Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi Vol. 2 No. 2 (2023)

E-ISSN: 2807-5935 DOI:10.20885/snati.v2i2.21

ANALISIS FORENSIK PENGGUNAAN FUNGSI HASH DALAM MENENTUKAN KEASLIAN VIDEO, METADATA IMAGE DAN MAGIC NUMBER FILE

Muhammad Adil Kustian
Magister Informatika
Universitas Islam Indonesia
Yogyakarta, Indonesia
21917034@students.uii.ac.id

***Abstrak*—Dalam ilmu digital forensik penggunaan nilai hash, metadata, serta magic number sangat diperlukan dalam menentukan keaslian dari sebuah file. Terdapat 3 tools untuk menganalisis dan menentukan keaslian sebuah file baik berupa video, gambar dan magic number. Ketiga tools tersebut adalah 1) Forevid yang digunakan untuk menentukan keaslian file dan metadata dari video, 2) ExifTool untuk menentukan metadata dari gambar, 3) WinHex untuk menentukan magic number atau ekstensi file asli dari sebuah file. Penggunaan tools ini memperlihatkan metadata asli dari sebuah file, nilai hash dari sebuah video untuk dicocokkan dengan video lainnya, serta magic number yang berbeda-beda untuk menentukan file signature. Eksperimen dilakukan menggunakan 2 buah file; satu dari 2 file tersebut diubah dan kemudian dicocokkan dengan nilai hash, metadata dan magic number-nya sehingga hasil yang akan didapatkan berupa perbandingan hash, metadata dan magic number file asli dengan file palsu yang sudah diedit. Dari hasil yang didapat, ketiga tools yang digunakan dalam penelitian ini dapat mengidentifikasi file-file yang diperlukan dalam proses forensik.**

Kata Kunci*—*forensik, hash, gambar, magic number, metadata, video

I. INTRODUCTION (*HEADING 1*)

Salah satu efek perkembangan teknologi adalah adanya penyebaran informasi palsu atau hoax yang kerap terjadi pada media sosial yang meresahkan masyarakat [1]. Bahkan termasuk video, gambar dan ekstensi file asli dari sebuah file yang diubah, guna menghilangkan barang bukti digital. Padahal dalam ilmu digital forensik jika seseorang menghilangkan barang bukti digital maka dapat terancam tindak pidana [2]. Data dari Kominfo (Kementerian Komunikasi dan Informatika Republik Indonesia) menunjukkan penyebaran berita bohong yang berkaitan dengan file video dan gambar sudah sangat sering terjadi dengan modus pelaku mengedit video atau gambar sebelum dipublikasikan di media sosial [3]. Contohnya pada kasus pengeditan video pasangan calon pada Pilkada Bontang tahun 2020. Sehingga diperlukan analisis pada fungsi hash dan metadata pada sebuah file untuk menentukan keasliannya.

Hash adalah suatu kode alfanumerik untuk menghasilkan sebuah digital kecil dari sembarang data [4] dan Metadata adalah informasi terstruktur yang menggambarkan, menjelaskan, menempatkan, atau membuat lebih mudah untuk mengambil, menggunakan, atau mengelola sebuah sumber informasi [5]. Sedangkan magic number adalah byte di dalam file yang digunakan untuk mengidentifikasi format dari sebuah file, biasanya dapat diidentifikasi pada bagian awal dari sebuah file [6].

Menurut Khairunnisak Ashari dkk (2020), dijelaskan tentang analisis forensik untuk mendeteksi citra digital menggunakan metode NIST (National Institute of Standards and Technology) [7]. Pada penelitian tersebut menjelaskan cara melakukan pendeteksian metadata dan nilai hash untuk mendeteksi citra digital dengan menggunakan 1 tools yaitu ExifTool. Sementara penelitian ini akan menggunakan 3 tools berbeda. Fahmi Anwar dkk (2020) menjelaskan tentang Analisis Validasi Image PNG File Upload menggunakan Metadata pada Aplikasi Berbasis Web. Pada penelitian tersebut membandingkan penggunaan metadata dan magic number dalam menyaring berkas image PNG [8].

Artikel ini menjelaskan dan menyajikan bagaimana cara kerja dari 3 tools analisis forensik untuk menentukan keaslian sebuah file. Susunan artikel ini adalah sebagai berikut: Teori pendukung akan disajikan pada Bab 2, sedangkan detil langkah analisis disajikan pada Bab 3. Hasil dan pembahasan akan ditunjukkan pada Bab 4, sebelum akhirnya ditutup dengan Bab 5 yang berisi kesimpulan dan saran.

