Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 3 Nomor 2 September 2019, pp. 193-200
ISSN:2548-9771/EISSN:2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Analisis *Forensic*s Untuk Mendeteksi Pemalsuan Video

Rusydi Umar[1], Abdu Fadlil[2], Alfiansyah Imanda Putra[3]
[1,3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta, Indonesia
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan Yogyakarta, Indonesia
Jalan Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia
rusydi@mti.uad.ac.id(1), fadlil@mti.uad.ac.id(2), alfian.imandaputra@gmail.com(3)

Abstract

The current technology is proving that the ease with which crimes occur using computer science in the field of video editing, in addition from time to time more and more video editing software and increasingly eassy to use, but the development of this technology is widely misused by video creators to manipulate video hoaxes that cause disputes, so many video cases are spread which cannot be trusted by the public. Counterfeiting is an act of modifying documents, products, images or videos, among other media. Forensic video is one of the scientific methods in research that aims to obtain evidence and facts in determining the authenticity of a video. This makes the basis of research to detect video falsification. This study uses analysis with 2 forensic tools, forevid and VideoCleaner. The result of this study is the detection of differences in metadata, hash and contrast of original videos and manipulated videos.

Keywords*: Videos, Digital Forensics, Video Forensics, Forensic Tools*

Abstrak

Pesatnya teknologi saat ini membuktikan bahwa mudahnya terjadi kejahatan yang menggunakan ilmu komputer dalam bidang video editing, selain itu juga dari waktu ke waktu semakin banyak softwere editing video dan semakin mudah digunakan, namun perkembangan teknologi ini banyak disalah gunakan oleh oknum video creator untuk memanipulasi video hoax yang menyebabkan perselisihan, sehingga banyak kasus- kasus video tersebar yang tidak bisa dipercaya begitu saja oleh masyarakat. Pemalsuan merupakan suatu tindakan memodifikasi dokumen, produk, gambar atau video, di antara media lain. Video forensic merupakan salah satu metode ilmiah dalam penelitian yang bertujuan untuk mendapatkan bukti- bukti dan fakta dalam menentukan keaslian video. Hal ini menjadikan dasar penelitian untuk mendeteksi pemalsuan video. Penelitian ini menggunakan analisa dengan 2 tools forensic yaitu forevid dan VideoCleaner. Hasil daripenelitian ini adalah terdeteksinya perbedaan metadata,hash dan kontras video asli dan video yang telah di manipulasi.

Kata kunci: *Video, Digital Forensic,Video Forensic,Tools Forensic*

1. PENDAHULUAN

Perkembangan teknologi digital pengolahan video dan kemampuan komputasi suatu *computer* yang sangat pesat membuat media digital sangat mudah untuk di manipulasi. Ditambah dengan banyaknya perangkat lunak pengolahan video yang mempermudah seseorang untuk melakukan manipulasi dan perusakan keaslian video yang didapat sesuai dengan kebutuhan yang diinginkan. Keberadaan barang bukti sangat penting dalam melakukan investigasi sebua kasus computer crime maupun related crime, karena dalam barang bukti inilah investigator dan analisis forensic dapat megungkap sebuah kasus yang terjadi dengan kronologis lengkap untuk selanjutnya melacak keberadaan pelaku dan menangkapnya [1].

Video yang telah dimanipulasi dapat digunakan untuk berbagai macam tujuan pelakunya, mulai dari iklan, hiburan, kriminal hingga untuk mengelabui penyidik. Sedangkan dari sisi pembaca konten, seperti pada kasus kriminal, adalah penyidik, video yang telah dimanipulasi dapat menyesatkan penyelidikan dan berujung pada penangkapan pelaku yang salah. Pada kasus pornografi, gambar dan video yang dimanipulasi dapat merusak nama dan reputasi seseorang hingga perusahaan. Mereka yang terkena dampak negatif dari manipulasi gambar dan video adalah korban yang jumlahnya banyak karena siapapun bisa menjadi korban [2].

