ekstrak tool forensik tentang *codec* audio yang digunakan berisikan format code untuk menerjemahkan biner kedalam *pixel* untuk dalam menerjemahkan data visual berupa format AVC (*advanced Video Codec*). Setelah mendapatkan informasi metadata terkait *codec* video [19] 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 mendapatkan 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 8 dibawah ini merupakan informasi metadata dari *codec* audio rekaman kamera CCTV.



Field	Value
▼ Audio	
ID	1
Format	ADPCM
Format profile	A-Law
Codec ID	6
Codec ID/Hint	CCITT
Duration	14 min 50 s
Bit rate mode	Constant
Bit rate	64.0 kb/s
Channel(s)	1 channel
Sampling rate	8 000 Hz
Bit depth	8 bits
Stream size	6.79 MiB (3%)

Gambar 9. Informasi Isi *Footer*

Selain mendapatkan informasi terkait isi dari metadata video, forensik metadata rekaman kamera CCTV didapatkan informasi *live data* menggunakan *ExifTool* yang berupa informasi *timestamps* [20] 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:



```

Desti-MacBook-Pro:~ dest.te$ exiftool /Volumes/WINUSB/1_01_R_09082020231900.avi
ExifTool Version Number      : 12.03
File Name                    : 1_01_R_09082020231900.avi
Directory                   : /Volumes/WINUSB
File Size                    : 238 MB
File Modification Date/Time  : 2020:08:09 23:38:02+07:00
File Access Date/Time       : 2020:10:22 00:00:00+07:00
File Inode Change Date/Time  : 2020:08:09 23:38:02+07:00

```

Gambar 10. *Timestamp 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* 22-10-2020 pukul 00:00:00+07:00 dengan keterangan catatan ketika sebuah *file* dibaca atau diakses didalam sebuah sistem, sedangkan *file Inode Change Date/Time* merupakan informasi kejadian saat simulasi kasus berlangsung pada tanggal 09-08-2020 Pukul 23:38:02 +07:00.

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.



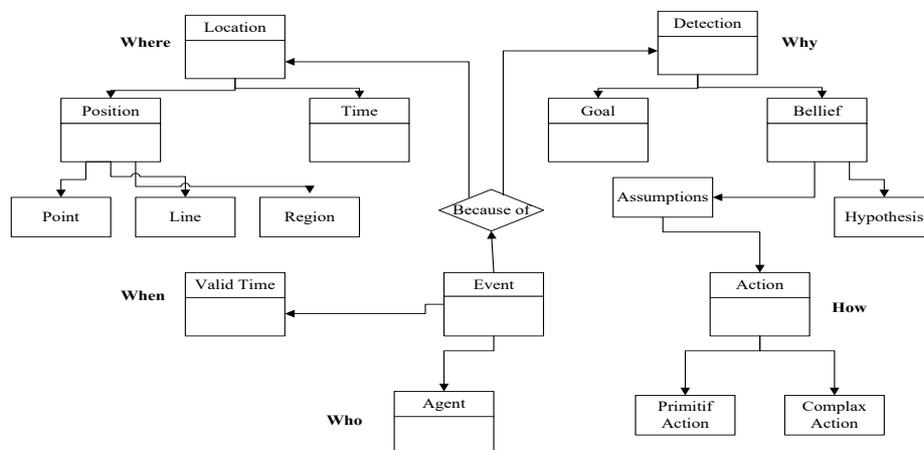
Gambar 11. Isi Kronologis

3.4. Reporting

Pada bagian *reporting* ialah melaporkan hasil analisis yang meliputi gambaran tindakan yang didapat dari file rekaman kamera CCTV berupa metadata yang berisi informasi yang didapat untuk di implemetasikan kedalam dokumen *Chain of Custody* yang menjelaskan detail catatan perjalanan barang bukti dan siapa saja yang bertanggung jawab terhadap bukti digital tersebut, *Chain of Custody* dilakukan untuk mengetahui aktivitas dan temuan yang diperoleh selama proses investigasi forensik. Semua catatan perjalanannya harus terdokumentasi dengan baik.

Sementara itu [18] memodelkan proses interaksi chain of custody meliputi 5 pelaku berbeda, yaitu: first responder, investigator, prosecutor, defense dan court. Menurut [19], 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 terdapat barang bukti elektronik berupa 3 (tiga) kepingan CD rekaman CCTV yang tidak mempunyai kekuatan hukum yang mengikat dikarenakan tidak diajukannya alat bukti surat yang merupakan hasil proses hashing [20] yang dicetak dalam bentuk surat untuk melihat keaslian dari suatu file. Hal ini menunjukkan bahwa pihak pengadilan tidak bisa menerima bukti yang diserahkan jika mereka tidak bisa memastikan bagaimana bukti tersebut ditangani.

Dari perkara tersebut Chain of Custody digunakan sebagai “A Road Map That Shows how evidence was collected, analyzed and preserved in order to presented as evidence in court” [21]. Pada gambar 12 merupakan implementasi pendokumentasian kronologis dari bukti digital kamera CCTV dapat memenuhi 5 ketentuan karakter *chain of custody* 4W dan 1 H yaitu: *why, who, when, where* dan *how*.



