ISSN : 1411-1624
e-ISSN: 2621-808

ANALISIS DIGITAL FORENSIK REKAYASA *IMAGE* MENGGUNAKAN *JPEGSNOOP* DAN *FORENSICALLY BETA*

Irwansyah [1], Helda Yudiastuti[2]
Dosen Universitas Bina Darma [1,2]
Jalan Jenderal Ahmad Yani No.3 Palembang
Sur-el : irwansyah@binadarma.ac.id[1], helda.yudiastuti@binadarma.ac.id[2]

Abstract : *The development of information technology is not only beneficial for humans, but often also used for negative purposes. Crime by utilizing digital image technology is very easy to do using a computer, so it is not surprising if more and more cases of cybercrime occur. The spread of digital images on social media in the form of images or videos raises public anxiety that these images or videos cannot be considered reliable evidence, because both images and videos can be easily engineered. The purpose of this study is to analyze a digital image that has been manipulated or engineered using a particular software or program. Image manipulation techniques that will be used are: Image splicing, copy-move, and retouching images. While the analysis tool uses the ELA method introduced by Krawetz which is available online from the website (https://29a.ch/photo-forensics/#forensic-magnifier) and Jpegsnoop software*.

Keywords: *Digital Image, Cyber Crime, Metode ELA.*

Abstrak : Perkembangan teknologi informasi tidak hanya bermanfaat bagi manusia, tetapi sering juga digunakan untuk kepentingan negatif. Kejahatan dengan memanfaatkan teknologi digital image sangat mudah dilakukan dengan menggunakan komputer, maka tidaklah heran jika semakin hari semakin banyak terjadi kasus cybercrime. Penyebaran digital image pada social media baik berupa gambar atau video menimbulkan kecemasan pada masyarakat bahwa gambar atau video tersebut tidak dapat dianggap sebagai bukti yang terpercaya, karena baik gambar maupun video dapat direkayasa dengan mudah. Tujuan dari penelitian ini adalah untuk menganalisis sebuah digital image yang telah dimanipulasi atau direkayasa dengan menggunakan software atau program tertentu. Teknik manipulasi gambar yang akan digunakan yaitu : Image splicing, copy-move, dan retouching images. Sedangkan alat analisis menggunakan metode ELA yang diperkenalkan oleh Krawetz yang tersedia secara online dari website (https://29a.ch/photo-forensics/#forensic-magnifier) serta software Jpegsnoop.

Keywords: *Digital Image, Cyber Crime, Metode ELA.*

1. PENDAHULUAN

Dalam perkembangan teknologi *digital image* yang sangat pesat dapat membantu bagi kehidupan manusia, dengan adanya bantuan teknologi ini pekerjaan manusia menjadi semakin mudah. Perkembangan teknologi bukan hanya memiliki banyak manfaat bagi manusia, tetapi juga mempunyai sisi negatif. Dengan memanfaatkan teknologi *digital image* kejahatan dapat dilakukan dengan mudah menggunakan komputer, sehingga tidak heran jika semakin hari semakin banyak terjadi kasus *cyber crime*. Penggunaan *software editing* yang bagus memungkinkan pengguna untuk memproses digital image dengan cara yang mudah. Sehingga pemalsuan *digital image* tidak dapat dihindari dan semakin meluas. Penyebaran *digital image* pada social media menimbulkan kecemasan pada masyarakat bahwa gambar atau video tidak dapat

ISSN : 1411-1624
e-ISSN: 2621-808

dianggap sebagai bukti yang terpercaya, karena baik gambar maupun video dapat direkayasa dengan mudah.

Penyebaran digital image yang telah dimanipulasi oleh pihak lain untuk kepentingan individu ataupun kelompok telah banyak merugikan semua pihak baik dari perorangan maupun organisasi. Karena sebuah *digital image* dapat dijadikan sebuah berita, ataupun bukti – bukti isu autentik pada masyarakat. Bermacam – macam tujuan dapat digunakan dalam manipulasi digital image, seperti untuk hiburan, iklan, hingga criminal yang dapat mengelabui penyidik. Contoh pada kasus pornografi sebuah image yang telah dimanipulasi dapat merusak nama dan reputasi seseorang hingga ke perusahaan.