II. TEORI PENDUKUNG DAN KAJIAN PUSTAKA

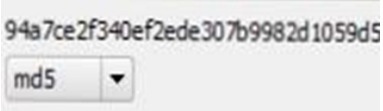
A. Nilai Hash

Secara garis besar istilah hash bertendensi pada pemrosesan matematis atau suatu fungsi yang berupa data dalam berbagai ukuran dan dimasukkan dalam operasi. Format data-data tersebut sangat penting dan memiliki sifat tetap. Apalagi yang berhubungan dengan proses transaksi yang cukup besar. Hash merupakan salah satu ilmu yang digunakan dalam mengubah informasi. Jadi data yang diinput nantinya akan berubah menjadi kombinasi antara angka, huruf atau ada karakter lain yang juga terenskripsi

dengan ukuran yang sama. Apabila data sudah terenskripsi, maka data tersebut tidak dapat dikembalikan. Algoritma fungsi hash juga dikenal dengan sebutan one way function atau encryption satu arah [9]. Ada beberapa fungsi hash yang dikenal di dunia kriptografi dan fungsi hash yang paling sering digunakan antara lain:

1. MD5 (Message-Digest Algorithm 5)
2. SHA-1 (Secure Hashing Algorithm 1)
3. RIPEMD-160 (Race Integrity Primitive Evaluation Mesaage Digest 160)
4. SHA-2 (Secure Hashing Algorithm 2)
5. SHA-3 (Secure Hashing Algorithm 3)

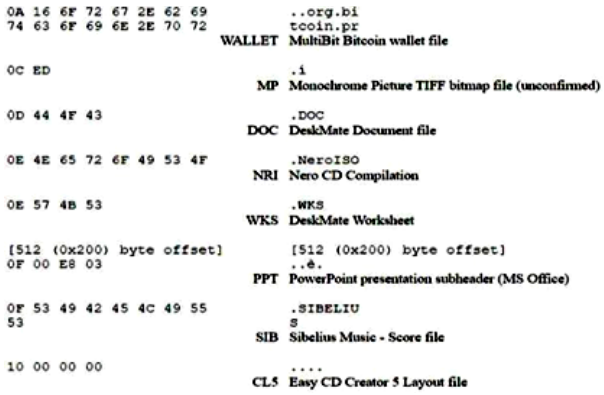
Artikel ini fokus pada Algoritma fungsi hash MD5 (Message Digest Algorithm 5). Contoh fungsi hash MD5 dapat dilihat pada Gambar 1, pada gambar tersebut terlihat kombinasi dari nilai hash berupa angka dan huruf. MD5 sendiri digunakan dengan nilai hash-nya yang berjumlah 128 bit dan sangat umum digunakan.



Gambar 1. Contoh Nilai Hash MD5

B. *Metadata*

Metadata merupakan penjelasan terkait dengan informasi terperinci dari sesuatu file. Dalam penerapannya metadata mempunyai banyak fungsi yaitu untuk melakukan identifikasi dengan membedakan satu file atau konten dengan konten lainnya, banyak elemen dalam melakukan identifikasi metadata antara lain nama, file, judul, author, tanggal pembuatan file dll. Dari metadata inilah yang selanjutnya dijadikan perameter sebagai perbandingan, selanjutnya fungsi dari metadata adalah pencarian konten yang tepat, jadi dengan menggunakan metadata konten yang akan kita cari dapat kita sesuaikan dengan penjelasan dokumen. Serta metadata juga berfungsi untuk melacak dan memantau penggunaan konten. Dengan metadata ini maka akan mempermudah kerja kita dalam melihat dan menganalisis terkait dengan deskripsi atau penjelasan dari sebuah file atau konten [10].



Gambar 2. Magic Number File

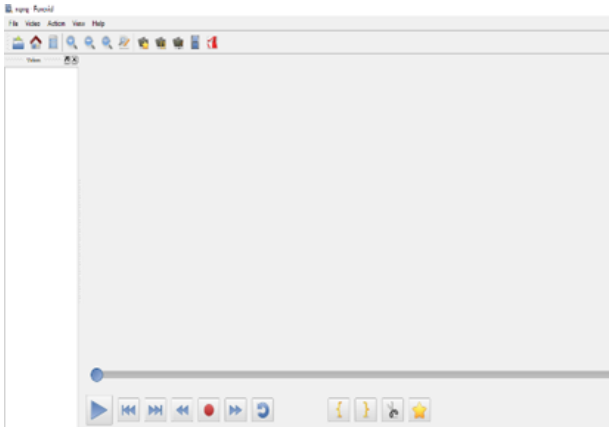
C. *Magic Number*

Magic Number dapat diartikan kumpulan byte yang terdapat dalam file dan digunakan untuk mengidentifikasi dari sebuah file tersebut. magic number ini terdapat di awal dari sebuah file . misalnya ekstensi file mp3 dengan magic number-nya 49 44 33. Setiap ekstensi file memiliki magic number yang berbeda-beda dan biasanya magic number itu terdiri dari 2-8 digit angka. Untuk melihat magic number dari sebuah file secara lengkap dapat dilihat pada website-nya File Signature (garykessler.net). magic number juga berfungsi untuk menentukan keaslian dari sebuah file. Penggunaan magic number sangat penting Ketika akan melakukan identifikasi terkait dengan sebuah file atau dokumen. Contohnya: Ketika kita menerima suatu file pdf dan tidak bisa dibuka, rusak atau corrupt maka disanalah peran penting dari magic number untuk memastikan file tersebut benar-benar rusak atau sengaja diubah ekstensinya.

Tampilan dari beberapa ekstensi file dapat dilihat pada Gambar 2 di mana di sebelah kanan adalah nama ekstensi dari suatu file dan disebelah kiri merupakan magic number dari file tersebut. Dapat dilihat dari Gambar 2 tersebut bahwa magic number dari setiap file berbeda dan memiliki 2 sampai 8 digit.

