ANALISIS FORENSIK DETEKSI KEASLIAN METADATA VIDEO MENGGUNAKAN EXIFTOOL

Alfiansyah Imanda Putra [(1)], Rusydi Umar [(2)], Abdul Fadlil [(3)]
[(1)(2)(3)] Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta
Yogyakarta, Indonesia
e-mail : alfian.imandaputra@gmail.com

Abstrak
Pesatnya perkembangan teknologi sekarang menyebabkan sering terjadinya penyalahgunaan sistem kinerja komputer yang banyak dimaanfaatkan sebagai salah satu tindak kejahatan memanipulasi video yang merugikan dan memprovokasi pihak lain. Digital Forensik atau komputer forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tools untuk mengekstrak dan memelihara barang bukti tindakan kiriminal. Metadata berisikan informasi yang menjelaskan karakteristik suatu data, terutama isi, kualitas, kondisi dan cara perolehannya. Dalam penelitian ini penulis akan menguji menganalisa metadata pada keaslian video dengan menggunakan exiftool. Hasil dari penelitian ini diharapkan dapat menunjukan informasi perbandingan metadata yang baik.

***Kata Kunci** : Digital Forensik, Metadata, Video, Exiftool.*

1. PENDAHULUAN

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 gratis 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.

Video editing merupakan suatu proses memilih atau menyunting gambar dari hasil shooting dengan cara memotong gambar ke gambar atau dengan menggabungkan gambar-gambar dengan menyisipkan sebuah transisi dan sound. Saat ini sangat banyak software yang bisa digunakan untuk video editing contohnya pada *software Adobe After Effect* yang di dalamnya banyak menyediakan tool untuk mengubah keaslian video dengan mudah,

Pemalsuan merupakan suatu tindakan memodifikasi dokumen, produk, gambar atau video, di antara media lain. Video yang sangat mudah di edit dan di palsukan ini membuat banyak para oknum yang tidak bertanggung jawab merusak keaslian video dan menyebar video ke media social sehingga informasi atau pesan pada video bisa berubah keasliannya, dari latar belakang inilah peneliti mengambil penelitian ini yaitu analisis deteksi keaslian video.

Metadata merupakan informasi tambahan yang menyertai dan mendeskripsikan tentang sebuah data tertentu. Misalnya, sebuah video memiliki metadata yang menginformasikan seberapa besar ukuran file video, kedalaman warnanya, resolusinya, kapan dibuat, dan sebagainya. Contoh lain, metadata sebuah dokumen teks berisi informasi tentang seberapa panjang dokumen tersebut, siapa yang membuat, kapan ditulis, dan ringkasan isinya. Adapun metadata pada halaman website adalah bagian yang dituliskan pada tag meta di bagian header halaman web, misalnya deskripsi singkat tentang website dan keywordnya.

Dari latar belakang tersebut peneliti melakukan penelitian ini yaitu Analisis Forensik Deteksi Keaslian Metadata Video, Dalam penelitian ini yang menggunakan tools Exiftool diharapkan dapat memudahkan dalam memahami karakteristik metadata file secara umum pada keaslian video dan memudahkan pencarian file-file berdasarkan korelasi metadata file tersebut.

2. TINJAUAN PUSTAKA

Bebera penelitian yang berkaitan dengan metadata forensic yaitu penelitian yang dilakukan oleh Moh. Subli,Bambang Sugiantoro dan Yudi Prayudi (2017) Metadata Forensik untuk Mendukung Proses Investigasi Digital. Penelitian ini menjelaskan bahwa Bahwa semua jenis file yang ada di dalam komputer, bisa dilihat detail metadatanya oleh algoritma metadata forensik yang sudah dibangun, termasuk tujuh macam file yang sudah dijadikan sampel yaitu *DOCX, PDF, JPG, MP3, MP4, DD* dan *E01*, Metadata pada setiap file dapat

dipahami secara umum, yaitu dibagi dalam tiga bagian; metadata secara general, metadata secara detail dan metadata nilai dari checksumnya. Metadata General terdiri dari lokasi file, nama file, type file, owner dan computer, Metadata Detail terdiri dari *CreationTime, LastAccessTime, LastModified Time, is Directory, isOther,isRegularFile, isSymbolicLink* dan Size, dan Metadata Checksum terdiri dari nilai *MD5* dan *SHA-256*.

Penelitian yang sama juga dilakukan oleh Dewi Yunita Sari, Yudi Prayudi,Bambang Sugiantoro (2017) Deteksi Keaslian Video Pada Handycam Dengan Metode Localization Tampering. Menjelaskan Konsep dasar dalam mendeteksi video pada handycam dengan membuat simulasi video tampering dengan attack dimana video asli dilakukan cropping, zooming, rotation, dan *grayscale*. Dari hasil attack tersebut terbentuk sebuah video tampering. Video asli dan video tampering kemudian dianalisis dengan menggunakan metode localization tampering dengan menganalisis frame by frame, dan grafik histogram.