Adapun tujuan pada penelitian ini yaitu untuk menganalisis sebuah *digital image* yang telah dimanipulasi atau direkayasa dengan menggunakan *software* atau program tertentu serta peralatan kamera digital yang digunakan pada proses pengambilan gambar. Manipulasi gambar dapat dikategorikan menjadi tiga jenis; Image splicing, manipulasi gambar copy-move, dan retouching images [1].

Analisis digital forensik memiliki cakupan yang cukup luas, sehingga dapat dikelompokan berdasarkan pada bentuk fisik maupun logis. Barang bukti yang dianalisis dengan cakupan komputer forensik yaitu, *mobile* forensik, audio forensik, video forensik, *image* forensik, dan *cyber* forensik. Dalam penelitian ini sendiri akan menggunakan *image* forensik, dimana forensik ini berkaitan dengan jenis barang bukti *digital* yang berupa *file* gambar *digital*. Sedangkan tools analisis yang digunakan pada penelitian ini yaitu *Jpegsnoop* dan *Forensically Beta.*

.

2. METODOLOGI PENELITIAN

2.1 Metode Penelitian

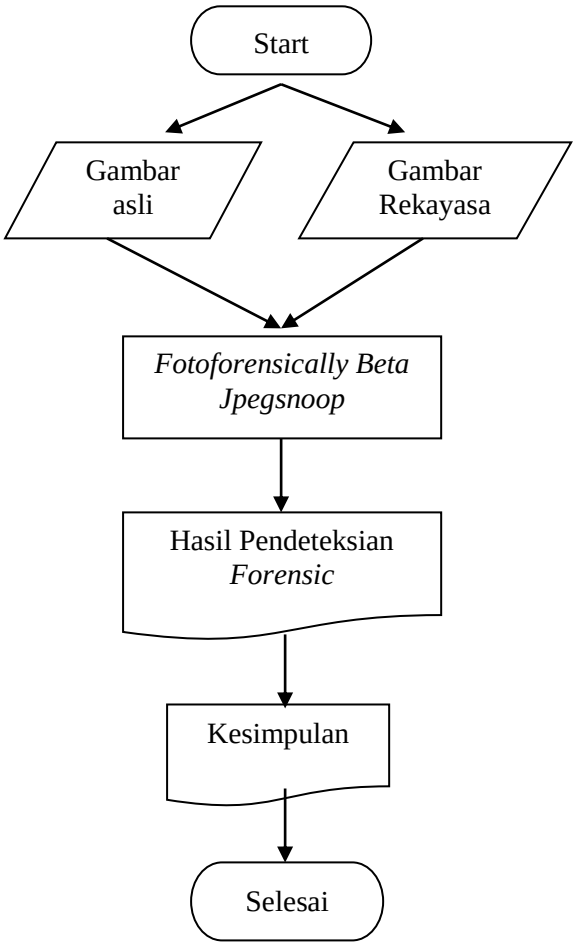
Metode yang s gunakan dalam penelitian adalah metode deskriptif. Metode deskriptif dapat diartikan sebagai prosedur pemecahan masalah yang diselidiki dengan menggambarkan keadaan subjek atau objek dalam penelitian dapat berupa orang, lembaga, masyarakat dan yang lainnya yang pada saat sekarang berdasarkan fakta-fakta yang tampak atau apa adanya.

Metode deskriptif merupakan suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran ataupun suatu kelas peristiwa pada masa sekarang. Tujuan dari penelitian deskriptif ini adalah untuk membuat deskripsi, gambaran, atau lukisan secara sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antarfenomena yang diselidiki [2].

Teori menyebutkan bahwa metode deskriptif adalah suatu metode yang digunakan untuk menggambarkan atau menganalisis suatu hasil penelitian tetapi tidak digunakan untuk membuat kesimpulan yang lebih luas [3].