D. *Forevid*

Forevid merupakan salah satu tools yang digunakan untuk mendeteksi nilai hash dan metadata dari sebuah video, ada banyak tools lain yang bisa digunakan dalam melakukan identifikasi keaslian video. Akan tetapi tools forevid dapat membandingkan sekaligus melihat nilai hash dan metadata dari video secara detail dan juga penggunaan dari tools forevid ini cukup simple dan mudah di mengerti. alur kerja dari tools ini adalah jadi sebuah video yang dianalisis nantinya akan di compare dengan video lain, apabila video tersebut asli maka nilai hash akan valid (berwarna hijau) tapi jika video tersebut sudah diedit atau dimanipulasi maka nilai hash-nya akan invalid (berwarna merah)[11]. Tools atau perangkat lunak forevid ini dibuat dengan menggunakan Bahasa pemrograman python. Adapun tampilan halaman dari tools forevid dapat dilihat pada Gambar 3.



Gambar 3. Tampilan Tools Forevid

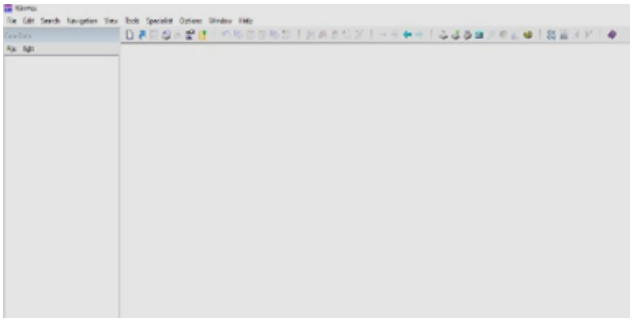
E. *Exiftool*

Exiftool merupakan salah satu tools yang digunakan dalam melihat, membaca, menulis, menentukan, dan memanipulasi metadata dari suatu file seperti gambar, audio, video dll. atau dapat melihat informasi yang tersembunyi dari suatu file [12]. Dengan tools ini kita dapat melihat secara detail keterangan dari sebuah file misalkan nama file, file type, directory, orientation dll. Pada umumnya kebanyakan pengguna tools ini lebih sering melakukan identifikasi ke gambar dengan melihat informasi terperinci meta data

gambar. Penggunaan dari tools ini sangat mudah dengan drag file yang kita pilih ke tools exiftool dan setelah itu akan muncul informasi lengkap terkait file yang dipilih.

F. Winhex

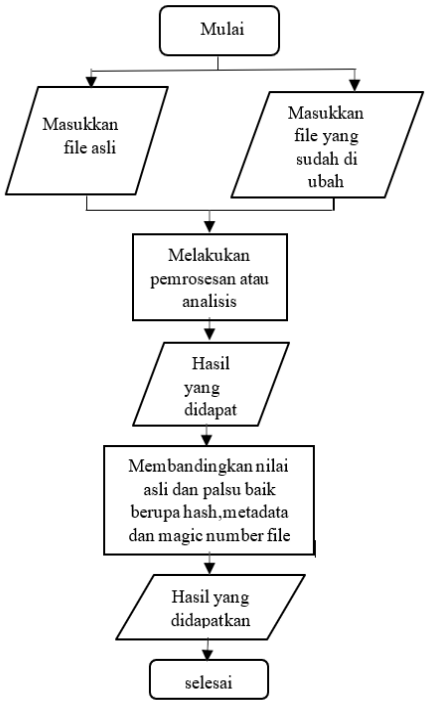
Winhex merupakan software editor hexadesimal universal, dan penggunaan winhex sendiri sangat berguna dalam bidang ilmu digital forensik. Selain berguna untuk memeriksa ekstensi file atau file signature dari sebuah file [13]. Tools winhex juga berfungsi untuk me recovery data yang sudah dihapus atau data yang hilang dari dari hard drive sistem file yang corrupt. Adapun kelebihan dari winhex antara lain adalah sebagai penerjemah data, menganalisis dan membandingkan file, sebagai pencarian paling fleksibel yang akan menggantikan fungsi-fungsi dan dapat menghapus file rahasia. Tampilan halaman dari tools winhex dapat dilihat pada Gambar 4.



Gambar 4. Tampilan Tools Winhex

III. METODOLOGI

Metodologi yang digunakan menggunakan skema tersendiri, untuk melakukan proses deteksi keaslian video dengan nilai hash, metadata foto dan magic number dalam mengidentifikasi file signature. Untuk lebih jelas dan lengkapnya skema metodologi yang digunakan dapat dilihat pada Gambar 5.



Gambar 5. Alur flowchart deteksi keaslian

Jadi berdasarkan Gambar 5 tersebut ada 3 parameter yang digunakan yaitu pelakuan perbandingan nilai hash antara 2 video yaitu video asli dan video palsu yang sudah diedit, memeriksa metadata dari suatu gambar, dan magic number dari sebuah file. Sementara ada 3 tools yang digunakan dalam proses analisis ini yaitu forevid yang berfungsi untuk compare nilai hash dari video, exiftool yang digunakan untuk metadata dari image dan winhex digunakan untuk mengidentifikasi magic number dari sebuah file. Dari metodologi atau kerangka kerja tersebut nantinya kita akan mendapatkan hasil yang valid yang berkaitan dengan judul jurnal tersebut.