Gambar 12. Kerangka Chain of Custody

Pada saat persidangan bukti yang diajukan tidak akan diragukan lagi karena semua proses investigasi barang bukti tersebut telah terdokumentasi dan tidak ada unsur barang bukti telah dimanipulasi. Gambar 13 merupakan hasil dokumen *Chain of Custody* rekaman kamera CCTV dengan menggunakan metode NIST diperoleh informasi metadata sebagai berikut:

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 Confirmed .avi		
	Hash Number : 7789fcfbc0efd516d0297a29a513214		

Gambar 13. Dokumen *Chain of Custody*

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 4 merupakan hasil laporan catatan analisis metadata pada rekaman CCTV berupa:

No.	Identifikasi	Keterangan
1	Seputar Tipe Alat Rekam	CCTV Stand Alone DVR Compressor Name Handler Description
2	Waktu Kejadian Dalam File	2020:08:09
3	Nama Rekaman	1_01_R09082020239000.avi
4	Format File	MP4 Video/x-msvideo
5	Durasi	0:14:50
6	Serial Number	221C10F2087C1924
7	Record Channel	Channel 4
8	Kualitas Video	Default
9	Frame Rate	124.5 KB/S

10	Frame Record Size	Width x Height=944 x 1080
11	Kapasitas	238 MB
12	Firmware	Probing DNS Code 0:/0/+000
13	Timestamps	Date/time Actual 09:08:2020 Pukul 23:38:02+07:00
14	Lokasi TKP	Jl. Melati Indah

4. KESIMPULAN

Penelitian ini adalah sebuah upaya untuk mendapatkan bukti digital rekaman kamera CCTV yang di terapkan menggunakan metode NIST (*National Institute of Standarts Technolog*) untuk investigasi digital forensik terkait rekaman kamera CCTV agar memperoleh informasi metadata file untuk dapat di implementasikan serta mengolah sebuah sumber informasi untuk dijadikan sebagai barang bukti yang diimplementasikan menggunakan dokumen *Chain of Custody* agar intergitas bukti digital tetap terjaga utuh dari awal ditemukan sampai di analisis informasi yang terdapat pada kamera CCTV, dengan demikian informasi alat bukti yang didapat dari rekaman kamera CCTV dapat diterima dan digunakan untuk memperkuat alat bukti dalam persidangan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Ristek Dikti yang telah memberi dukungan financial terhadap penelitian ini.

DAFTAR PUSTAKA

- [1] 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.
- [2] A. Iswardani and N. Arif, "Forensic Readiness Analysis of CCTV System in Surakarta," *Int. J. Comput. Appl.*, vol. 177, no. 30, pp. 36–38, 2020, doi: 10.5120/ijca2020919786.
- [3] D. Y. Sari, "Deteksi Keaslian Video Pada Handycam Dengan Metode Localization Tampering," *J. Online Inform.*, vol. 2, no. 1, p. 10, 2017, doi: 10.15575/join.v2i1.85.
- [4] M. N. Al Azhar, *Praktical Guidelines for Computer Investigation*. 2529.
- [5] 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.
- [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] 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.
- [9] 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.
- [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/ijarsse.v7i7.109.
- [11] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.
- [12] 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.
- [13] 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.

- [14] W. Pranoto, I. Rladi, 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.
- [15] 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>.
- [16] 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/ICACTION.2017.7890148.
- [17] J. L. J. Carter and M. M. N. M. Wegman, "Classes of Hash Functions," *J. Comput. Syst. Sci.*, pp. 143–154, 1979, [Online]. Available: <http://www.sciencedirect.com/science/article/pii/0022000079900448>.
- [18] 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.
- [19] G. Wicaksono and Y. Prayudi, "Teknik Forensika Audio Untuk Analisa Suara Pada Barang Bukti Digital," *Semnas Unjani*, 2013.
- [20] 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.
- [21] G. Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," *Int. J. Comput. Sci. Netw. Secur.*, vol. 11, no. 1, pp. 1–9, 2011.
- [22] Shahraki, A. S., Sayyadi, H., & Amri, M. H. (2013). Survey: Video Forensic Tools, 47(1), 98–107.
- [23] Satti, R. S., & Jafari, F. (2015). Domain Specific Cyber Forensic Investigation Process Model. *Journal of Advances in Computer Networks*, 3(1), 75–81. <https://doi.org/10.7763/JACN.2015.V3.145>.
- [24] Y. Prayudi, "Problema dan Solusi Digital Chain Of Custody dalam Proses Investigasi Cybercrime," 2014.

BIOGRAFI PENULIS



Desti Mualfah memperoleh gelar Sarjana Komputer Teknik Informatika pada Tahun 2014 di Universitas Muhammadiyah Magelang dan mendapatkan gelar Magister Komputer Teknik Informatika di Universitas Islam Indonesia pada Tahun 2017. Saat ini sebagai Dosen pada Universitas Muhammadiyah Riau, selain itu aktif melakukan penelitian di bidang Digital Forensik, *Network Security* dan *Networking*. Memiliki lisensi dan sertifikat CEH (*Certified Ethical Hacking*) dan CHFI (*Computer Hacking Forensic Investigator*). Penulis dapat dihubungi melalui email: destimualfah@umri.ac.id



Rizdqi Akbar Ramadhan memperoleh gelar Sarjana Komputer Teknik Informatika pada Tahun 2013 di Universitas Islam Indonesia dan mendapatkan gelar Magister Komputer Teknik Informatika pada Tahun 2017 di Universitas Islam Indonesia. Saat ini sebagai Dosen di Universitas Islam Riau, selain itu aktif melakukan penelitian di bidang Digital Forensik. Memiliki lisensi dan sertifikat CHFI (*Computer Hacking Forensic Investigator*). Penulis dapat dihubungi melalui email: rizdqiramadhan@eng.uir.ac.id