Pada penelitian ini peneliti menggunakan skenario sendiri untuk melakukan pendeteksian dalam mendapatkan suatu bukti digital. Berikut flowchart alur proses dalam analisis *forensics digital image.*

ISSN : 1411-1624
e-ISSN: 2621-808



Gambar 1. Flowchart Proses Penelitian

2.2 Error Level Analisis (ELA)

Error Level Analysis adalah metode forensik untuk mengidentifikasi bagian-bagian dari suatu gambar dengan tingkat yang berbeda dari kompresi. Teknik ini dapat digunakan untuk menentukan apakah gambar telah dimodifikasi secara digital. Teknik ELA diperkenalkan oleh Krawetz yang tersedia secara online dari website (https://29a.ch/photo-forensics/#forensic-magnifier) [4].

2.3 Analisis

Analisis adalah kegiatan berfikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda – tanda komponen, hubungannya satu sama lain dan fungsi masing – masing dalam satu keseluruhan terpadu [5]. Analisis juga dapat dijelaskan sebagai penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan [6].

Analisis adalah mengelompokkan, membuat suatu urutan, memanipulasi, serta menyingkatkan data sehingga mudah dibaca [2]. Analisis data merupakan salah satu rangkaian dalam kegiatan penelitian. Sehingga kegiatan menganalisis data berkaitan dengan rangkaian kegiatan sebelumnya mulai dari jenis penelitian yang telah dipilih, rumusan masalah dan tujuan penelitian, jenis data, jumlah variabel, serta asumsi-asumsi teoritis yang melandasi kegiatan-kegiatan penelitian. Dengan demikian, dalam melakukan analisis data perlu memperhatikan rangkaian tahap sebelumnya sebagai rujukan agar penelitian yang dilaksanakan bertalian atau berhubungan dengan tahap-tahap penelitian yang lain.

2.4. Digital forensik

Digital forensik adalah cabang ilmu komputer yang berfokus pada pengembangan bukti yang berkaitan dengan *file digital* untuk digunakan dalam pengadilan perdata atau pidana. Bukti forensik digital akan berhubungan dengan dokumen komputer, email, teks, foto *digital*, program perangkat lunak, atau rekaman digital lainnya yang berkaitan dengan kasus hukum [7].

ISSN : 1411-1624
e-ISSN: 2621-808

Forensik *digital* (kadang-kadang dikenal sebagai ilmu forensik *digital*) adalah cabang dari ilmu forensik meliputi pemulihan dan investigasi dari barang yang ditemukan dalam perangkat *digital*, kaitannya dengan kejahatan komputer. Istilah forensik *digital* awalnya digunakan sebagai sinonim untuk forensik komputer tetapi diperluas untuk mencakup penyelidikan semua perangkat yang mampu menyimpan data *digital.* Investigasi forensik digital memiliki berbagai aplikasi. Yang paling umum adalah untuk mendukung atau menolak hipotesis sebelum pengadilan pidana atau perdata (sebagai bagian dari proses penemuan bukti elektronik)..

2.5. *Image* Forensik

Teknik forensik untuk memeriksa keaslian *file* foto, merupakan salah satu bagian dalam teknik fotografi forensik, yang digunakan untuk memeriksa suatu alat bukti, dalam bentuk *file* gambar yang menjadi salah satu alat bukti yang bisa diajukan ke persidangan, apabila *file* foto tersebut sesuai dengan standar yang ditetapkan hukum, selain itu juga bisa digunakan untuk fungsi dokumentasi, analisis intelijen. Dalam pemeriksaan keaslian *file* foto digunakan beberapa teknik forensik untuk pembuktian dan pemeriksaan terhadap foto tersebut baik dengan menggunakan *software* yang digunakan untuk memeriksa data sensitif yang terdapat di dalam foto dengan bantuan alat-alat dan teknik fotografi.

Dalam *image forensic*, objek yang diperiksa dan dianalisis adalah *image file*. *Image file* itu sendiri memiliki dua pengertian yang berbeda. Pertama merujuk pada hasil *forensic imaging* (duplikasi secara fisik sektor per sektor) yang menggunakan metode terkini *disk to file*. Kedua merujuk pada *file* gambar hasil fotografi menggunakan kamera, *handycam*, atau *handphone* yang menggunakan sistem penyimpanan *file digital*. *File* gambar digital berasal dari hasil proses *capturing* (menangkap) objek dengan menggunakan peralatan kamera yang bersifat digital. Ini dilakukan oleh seseorang dalam rangka mengabadikan momen-momen penting di sekitarnya sehingga di kemudian hari bisa membuka dan melihat kembali momen tersebut melalui *file* gambar digital yang telah dihasilkan. Ketika seseorang merasa momen yang penting dan baik tersebut perlu untuk di *sharing* (dibagi), maka akan berbagi *file* gambar tersebut dengan mereka. Adakalanya gambar tersebut diolah terlebih dulu dengan bantuan aplikasi komputer sebelum di*upload* oleh *editing* grafis.