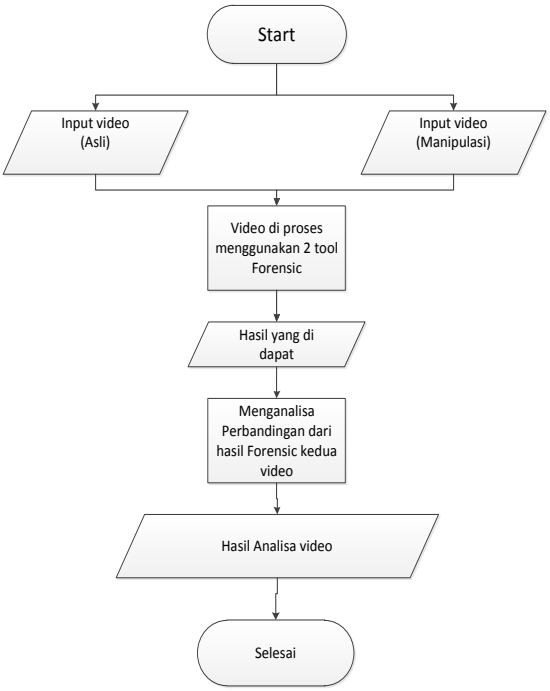
Setiap kali video dijadikan sebagai barang bukti dalam persidangan pengadilan, diperlukan proses autentifikasi video sebelum dijadikan sebagai barang bukti, karena itu video sangat penting untuk dijadikan sebagai sumber utama sebuah informasi. Berbagai perangkat lunak editing video yang semakin berkembang pesat menyulitkan seseorang untuk membedakan antara video asli dan video palsu [3].Berikut ini adalah contoh peristiwa mengapa identifikasi pemalsuan video perlu dilakukan : Sebuah frame video dapat dirusak atau dimanipulasi dengan berbagai cara, hal ini digunakan untuk mencemarkan nama baik seseorang, penjahat sering dibebaskan karena video yang digunakan sebagai barang bukti kejahatan tersebut telah dimanipulasi [4].

Istilah *forensisc* dapat didefinisikan sebagai penerapan sebuah ilmu pengetahuan untuk menyelesaikan kasus hukum. Definisi paling popular tentang digital *forensics* berasal dari definisi *computer forensic*s yaitu teknik pengumpulan, analisis, dan penyajian barang bukti elektronik yang digunakan untuk menyelesaikan suatu kasus hokum dalam persidangan [5]. Digital forensik merupakan ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital adalah hasil ekstrak dari barang bukti elektronik seperti Personal *Computer*, *Mobile Phone, notebook,* server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa sebagai barang bukti [5]. Metadata merupakan suatu informasi terstruktur yang menggambarkan, menjelaskan, menempatkan, atau membuat lebih mudah untuk menggunakan atau mengelola sebuah sumber informasi [6]. Metadata adalah informasi yang ditanam pada sebuah file tersebut. Metadata mengandung informasi mengenai isi dari suatu data yang dipakai untuk keperluan manajemen file atau data itu nantinya dalam suatu basis data. Pendit, Putu Laxman [7]. Penelitian yang akan dilakukan merupakan penelitian lanjutan dari penelitian yang sebelumnya oleh Alfiansyah Imanda Putra, Rusydi Umar dan Abdul Fadlil di tahun 2018 dengan judul "Analisi Forensik Deteksi Keaslian Video menggunakan *Exiftool*"[8]. Sedangkan penelitian yang dilakukan ini mengggunakan 2 tool *Forensic*, yaitu Forevid dan *VideoCleaner.*

2. METODOLOGI PENELITIAN

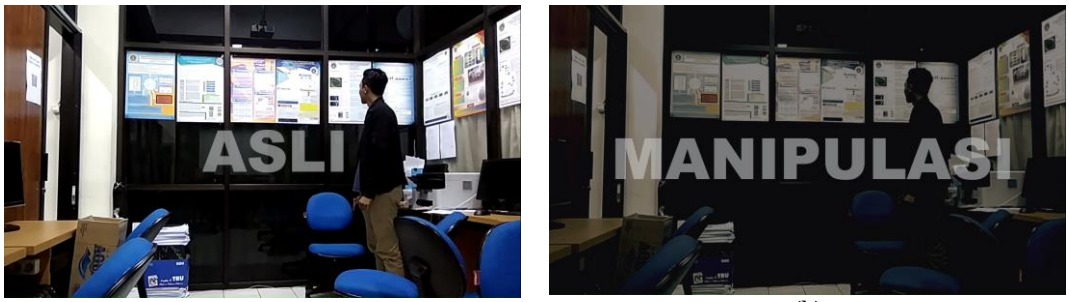
Penelitian ini menggunakan skema sendiri untuk melakukan proses pendeteksi video dalam mendapatkan sebuah bukti digital yang akan

digunakan untuk dianalisa. Gambar 1 merupakan skema Flowchart dalam proses forensic pendeteksian.



Gambar 1. *Flowchart* proses pendeteksi.