IV. HASIL DAN PEMBAHASAN

A. Hasil Identifikasi menggunakan tools forevid

Dalam melakukan proses pendeteksian akan Diawali dengan menyiapkan 2 video dengan 1 video asli dan 1 video hasil editing. Kemudian video akan diproses menggunakan tools forevid.

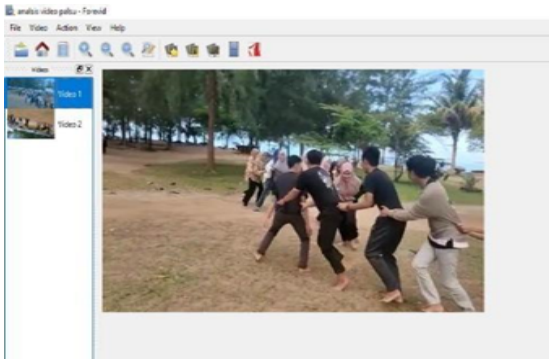
1) Penggunaan Tools Forevid Nilai Hash.

   Perangkat lunak software yaitu tools forevid memiliki beberapa fungsi diantaranya adalah berkaitan dengan penggunaan fungsi hash dalam melakukan analisis terkait dengan video selain itu forevid juga dapat digunakan untuk memeriksa dan melihat metadata atau keterangan asli dari suatu video. ada beberapa metode algoritma yang dapat digunakan di dalam tools forevid diantaranya adalah MD5, SH1, SH224, SH256 dan SH512. Dalam penelitian atau penggunaan kali ini penulis akan berfokus menggunakan algoritma hash MD5(Message Digest Algoritm 5). Penggunaan dari tools forevid sangat mudah yaitu hanya dengan memilih pilihan open yang ada dalam menu bar dan selanjutnya memilih video yang akan dilakukan identifikasi.

2) Analisis Fungsi Hash Tools Forevid.

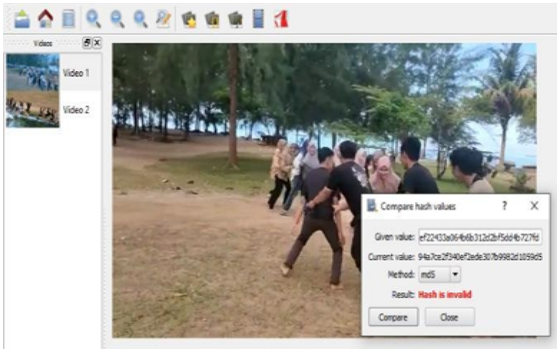
   Salah satu Fungsi hash adalah sebagai bahan enskripsi yang terdiri dari kombinasi antara angka dan huruf. Dalam analisis kali ini nantinya akan dilakukan 2 kali percobaan yang menghasilkan output berupa note “valid” dengan warna hijau dan “invalid” dengan warna merah. Dengan penjelasan valid berarti nilai hash dari video sama dalam artian lain video tersebut asli tanpa rekayasa. Invalid yang berarti bahwa video tersebut memiliki nilai hash yang berbeda dan tidak sama dengan video aslinya atau sudah direkayasa atau diedit.

   a. Analisis Hash Video Asli dan Palsu (Editing); Di dalam Gambar 6 dapat dilihat bahwa ada video di sebelah kanan tools yang akan dilakukan analisis. Di mana salah satu dari video tersebut adalah hasil dari editing Dan satu dari video tersebut adalah video asli maka akan dilakukan analisis untuk memeriksa nilai hash.



Gambar 6. Tampilan video

Tools forevid digunakan dalam memeriksa fungsi hash. Oleh karena itu hasil perhitungan dari nilai hash dapat juga dilakukan dengan string teks. Fungsi nilai hash salah satunya adalah dapat menerima masukan nilai string yang memiliki Panjang sembarang karena fungsi tersebut akan dikonversikan menjadi string yang output-nya memiliki nilai tetap. Hasil dari fungsi hash disebut juga dengan checksum.



Gambar 7. Hasil nilai hash invalid

Gambar 7 menunjukkan bahwa salah satu video yang dimasukkan adalah video editing dan tidak sama dengan video aslinya, itu dibuktikan berdasarkan fungsi hash yang sudah diuji. Algoritma yang digunakan pada analisis tersebut adalah algotitma MD5 (Message Digest Algoritm 5). Pada Gambar 7 tersebut memperlihatkan hasil dari fungsi hash video pertama dan kedua hasilnya berbeda, di mana fungsi hash dari video menghasilkan "hash is invalid" dan berwarna merah yang artinya video asli yang pertama tidak sama dengan video yang kedua atau video palsu dan editan.