Gambar-gambar *digital* tersebut bisa menyenangkan hati bagi orang yang melihat, namun bisa juga menimbulkan masalah ketika gambar tersebut menunjukkan momen yang menjelek-jelekkan orang lain. Misalnya memfitnah orang lain dengan merekayasa gambar tersebut dengan bantuan aplikasi komputer seolah-olah orang tersebut melakukan hal yang tidak senonoh atau tidak sepantasnya, sehingga orang tersebut merasa malu dan tercemar nama baiknya. Untuk sebagian masyarakat awam yang tidak memahami rekayasa gambar digital, maka mereka akan menganggap bahwa momen palsu ada di gambar digital tersebut seakan asli. Hal ini dapat

ISSN : 1411-1624
e-ISSN: 2621-808

berakibat harga diri dan posisi orang yang dijelek-jelekkan menjadi jatuh, baik dimata keluarga maupun rekan kerabat. Untuk hal-hal seperti ini, terhadap gambar digital tersebut perlu dilakukan pemeriksaan dan analisis yang mendalam untuk memastikan apakah gambar tersebut palsu hasil rekayasa grafis komputer, atau justru asli hasil *capturing* dengan menggunakan peralatan fotografi [7].

2.6 *JPEGSnoop*

JPEGSnoop merupakan aplikasi gratis yang dapat mendeteksi apakah sebuah foto telah dimanipulasi atau merupakan sebuah foto original. *JPEGsnoop* dapat mendeteksi berbagai macam *setting* yang digunakan pada sebuah kamera digital *(EXIF metada*ta, IPTC) dan juga dapat membandingkan sebuah foto dengan banyak parameter variasi kompresi. Parameter ini bervariasi, tergantung kamera atau *software* yang digunakan. *JPEGSnoop* memberikan banyak informasi mengenai sebuah foto, termasuk *quantization table matrix (chrominance dan luminance), chroma subsampling*, perkiraan 41 kualitas JPEG, *setting resolusi JPEG, tabel Huffman, EXIF metadata, Makernotes, histogram RGB* dan masih banyak lagi [8]. *JPEGSnoop* dapat membaca file yang berformat seperti, *(.JPG, .THM, .AVI, .DNG, .CRW, .CR2, .NEF, .ORF, .PEF, .RAW, .MOV, .PDF)* [8].

3. HASIL

Dalam penelitian ini ada beberapa tahapan yang dilakukan yaitu rekayasa *image* atau manipulasi gambar dan analisis *image digital*.

3.1 Rekayasa Image atau Manipulasi Gambar.

Rekayasa Image dapat dikategorikan me njadi 3 jenis yaitu :

a. Rekayasa *Image Splicing.*

Image splicing yaitu proses menggabungkan dua gambar atau lebih untuk membuat gambar baru. Contoh *Image Spilicing* dapat dilihat pada gambar 2. Rekayasa *Image Splicing.*

(a)

(b)

ISSN : 1411-1624
e-ISSN: 2621-808

(c)

Gambar 2. Rekayasa *Image Splicing* (a) gambar asli 1 (b) gambar asli 2 (c) gambar hasil rekayasa.

b. Rekayasa *Image Copy - Move.*

Rekayasa *Image Copy - Move* yaitu proses yang dilakukan dengan cara penyalinan atau penyisipan gambar tertentu dalam gambar asli yang sama. Contoh Rekayasa *Image Copy - Move* dapat dilihat pada gambar 3. Rekayasa *Image Copy – Move.*

(a)

(b)

Gambar 3. Rekayasa *Image Copy – Move* (a) gambar asli (b) gambar hasil rekayasa.

c. Rekayasa *Retouching Images.*

Retouching Images yaitu proses pengubahan piksel pada gambar. Hal ini dilakukan dengan misalnya merubah warna gambar tanpa mengubah arti yang sebenarnya. Contoh Rekayasa *Retouching Images* dapat dilihat pada gambar 4. Rekayasa *Retouching Images*