Selanjutnya Shraddha Suratkar dan Harmeet Khanuja (2014) Menjelaskan bahwa volume besar metadata tersedia dalam infrastruktur pada database yaitu untuk keperluan penyelidikan tetapi sebagian besar usaha terletak pada pengambilan dan analisis informasi dari sistem komputasi. Dengan demikian, dalam penelitian ini terutama relevansi metadata dalam desain dari alat forensik database yang umum independen dari DBMS yang difokuskan.

Penelitian selanjutnya Mark Phillips (2013) menjelaskan metodologi secara keseluruhan, memperkenalkan dua tools opensource sederhana yang dikembangkan untuk membantu memberikan contoh perintah dalam menunjukkan beberapa permintaan analisis metadata secara umum dan Kam Woods, Alexandra Chassanoff & Christopher A. Lee fokus pada metadata yang dihasilkan oleh tools open source yang mendukung Digital Forensik *XML (DFXML).* Bagian-bagian dari metadata ini dapat digunakan saat merekam peristiwa PREMIS untuk menggambarkan kegiatan yang relevan dengan pelestarian dan akses dari metadata tersebut.

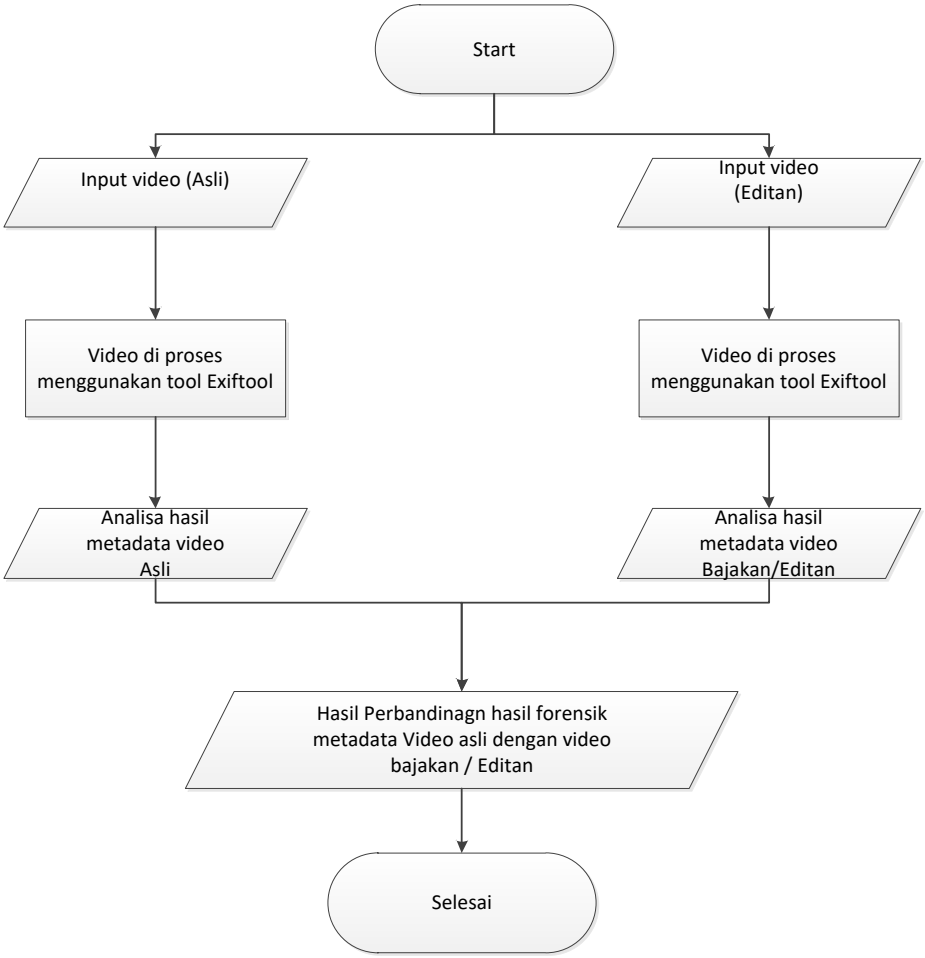
Pelnelitian lain juga dilakukan oleh A.Gupta, S. Gupta, dan A. Mehra, Video *Authentication* in Digital forensic (2015) . Penelitian ini ini menyajikan sebuah algoritma yang dibagi dalam dua bagian yaitu, menghitung frame yang diulang dengan memproses pixel pada gambar untuk menghasilkan waktu gerak frame demi frame dan menghitung serangan gangguan dan lokasinya dengan bantuan dari *Support Vector Machine*. Penelitian ini membantu memprediksi keaslian video apakah video yang diteliti telah dirusak atau tidak.