Parameter yang digunakan dalam pendeteksi pemalsuan video ini adalah Hash analis, Metadata dan perbedaan kontras antara video manipulasi dan video asli. Penelitian ini menggunakan 2 buah *tools forensics,* yaitu *Forevid* untuk melakukan hash analis dan metadata, *VideoCleaner* untuk menganalisis penyisipan objek pada video manipulasi dengan memanfaatkan *forensics* filters. Gambar 2. Merupakan bahan penelitian yaitu, video asli dan video yang telah di manipulasi dengan menyisipkan objek video lain dan merubah kontras video.



(a) (b)

Gambar 2. Video bahan penelitian (a) Asli (b) manipulasi / Video editan

3. HASIL DAN PEMBAHASAN

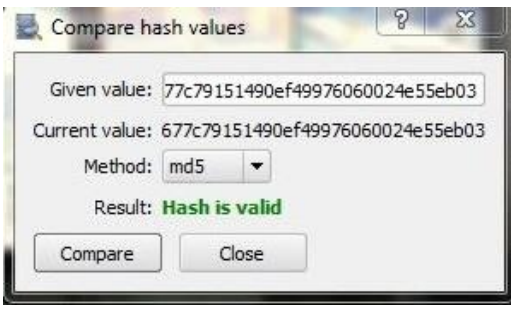
Proses pendeteksi diawali dengan membuat sekenario berupa menyiapkan 2 video yang merpakan 1 video asli dan 1 video yang telah diedit atau dimanipulasi kemudian semua video tersebut diproses dengan menggunakan 2 tools yang sudah disiapkan. Hasil dari proses 2 tools tersebut adalah sebagai berikut.

3.1. Forevid

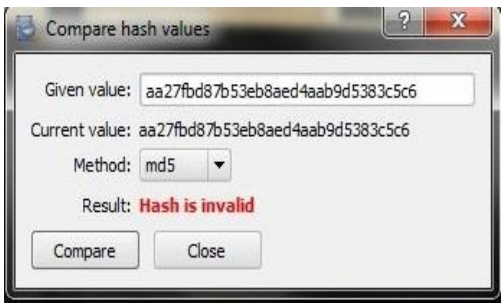
Percobaan pertama dilakukan dengan menggunakan tools *Forevid yaitu* perangkat lunak pemrosesan video forensik yang berfungsi untuk menganalisis video foresic. *ForeVid* menggunakan *Avisynth* sebagai alat pembuka dan pengeditan video.. Perangkat lunak *ForeVid* dibuat menggunakan bahasa pemrograman *Python. GUI* dibuat menggunakan *PyQt* 4.0 yang merupakan *Qt GUI-library* dimoderasi untuk *Python* (Hautamaki 2011)[9].

3.1.1. Analisa *hash*

Tools ForeVid dapat digunakan untuk menganalisa *hash*. Nilai *hash* adalah hasil perhitungan yag dapat dlakukan pada stringteks, file elektronik atau seluruh isi harddisk. Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (*fixed*). Fungsi hash dapat menerima masukkan string apa saja. [10] Hasilnya dapat disebut *checksum*, kode *hash* atau *hash*. Nilai hash digunakan untuk mengidentifikasi image forensic atau cloning yang dilakukan berhasil dan tidak ada perubahan sedikitpun.. Berikut ini adalah hasil dari *ForeVid*.