(a)

(b)

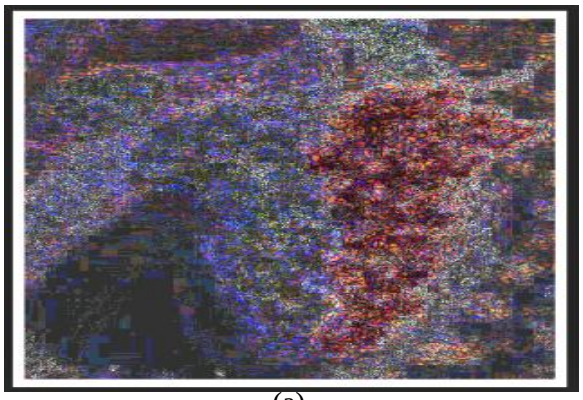
Gambar 4. Rekayasa *Retouching Images*

3.2 *Forensically Beta pada* Rekayasa *Image Splicing.*

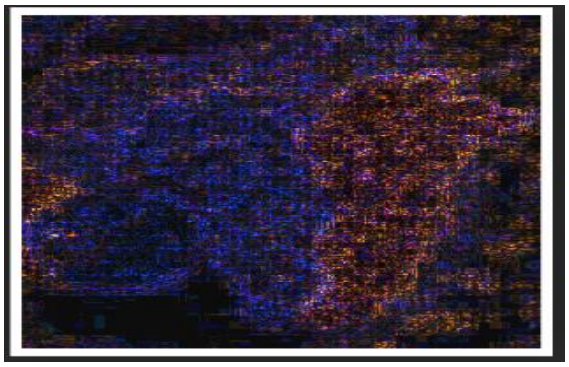
Adapun hasil pendeteksian ELA (Error Level Analysis) menggunakan *Forensically Beta* pada sebuah gambar jpeg yang telah

ISSN : 1411-1624
e-ISSN: 2621-808

direkayasa menggunakan cara Image Splicing akan menghasilkan gambar bintik – bintik yang lebih gelap. Sedangkan gambar yang asli atau gambar yang belum di manipulasi menghasilkan bintik bintik warna putih terang. Hasil dapat dilihat pada gambar 5. Hasil *Forensically Beta ELA.*



(a)



(b)

Gambar 5. Hasil *Forensically Beta ELA* (a) gambar asli (b) gambar manipulasi dengan *Image Splicing*.

3.3. *Forensically Beta pada* Rekayasa *Image Copy - Move.*

Hasil analysis *Forensically Beta ELA* pada gambar jpeg yang telah direkayasa menggunakan cara Rekayasa *Image Copy – Move* akan menghasilkan gambar bintik – bintik yang lebih gelap. Sedangkan gambar asli menghasilkan bintik bintik warna putih terang, hasil ini sama dengan gambar yang direkayasa menggunakan Image Splicing. Hasil dapat dilihat pada gambar 6. Hasil *Forensically Beta ELA* Rekayasa Image Copy Move.

(a)

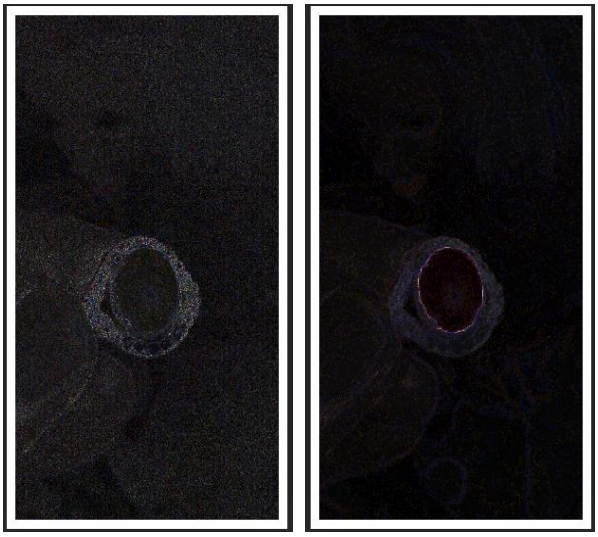
(b)

Gambar 6. Hasil *Forensically Beta ELA* (a) gambar asli (b) gambar manipulasi dengan *Image Copy Move*.