S V Raghavan (2016) Engine for Analyzing Metadata Based Associations in Digital Evidence. Penelitian ini mempresentasikan tentang desain forensik dan alat analisis yang mengekstraksi metadata dari file, catatan log dan paket jaringan dan mengidentifikasi asosiasi metadata ke grup . Alat ini menggunakan metadata untuk mengakses dan menganalisis beberapa artefak di satu atau lebih sumber bukti digital bersama. Proses pengelompokan juga tidak membutuhkan konstan pemantauan atau masukan pengguna tidak seperti alat saat ini. diilustrasikan fitur alat ini jika dibandingkan dengan forensik yang ada alat dan menunjukkan bagaimana metadata dapat digunakan untuk menguatkan informasi di seluruh sumber untuk menyelesaikan file klasik masalah kepemilikan. Ini menunjukkan penggunaan metadata asosiasi dapat mengaitkan kepemilikan dengan yang benar individu yang merupakan aspek penting dari forensik digital analisis. Kami juga membahas beberapa hasil awal kinerja di seluruh dataset yang berisi file gambar digital dan dokumen pengolah kata.

Ezz El-Din Hemdan & Manjaiah D.H (2015) dalam penelitiannya melakukan pendekatan analisis forensik untuk barang bukti digital seperti foto digital dan dokumen. Barang bukti ini berisi metadata penting yang dapat digunakan oleh penyidik untuk membantu menyelidiki kejahatan yang berkaitan dengan cloud. Metadata dapat digunakan juga oleh penyerang untuk melakukan kegiatan ilegal sehingga ada kebutuhan serius untuk melindungi metadata karena memberikan peneliti dengan informasi yang dapat dipercaya untuk melakukan penyelidikan forensik. Dalam pendekatan ini, metadata yang dihasilkan dari barang bukti dan juga algoritma *hash* diterapkan untuk menghasilkan nilai hash untuk menjamin integritas data yang diunggah ke layanan *cloud* seperti *ADrive, Box, Microsoft onedrive, Google Drive, Copy dan Dropbox.*

3. METODE PENELITIAN

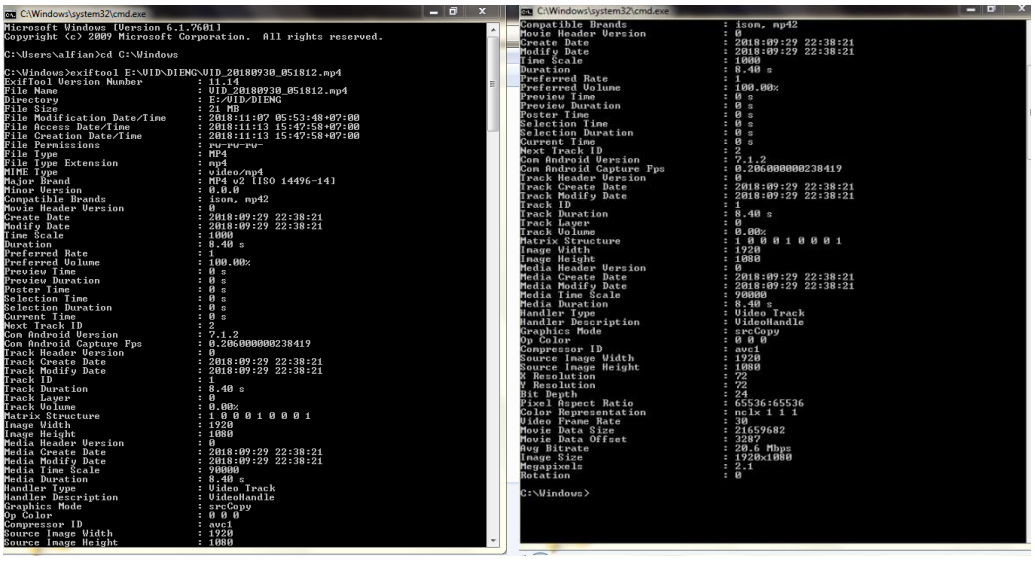
Prosedur penelitian ini menggunakan beberapa metode menjelaskan secara terperinci mengenai langkah yang digunakan untuk melakukan sebuah penelitian ini dan menjelaskan alur system yang digunakan, yaitu Exiftool.