Gambar 3. Informasi *Hash* video asli

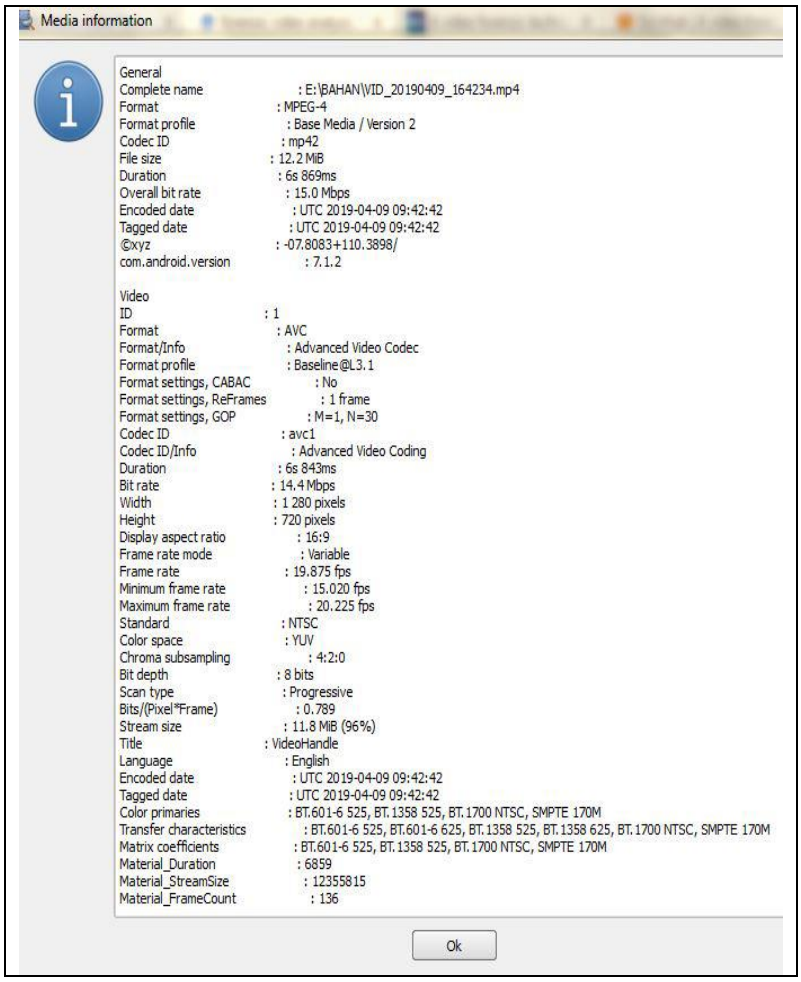


Gambar 4. Informasi *Hash* video manipulasi.

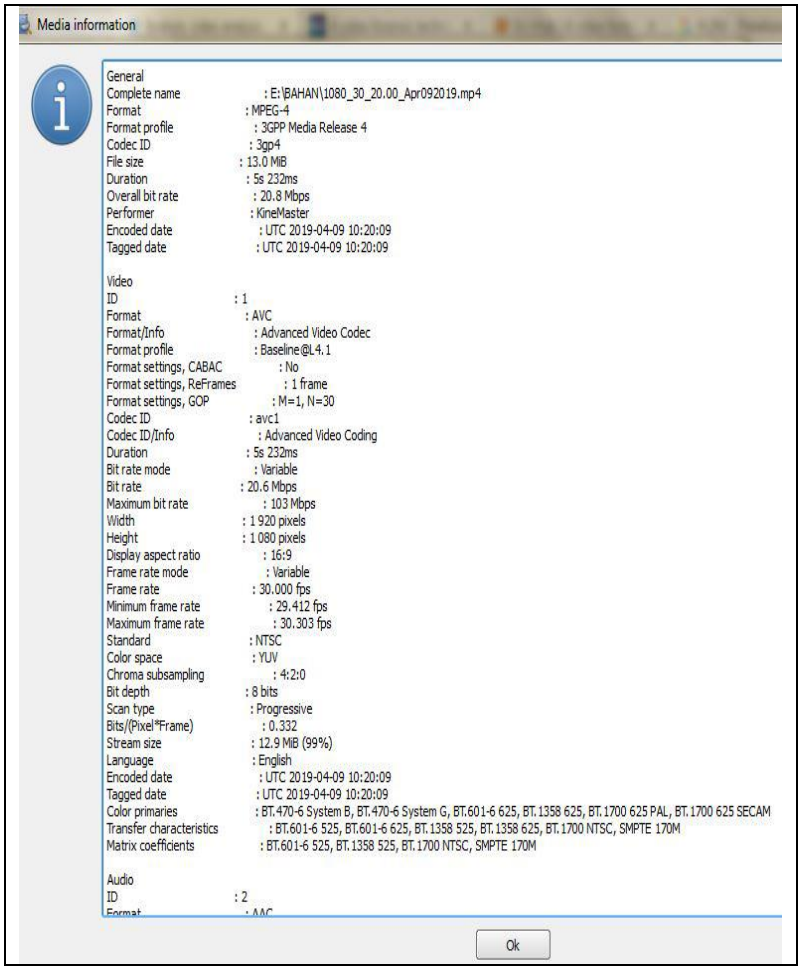
Gambar 3. Menunjukan hasil informasi *hash* pada video asli, menunjukan *hash is valid* yang berarti pada video tersebut tidak ada kecurigaan atau perubahan. Sedangkan di gambar 4 menunjukan informasi *hash* dari video yang telah dimanipulasi, menunjukan informasi *hash is invalid* yang berarti video telah di edit atau telah dilakukan perubahan.