3.4 *Forensically Beta pada* Rekayasa *Retouching Images.*

Pada rekayasa *Retouching Images* hasil dari *tools forensically Beta* dengan menggunakan metode ELA juga teridentifikasi gambar berbintik – bintik yang gelap. Hasil forensic metode ELA dapat dilihat pada gambar 7.

ISSN : 1411-1624
e-ISSN: 2621-808

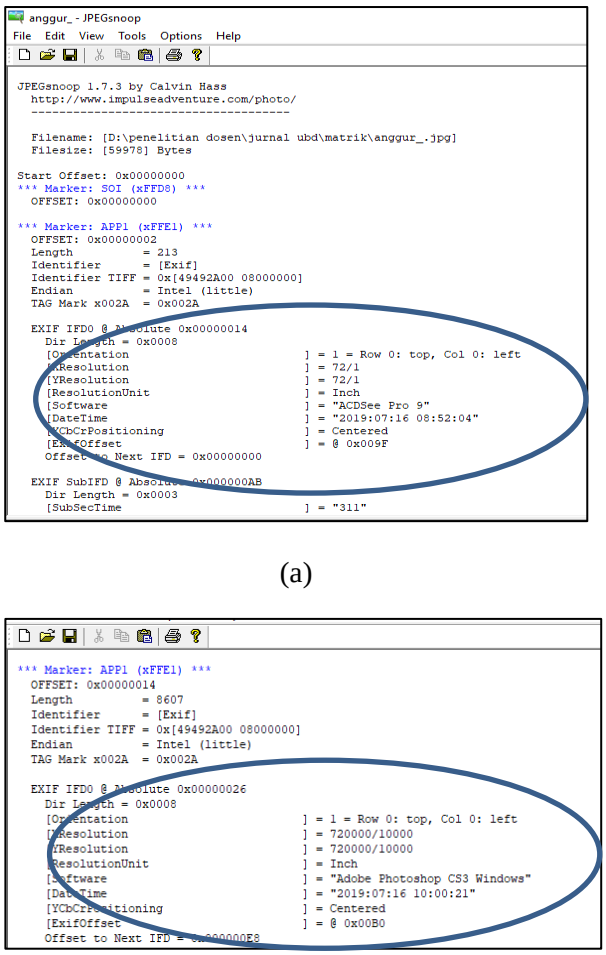


(a) (b)

Gambar 7. Hasil *Forensically Beta ELA* (a) gambar asli (b) gambar manipulasi dengan rekayasa *Retouching Images.*

3.5 Analisis *Forensic Jpegsnoop pada* Rekayasa *Image Splicing.*

Hasil yang didapat dari gambar asli (a) dan (b) dan gambar yang telah direkayasa Image Splicing (c) terdapat perbedaan yaitu : bahwa gambar asli diambil menggunakan *software ACDSee Pro 9*, tanggal 16 Juli 2019, dengan resolusi 72. Sedangkan gambar yang telah direkayasa terlihat telah direkayasa menggunakan *software Adobe Photoshop CS3 Windows*, tanggal 16 Juli 2019 dengan resolusi 720000. Hasil Jpegsnoop dapat dilihat pada gambar 8. Hasil *Forensic Jpegsnoop Rekayasa Image Splicing*.



(a)

(b)

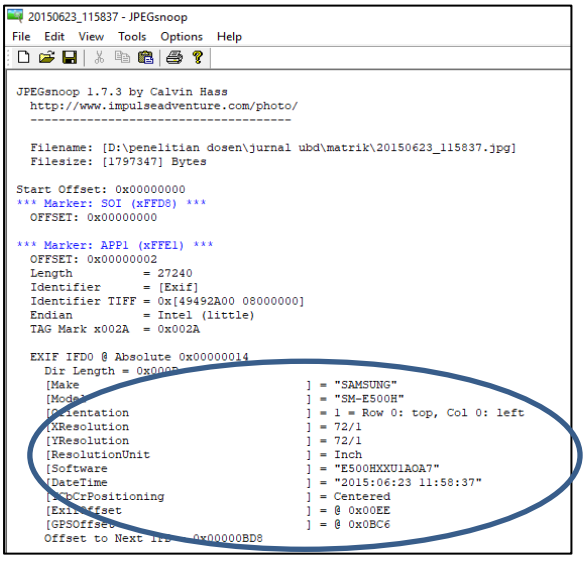
Gambar 8. Hasil *Forensic Jpegsnoop Rekayasa Image Splicing* (a) gambar asli (b) gambar rekayasa