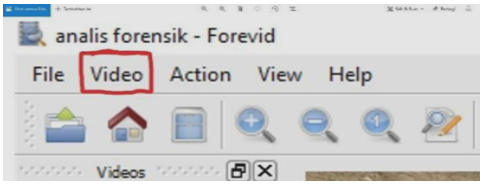
b. Hasil Analisis Hash Video Asli; Untuk mempertajam, menambah dan lebih memahami terkait penggunaan tools forevid dan fungsi hash, dilakukan percobaan terkait dengan fungsi hash yang sama dengan memasukkan 2 video yang sama tanpa editan dan akan membandingkan fungsi hash dari kedua video, serta hasil yang didapatkan dari perbandingan dua video tersebut. Pada analisis kedua ini akan digunakan metode algoritma yang sama dengan percobaan pertama yaitu menggunakan algoritma MD5 (Message Digest Algoritm 5). Dapat dilihat pada Gambar 8 terdapat dua buah video dalam tools forevid. Yang dijadikan input adalah video asli tanpa editan.

Gambar 8.. Tampilan Nilai hash valid

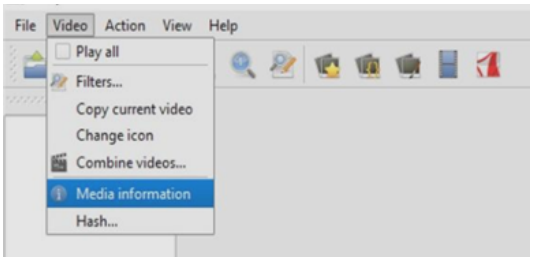
Dari hasil analisis fungsi hash yang dilakukan yang terlihat pada Gambar 8. Dengan membandingkan nilai hash antara dua video yang menjadi input menghasilkan nilai "valid" dan berwarna hijau yang artinya dua buah video yang dijadikan input tersebut adalah video asli tanpa mengalami perubahan, rekayasa atau editan sebelumnya dan juga nilai hash-nya juga sama, yang terlihat dari Given Value dan Current Value yang masing-masing memiliki kesamaan. Analisis fungsi hash ini menggunakan algoritma hash MD 5 (Message Digest Algoritm 5). Hasil dari analisis ini berbanding terbalik dengan hasil yang diperoleh pada Gambar 7 yang memiliki nilai invalid karena nilai hash video yang berbeda.

3) Penggunaan Tools Forevid Metadata.

Tools forevid selain bisa digunakan untuk memeriksa dan mencocokkan nilai hash tapi juga bisa digunakan untuk melakukan analisis terkait dengan metadata dari sebuah video. Metadata adalah keterangan lengkap terkait dengan video, metadata dapat diartikan sebagai suatu informasi yang menyimpan suatu data dalam Warehouse dan tentang keasliannya. dari penggunaannya ada beberapa jenis metadata diantaranya adalah deskriptif yaitu metadata yang bisa menjelaskan dari berbagai sumber informasi yang penting, Structural yaitu memiliki aktor penting dalam menggabungkan objek digital dan menjadi kesatuan juga akan terkoneksi satu dan lainnya, administratif yaitu metadata yang akan menampilkan informasi penting untuk melakukan setting terhadap suatu sumber informasi yang terpenting di metadata ini adalah mampu merubah siapa saja yang diizinkan untuk mengakses file. dengan metadata ini kita juga bisa mencocokkan mana video asli dan video rekayasa. Dengan penggunaan tools forevid dalam pemeriksaan terhadap metadata sangat mudah yaitu di bagian menu bar pada tools ini terdapat menu video dan di dalam menu video tersebut terdapat media information yang berguna untuk melihat metadata dari sebuah video. Untuk lebih jelasnya alur pemeriksaan metadata dapat dilihat pada Gambar 9 dan 10. Dari gambar tersebut dapat dilihat alur penggunaan tools forevid apabila ingin melakukan analisa terhadap metadata dari sebuah video.



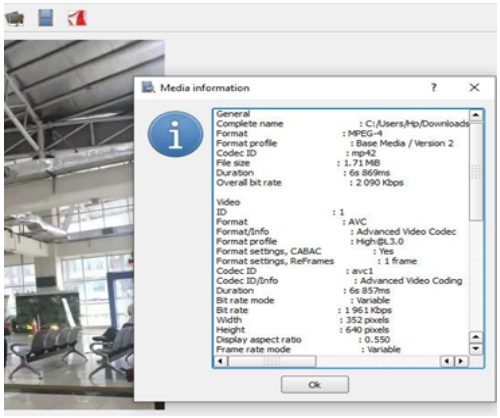
Gambar 9. Menu bar video



Gambar 10. Media information

4) Hasil Analisis Metadata Forevid.

Dalam analisis ini penulis akan menggunakan percobaan dengan memasukkan sebuah video di tools forevid. video tersebut akan dilakukan analisis untuk mendapatkan dan memperlihatkan metadatanya, metadata yang tampil adalah keterangan asli dari video yang diinputkan tersebut. Video yang akan diinputkan adalah video dengan nilai hash yang valid yang terdapat pada gambar 8. dan nantinya output dari proses tersebut adalah akan menampilkan isi lengkap dan detail terkait video tersebut seperti complete name, format, format profile, file size, duration, overall bit rate dll. Untuk lebih jelasnya terkait hasil analisis ini dapat dilihat pada Gambar 11.