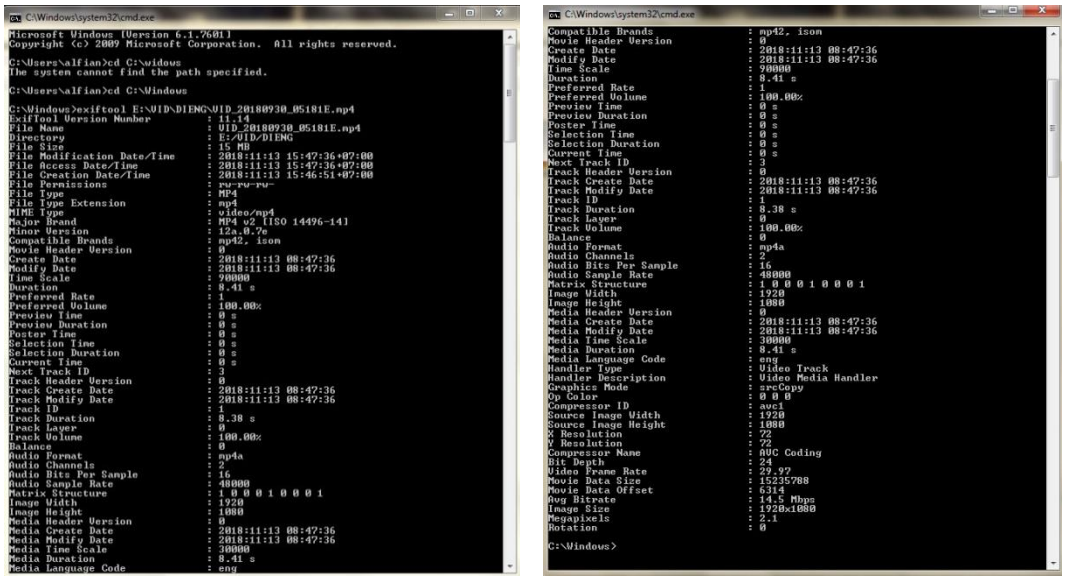
Gambar 1. Hasil metadata video asli dan video editan

4. HASIL DAN PEMBAHASAN

Vidio yang sudah dipilih yaitu video asli dan video sample / editan yang akan dianalsa hasil metadatanya menggunakan aplikasi exiftool, Berikut ini merupakan hasil metadata dari video asli dan video editan.



Gambar 2. Hasil metadata video asli



Gambar 3. Hasil metadata video Editan/Palsu

Setelah melakukan percobaah dengan menggunakan exiftool pada cmd, mendapatkan suatu informasi metadata seperti gambar diatas, dan setelah melakukan tahap ini selanutnya adalah melakkan analisa terhadap hasil metadata yang diperoleh dari video asli dengan video editan.

4. KESIMPULAN

Setelah melakukan beberapa hal, terkait dengan perancangan deteksi dan analisis deteksi keaslian metadata pada video. konsep dasar dalam melakukan analisis deteksi video ini adalah dengan membuat sample video editing, dimana sample video editing digunakan untuk membandingkan metadata rekaman video asli dan kemudian selanjutnya tahap Processing Exiftool, dimana tahap ini adalah proses membaca metadata video dengan exiftool dan tahap akhir adalah analisa hasil metadata.

DAFTAR PUSTAKA

Moh. Subli, Bambang Sugiantoro & Yudi Prayudi. 2017. Metadata Forensik untuk Mendukung Proses Investigasi Digital. Jurnal Nasional Teknik Informatika UIN Sunan Kalijaga Yogyakarta.

Dewi Yunita Sari, Yudi Prayudi & Bambang Sugiantoro. 2017. Deteksi Keaslian Video Pada Handycam Dengan Metode Localization Tampering. Jurnal Nasional Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia.

A. Gupta, S. Gupta, dan A. Mehra. 2015. Video authentication in digital forensic. 1st Int. Conf. Futur. Trends Comput. Anal. Knowl. Manag. ABLAZE 2015, no. Ablaze, hal. 659–663, 2015.

Mark Phillips. (2013). Metadata Analysis at the CommandLine. International Journal. Code{4}lib Journal. Issue 19, 2013- 01-15.

Alanazi, Jones. (2015). The Value of Metadata in Digital Forensics. European Intelligence and Security Informatics Conference.

Florian Buchholz & Eugene Spafford (2014). On the role of file system metadata in digital forensics, Digital Investigation1, 298e309.

Harmeet Kaur Khanuja, D.S & Adane. 2012. A framework for database forensic analysis, Computer Science & Engineering: an International Journal (CSEIJ), vol.2, no.3.

Salama et al. 2012. Metadata Based Forensic Analysis of Digital Information in the Web. ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE & SECURE KNOWLEDGE MANAGEMENT, JUNE 5-6, 2012, ALBANY, NY.

Ryan Harris, Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem, Science Direct Digital investigation 3 s 2006 s 44 – s49.

Carrier, B. D., 2003. Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers. International Journal of Digital Evidence (IJDE), Vol. 1(4), pp. 1-12.

O.M. Fasan and M.S. Olivier.2012. On dimensions of reconstruction in database forensics, Seventh International workshop on Digital Forensics & Incident Analysis (WDFIA)2012.