3.6 Analisis *Forensic Jpegsnoop pada* Rekayasa *Image Copy - Move.*

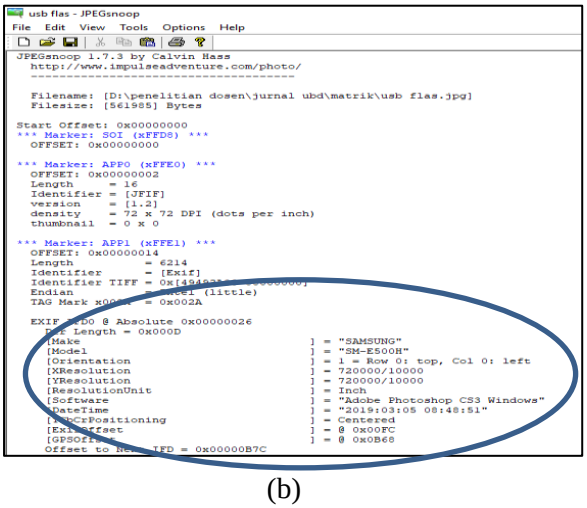
Adapun hasil analisis menggunakan tools *forensic Jpegsnoop* pada gambar (a) dan gambar (b) yang direkayasa menggunakan *Copy - Move* adalah sebagai berikut : pada gambar (a) terlihat Ada beberapa perbedaan pada gambar pertama yang merupakan gambar asli diambil menggunakan kamera Samsung dengan model SM-E500H. Resolusi gambar sebesar 72 X 72. Gambar diambil pada tanggal 23 Juni 2015. *Software* kamera menggunakan

ISSN : 1411-1624
e-ISSN: 2621-808

"E500HXXU1AOA7". Sedangkan untuk gambar ke dua atau gambar yang telah direkayasa, telihat bahwa gambar telah dirubah menggunakan software Adobe Photoshop CS3 Windows pada tanggal 05 Maret 2019. Resolusi gambar juga terjadi perubahan dari 72 menjadi 720000. Tetapi tidak terjadi perubahan pada kamera yang digunakan termasuk model dari kamera. Hasil Jpegsnoop dapat dilihat pada gambar 9. Hasil *Forensic Jpegsnoop Rekayasa Copy Move.*



(a)

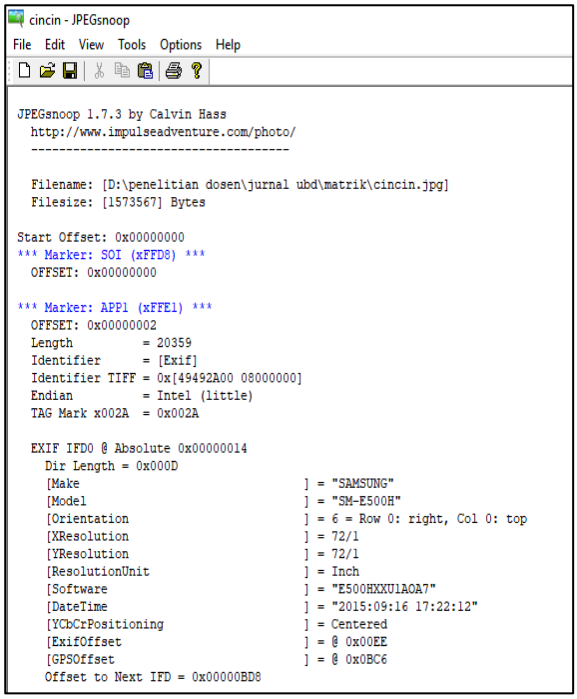


(b)

Gambar 9. Hasil *Forensic Jpegsnoop Rekayasa Copy - Move* (a) gambar asli (b) gambar rekayasa