Gambar 11. Metadata Video

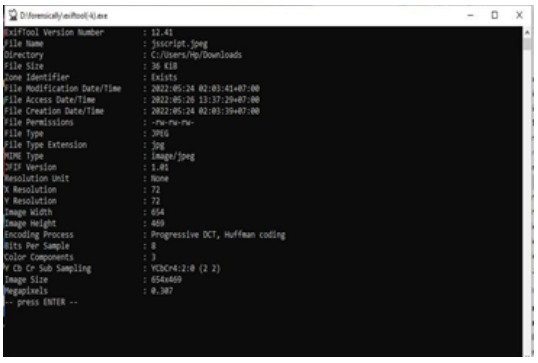
Dari hasil analisis pada tampilan Gambar 11 dapat dilihat bahwa ada banyak keterangan terkait dengan metadata yang ditampilkan. Pada tampilan metadata tersebut tidak hanya menampilkan keterangan terkait video tapi juga menampilkan keterangan mengenai audio serta tempat penyimpanan dari video. Dari hasil identifikasi inilah yang akan menjadi perbandingan dan menjawab pertanyaan terkait dengan siapa, apa, kapan dan di mana. Serta menjadi keterangan terhadap keaslian dari data tersebut.

B. Hasil Identifikasi menggunakan tools Exiftool

Dalam melakukan proses deteksi maka diawali dengan menyiapkan satu buah gambar, deteksi dilakukan dengan menggunakan exiftool pada cmd (Command Pront), di mana gambar akan dicocokkan metadata dengan menggunakan tools exiftool. Tools exiftool sendiri tidak hanya bisa mendeteksi metadata dari image tapi juga bisa untuk memeriksa metadata dari video dan audio. Serta tools exiftool juga berguna dalam memeriksa ekstensi file dari gambar, video maupun audio yang ekstensi file tersebut telah mengalami perubahan. exiftool yang digunakan dalam melakukan pemeriksaan metadata kali ini adalah exiftool dengan Version Number 12.41.

1) Hasil Analisis metadata gambar.

Tahap ini dilakukan adalah untuk melihat metadata dari sebuah gambar. Yang bertujuan untuk mendapatkan data yang mendukung. Metadata yang akan dilakukan analisis adalah metadata gambar sebuah gambar akan di drag ke tools exiftool dan akan akan menampilkan metadata dari gambar tersebut, metadata yang ditampilkan oleh tools exiftool sendiri lebih lengkap. gambar yang akan dilakukan analisis adalah gambar yang diberi nama "jsscript" dan memiliki ekstensi "jpeg". Untuk hasil dari percobaan terkait dengan metadata gambar exiftool dapat dilihat pada Gambar 4.7. Pada Gambar 4.7 dapat dilihat bahwa sebuah file dengan nama file jssript sudah di drag dan berada dalam tools exiftool.



Gambar 12. Hasil Metadata Gambar

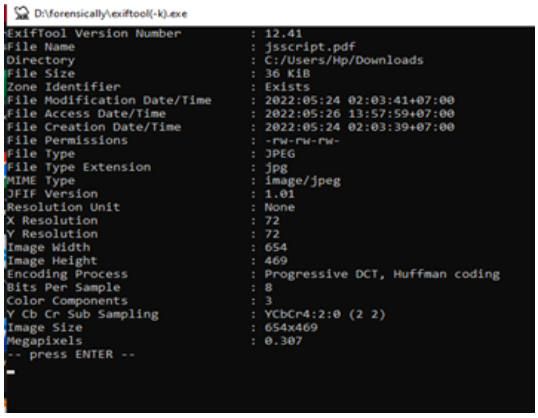
Dari hasil metadata pada Gambar 12 dapat dilihat dengan jelas metadata atau keterangan asli dari file tersebut. Untuk melakukan perbandingan metadata maka penulis akan mengubah ekstensi dari file gambar asli tersebut dari sebelumnya berekstensi "jpeg" akan di modifikasi ke ekstensi "pdf" dan akan dibandingkan metadata dari kedua file gambar tersebut.

2) Hasil perbandingan Analisis metadata asli.

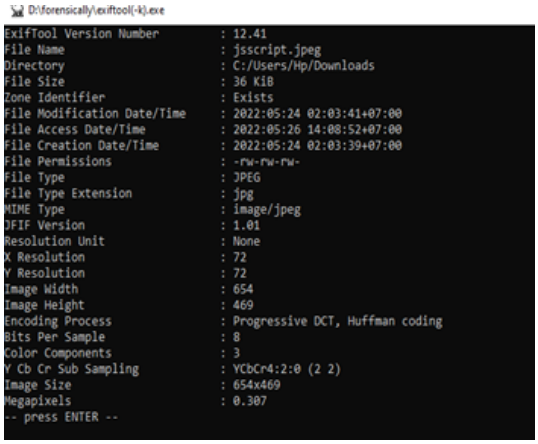
Dalam proses perbandingan metadata ini masih menggunakan file gambar yang sama dengan percobaan sebelumnya di mana ekstensi dari file gambar tersebut diubah ke pdf dan hasil dari perbandingan tersebut dapat dilihat pada Gambar 13 dan Gambar 14.