3.1.2. Analisa Metadata

Penelitian *Forevid* selanjutnya adalah dengan menganalisa perbedaan metadata dari video asli dan video yang sudah dimaniulasi . Gambar 5 merupakan hasil proses menggunakan *forevid* menggunakan teknik analisis metadata. Terlihat perbedaan data yang tertera pada metadata pada metadata vide maniulasi tertera performer : *KineMaster*, menunjukan bahwa video tersebut telah mengalami pengeditan menggunaan software *KineMaster*, pada pixel juga menunjukan perbedaan yang sangat sangant jelas,selanjutnya perbedaan pada informasi frame video manipulasi, pada metadata, menunjukan bahwa video manipulasi telah disisipkan frame.



Gambar 5. Hasil metadata video asli

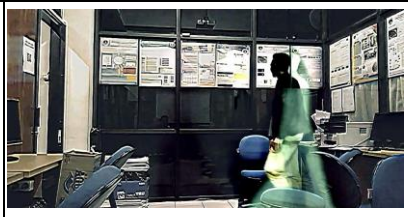


Gambar 6. Hasil metadata video asli.

Gambar 5 dan 6 memmnunjukan hasil setelah diproses dengan menggunakan *Forevid*, jelas terlihat perbedaan pada metadata tersebut. Pada baris ke 8 terlihat informasi performer : *KineMaster* . Hal tersebut menunjukan bahwa video sudah pernah di edit menggunakan software *Kinemaster.*

3.2. Video Cleaner

Percobaan tools kedua yaitu dengan menggunakan tools *VideoCleaner,* yaitu sebuah tools *offline* video forensic yang digunakan untuk menganalisis video dengan menggunakan forensic filters yang ada didalamnya. Berikut ini adalah hasil dari tools *VideoCleaner* :

Analysis	
Original Video	Video Tampering
	
Frame 32	Frame 32
	
Frame 36	Frame 36
	
Frame 60	Frame 60

Gambar 7. *Hasil VideoCleaner*

Gambar 3. Meununjukan hasil setelah diproses menggunakan *VideoCleaner* dengan menganalisis video tampering pada video dengan memanfaatkan *Forensic Filters* yang ada di V*ideoCleaner* . Dari sample frame diatas terlihat jelas perbedaan kontras dan terlihat video yang telah di sisipkan objek dengan menggunakan *greenscren.*

4. SIMPULAN

Kesimpulan yang didapat dari penelitian ini adalah *tools* yang sudah digunakan dari ketiga *tools* dapat memberikan hasil pendeteksian. Komparasi ketiga *tools* berhasil dilakukan dengan masing-masing analisis yang sudah berjalan, sehingga didapat hasil pendeteksian foto. Bahan foto yang digunakan masih menggunakan foto asli dan foto manipulasi yang diedit dari foto asli, bukan dari foto yang sudah beredar di media sosial dan internet

Saran untuk penelitian selanjutnya adalah menggunakan foto yang beredar di media sosial dan internet sehingga cukup menggunakan 1 foto sudah bisa mendeteksi kepalsuan foto tersebut. Sehingga diharapkan dapat menggunakan

tools dan teknik yang berbeda sehingga dapat mencari perbandingan *tools image forensics* yang terbaik.

DAFTAR PUSTAKA

[1] I. Riadi and A. Firdonsyah, "Identification Of Digital Evidence On Android ' s Blackberry Messenger Using Identification Of Digital Evidence On Android ' s Blackberry Messenger Using NIST Mobile," no. May, 2017.
[2] C. Sahera, D. M. Analisis, F. Analisis, and P. Analisis, "Forensik Gambar dan Video."
[3] C. Feng, Z. Xu, W. Zhang, and Y. Xu, "Automatic Location of Frame Deletion Point for Digital Video Forensics," pp. 171–179, 2014.
[4] R. C. Pandey, S. K. Singh, and K. K. Shukla, "Passive Copy- Move Forgery Detection in Videos," pp. 301–306, 2014.
[5] W. A. Mukti, S. U. Masruroh, D. Khairani, and B. Forensik, "Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada Smartphone Android," vol. 10, no. 1, 2017.
[6] Y. Vanda, S. A. Cahyono, T. Elektronika, and T. Elektronika, "Konsep Metadata Untuk Aplikasi E-Learning," pp. 76–88, 2015.
[7] A. Pendahuluan, "MODS Metadata Alternatif dalam Pengembangan Aplikasi," pp. 1–15, 2012.
[8] T. Pustaka, "Analisis forensik deteksi keaslian metadata video menggunakan exiftool," vol. 2018, no. November, pp. 21–25, 2018.
[9] D. Moreira, A. Bharati, S. Member, J. Brogan, and S. Member, "Image Provenance Analysis at Scale," no. September, 2018.
[10] P. F. H. Satu-arah, "Penggunaan fungsi," vol. 7, no. 3, pp. 138–146, 2008.