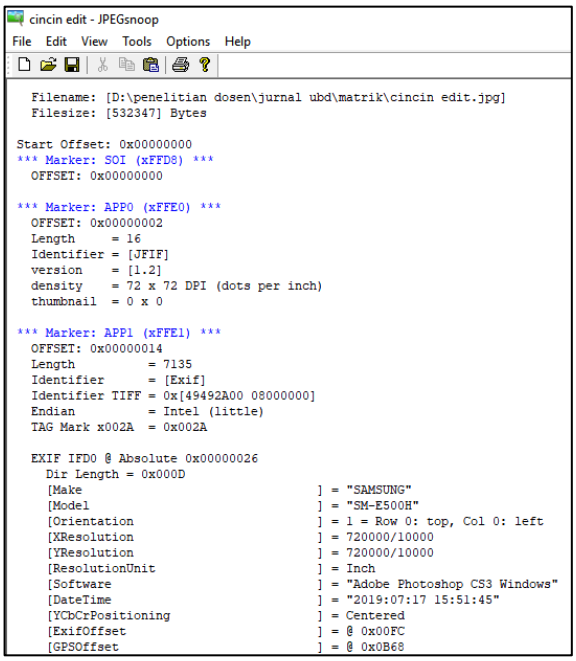
3.7 Analisis *Forensic Jpegsnoop pada* Rekayasa *Retouching Images.*

Hasil *forensic Jpegsnoop* gambar yang direkayasa menggunakan *Retouching Images* terdapat perbedaan yaitu : pada gambar pertama (a) yang merupakan gambar asli menggunakan kamera Samsung dengan type atau model SM-E500H dan resolusi gambar sebesar 72. Gambar diambil pada tanggal 16 September 2015. Software kamera yang digunakan yaitu E500HXXU1AOA7. Sedangkan pada gambar yang ke dua (b) atau gambar yang telah direkayasa, bahwa gambar telah terjadi perubahan menggunakan software Adobe Photoshop CS3 Windows pada tanggal 17 Juli 2019, dan menghasilkan resolusi gambar menjadi 720000. *Hasil Jpegsnoop* dapat dilihat pada gambar 10. Hasil *Forensic Jpegsnoop Rekayasa Retouching Images.*



(a)

ISSN : 1411-1624
e-ISSN: 2621-808



(b)

Gambar 10. Hasil *Forensic Jpegsnoop Retouching Images* (a) gambar asli (b) rekayasa

4. SIMPULAN

Adapun simpulan yang dapat diambil setelah melakukan *forensic image* dengan menggunakan *tools forensically beta* dan *jpegsnoop* adalah sebagai berikut :

Pendeteksian ELA (Error Level Analysis) menggunakan *Forensically Beta* terhadap rekayasa *Image splicing, Copy – Move dan Retouching Images* dapat mendeteksi perbedaan pada kedua objek. Selain itu analisis forensik image menggunakan aplikasi *JPEGSnoop* menampilkan hasil yang jelas terhadap perbedaan antara gambar yang asli dengan gambar yang telah direkayasa.

DAFTAR RUJUKAN

[1] Riadi, I., Fadlil, A., & Sari, T. (2017). *Image Forensic for detecting Splicing Image with Distance Function Image*,169

[2] Moh Nazir. 2003. *Metode Penelitian*. Jakarta: Ghalia Indonesia, 2003

[3] Sugiyono 2011. *Memahami Penelitian Kualitatif*. Alfabeta, Bandung.

[4] https://29a.ch/photo-forensics/#forensic-magnifier [accesed: 10-09-2018]

[5] Komarudin, 2001, *Eksiklopedia Manajemen*, Edisi IX, Jakarta : Bumi Aksara

[6] Alwi, Hasan. 2002. Kamus Besar Bahasa Indonesia Edisi Ketiga: Jakarta Balai Pustaka

[7] Al-Azhar, Muhammad Nuh, 2012, *Digital Forensic Panduan Praktis Investigasi Komputer*, Salemba Infotek, Jakarta.

[8] Calvinhass. (2017). *JPEGsnoop. Retrieved from* https://sourceforge.net/projects/jpegsnoop/[accesed: 10-09-2018]