Dari hasil analisis dua file gambar yang mana salah satu file sudah diubah ekstensinya maka diperoleh hasil yang sesuai dengan gambar, bahwa pada gambar 12 adalah gambar bertipe pdf yang hasil metadata setelah dibandingkan sama dengan metadata pada gambar 14

tetapi yang membedakan adalah terdapat pada file name-nya di mana file name pada gambar 13 yang bertipe pdf tersebut setelah di identifikasi ternyata tidak sesuai dengan isi metadata yang terdapat dalam file yang mana isi file type dalam file adalah berformat jpeg sementara pada gambar 14 yang bertipe jpeg tersebut sama dengan file type dalam metadata. Artinya adalah file yang bertipe pdf pada gambar 13 adalah file palsu yang sudah diubah atau dimodifikasi terlebih dahulu dan file pada gambar 14 adalah file asli yang dapat dibuktikan dari metadata nya.



Gambar 13. Hasil Metadata File Gambar Pdf



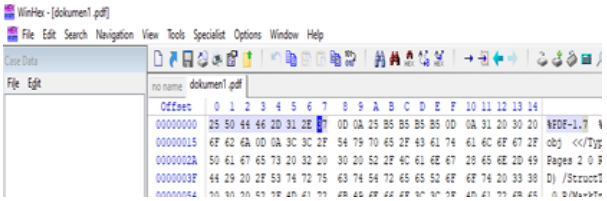
Gambar 14. Hasil Metadata File Gambar Jpg

C. *Hasil Identifikasi menggunakan tools Winhex*

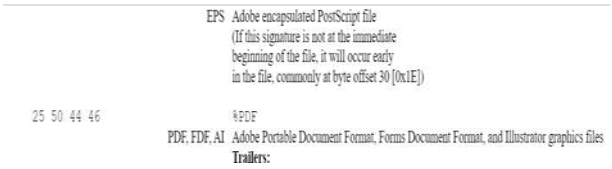
Dalam melakukan proses deteksi dan analisis, diawali dengan menyiapkan 2 buah file salah satu file tersebut akan diubah ekstensi file-nya. Pada tahap ini bertujuan untuk melihat magic number dari sebuah file yang ekstensi file-nya sudah dimodifikasi. Dan hasilnya akan akan dicocokkan dengan magic number dari file tersebut. Ada 2 file yang sudah dilakukan analisis file pertama Bernama dokumen1.pdf (file pdf) dan file kedua adalah dokumen1 (file yang sama tapi ekstensinya dimodifikasi ke doc).

1) Hasil analisis magic number

Hasil yang didapatkan akan dibandingkan dengan dengan magic number atau file asli yang terdapat pada website-nya Garykessler. Hasil dari percobaan dari dokumen1 dapat dilihat pada tampilan Gambar 15 dan Gambar 16 menunjukkan file signature atau magic number asli.



Gambar 15. Hasil Magic Number Format Pdf

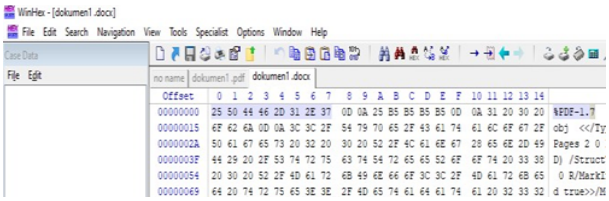


Gambar 16. Magic Number Asli Pada Website Garykessler

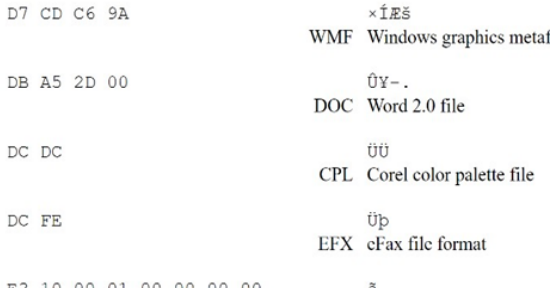
Jadi hasil yang didapatkan adalah gambar 15 akan muncul magic number atau file signature dari ekstensi pdf dan akan dicocokkan dengan gambar 16 yaitu magic number asli. Terlihat pada gambar 16 tersebut magic number dari file pdf adalah berjumlah 4 digit angka yaitu 25 50 44 46 sementara hasil dari magic number atau nilai asli pada tools winhex pada gambar 15 adalah 25 50 44 46 2D 31 2E 37 yang artinya adalah 4 digit awal yang terdapat pada gambar 15 itu sama persis dengan magic number pada gambar 16. bahkan pada bagian sebelah kiri gambar 15 sudah terlampirkan format yang bertuliskan pdf. oleh karena itu file pdf yang dilakukan analisis di tools winhex adalah file pdf asli tanpa mengalami perubahan atau modifikasi.

2) Hasil analisis magic number yang dimodifikasi ke doc

Untuk memperjelas penggunaan dari tools winhex maka penulis melakukan percobaan terkait dengan file yang sama dengan gambar 15 yang Bernama dokumen1.pdf dimodifikasi ekstensinya ke doc sehingga menjadi dokumen1.doc dan akan dibandingkan dengan website Garykessler seperti yang terdapat pada gambar 16. setelah dilakukan analisis maka hasil yang didapatkan dapat dilihat pada Gambar 17.



Gambar 17. Hasil Magic Number File Doc



Gambar 18. Hasil Magic Number Asli Doc

Jadi hasil yang didapatkan dapat dilihat pada gambar 17 terlihat magic number atau file yang muncul yaitu 25 50 44 46 2D 31 2E 37 yang berjumlah 8 digit. Sedangkan pada magic number atau file signature dengan ekstensi doc dapat dilihat pada gambar 4.13 dengan DB A5 2D 00 yang jumlah nya 4 digit. Maka magic number doc yang terdapat pada gambar 17 mengalami perbedaan dengan magic number file aslinya yang terlihat pada gambar 18. jadi berdasarkan analisis tersebut dapat dipastikan bahwa file yang terdapat pada gambar 17 adalah file palsu yang sudah diedit atau dimodifikasi ekstensinya. Apabila dicocokkan magic number doc pada gambar 17 adalah magic number, file asli atau ekstensi file-nya pdf yang sudah mengalami perubahan. Pada tools winhex di bagian sebelah kiri juga terdapat keterangan bahwa file tersebut adalah file pdf.

V. KESIMPULAN

Setelah dilakukan analisis maka dapat disimpulkan bahwa setiap tools yang digunakan dalam mengidentifikasi nilai hash, metadata video dan magic number mempunyai kelebihan dan kekurangan masing-masing. Tools forevid digunakan dalam mengidentifikasi fungsi hash dan metadata video, tools exiftool digunakan dalam memeriksa metadata file baik berupa video, gambar, audio selain itu tools ini juga bisa memeriksa ekstensi file dan begitu juga dengan tools winhex yang penggunaannya berfungsi dalam memeriksa magic number atau file signature dari sebuah file.

Penggunaan dari ketiga tools tersebut sangat penting dalam ilmu digital forensik, apalagi dengan adannya beberapa kasus seperti penyebaran video ,gambar yang sudah diedit dan kemudian di publikasikan serta ekstensi file yang diubah guna menghilangkan jejak. Jadi ketiga tools tersebut mempunyai korelasi karena berkaitan dengan pembuktian terkait barang bukti digital.

DAFTAR PUSTAKA

[1] R. Pakpahan, "Analisis Fenomena Hoax Diberbagai Media Sosial Dan Cara Menanggulangi Hoax," Konferensi Nasional Ilmu Sosial dan Teknologi, Vol. 1, No. 1, 2017.

[2] G. A. Anes, V. Y. Gosal, & D. Rumimpunu, "Tindak Pidana Tersangka Akses Ilegal Akun Instagram Yang Disita Penyidik Sebagai Alat Bukti Berdasarkan Kitab Undang-Undang Hukum Pidana," Lex Privatum, Vol. IX, No. 13, 2021

[3] Kominfo, "Cara Demokratis Menangkal Hoax", 2017. https://kominfo.go.id/content/detail/8812/cara-demokratis-menangkal-hoax/0/sorotan_media (accessed May 27, 2022).

[4] K. Aryasa & Y. T. Paulus, "Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Dalam Library Pada Pemrograman Java," Creative Information Technology Journal, Vol. 1, No. 1, 2013.

[5] B. Sugiantoro & Y. Prayudi, "Metadata Forensik Untuk Analisis Korelasi Bukti Digital," Student Thesis, UII, 2018. [Online]. Available: https://dspace.uii.ac.id/handle/123456789/9452.

[6] S. Morianus, "Komputer Forensik - E-Documents Fasilkom Unsri," 2017. http://edocs.ilkom.unsri.ac.id/1135/

[7] K. Khairunnisak, H. Ashari, & P. A. Kuncoro, "Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode Nist" J. Resist. (Rekayasa Sist. Komputer), Vol. 3, No. 2, pp. 72–81, 2020

[8] F. Anwar, A. Fadlil, I. Riadi & A. Dahlan, "Analisis Validasi Image PNG File Upload menggunakan Metadata pada Aplikasi Berbasis Web," Edu Komputika J., Vol. 7, No. 1, pp. 10–15, Jun. 2020.

[9] Jamaludin et. al., "Kriptografi: Teknik Keamanan Data," Kita Menulis, April 2022.

[10] A. L. Firmansyah, "Analisis Metadata Forensik Untuk Korelasi Bukti Digital," Repositori Thesis Universitas Siliwangi, 2020. http://repositori.unsil.ac.id/2421/

[11] R. Umar, A. Fadlil & I. A. Putra, "Analisis Forensics Untuk Mendeteksi Pemalsuan Video," J-SAKTI (Jurnal Sains Komput. dan Inform.), Vol. 3, No. 2, pp. 193, 2019. doi: 10.30645/j-sakti.v3i2.140.

[12] M. F. Armandani "QR Code Digitalisasi Manajemen Sistem Dokumen Menggunakan Qr Code Generator dan Digital Signature," Techno Xplore J. Ilmu Komput. dan Teknol. Inf., Vol. 6, No. 2, pp. 68–74, Oct. 2021, doi: 10.36805/TECHNOXPLORE.V6I2.1761.

[13] M. Simanjuntak & J. Panjaitan, "Analisa Recovery Data Menggunakan Software Komputer Forensik," JUTISAL Jurnal Teknik Informatika Universal, Vol. 1, No. 1, 2021. https://jurnal.universal.ac.id/index.php/jutisal/article/view/3