



Perbandingan Hasil Analisa **FOTO HOAX**

Menggunakan
Metode Exif/Metadata Reverse Image
dan Image Forensics

Mof. Subli
Muhammad Masjun Efendi

Perbandingan Hasil Analisa FOTO HOAX

**Menggunakan
Metode Exif/Metadata Reverse Image
dan Image Forensics**

**Mofi. Subli
Muhammad Masjun Efendi**

PERBANDINGAN HASIL ANALISA FOTO HOAX MENGUNAKAN METODE EXIF/METADATA, REVERSE IMAGE DAN IMAGE *FORENSICS*

Tim Penulis:

MOH. SUBLI & MUHAMAD MASJUN EFENDI

Desain Cover:

Ridwan

Tata Letak:

Handarini Rohana

Editor:

Neneng Sri Wahyuni

ISBN:

978-623-5811-51-2

Cetakan Pertama:

Desember, 2021

Hak Cipta 2021, Pada Penulis

Hak Cipta Dilindungi Oleh Undang-Undang

Copyright © 2021

by Penerbit Widina Bhakti Persada Bandung

All Right Reserved

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari Penerbit.

PENERBIT:

WIDINA BHAKTI PERSADA BANDUNG

(Grup CV. Widina Media Utama)

Komplek Puri Melia Asri Blok C3 No. 17 Desa Bojong Emas
Kec. Solokan Jeruk Kabupaten Bandung, Provinsi Jawa Barat

Anggota IKAPI No. 360/JBA/2020

Website: www.penerbitwidina.com

Instagram: [@penerbitwidina](https://www.instagram.com/penerbitwidina)

PRAKATA

Buku dengan judul “Perbandingan Hasil Analisa Foto Hoax Menggunakan Metode Exif/Metadata, Reverse Image Dan Image *Forensics*” ini ditujukan kepada masyarakat untuk berfikir dewasa dan penuh pertimbangan dalam menyebarkan sebuah informasi berupa foto-foto atau gambar-gambar yang belum tentu teruji kebenarannya, sehingga fokus pada buku ini adalah dengan melihat dan menganalisa sebuah informasi tersembunyi pada sebuah foto dengan beberapa metode/tools yang sudah di uji cobakan, yang kesimpulannya masyarakat bisa membedakan mana foto asli dan mana foto yang sudah di edit/manipulasi dengan menggunakan metode/tools tersebut.

Buku ini menerapkan perkembangan teknologi terkini dan mudah digunakan oleh masyarakat awam sekalipun setelah membaca petunjuk-petunjuk pada buku ini, mulai dari penerapan *Tools Exif/Metadata Exiftool By Phil Harvey, Tools Jeffrey's Image Metadata Viewer, Exif & Metadata Viewer, Reverse Image Dan Image Forensics*. Nantinya kritik dan saran yang membangun dari berbagai pihak sangat diharapkan demi penyempurnaan buku ini di masa mendatang.

Penulis mengucapkan terima kasih banyak kepada semua pihak, terkhusus Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi yang telah memberi dukungan financial terhadap buku ini dan ucapan terima kasih banyak juga kepada pihak kampus Universitas Teknologi Mataram yang telah memberi kesempatan dan dukungan kepada penulis untuk menyelesaikan proses pembuatan buku ini, sehingga terlaksana dengan baik dan lancar sesuai dengan jadwal yang telah ditetapkan.

Semoga buku ini dapat memberikan manfaat bagi para pembaca, masyarakat umum dan penulis khususnya.

Mataram, 17 Desember 2021

Penulis

DAFTAR ISI

PRAKATA	iii
DAFTAR ISI	iv
BAB 1 PENDAHULUAN.....	1
A. Latar Belakang	1
B. Tujuan Penelitian	3
C. Luaran Hasil Penelitian	3
BAB 2 TINJAUAN PUSTAKA.....	5
A. Landasan Teori.....	5
1. Informasi Hoax	5
2. Manipulasi Foto	6
3. Metode / Tools.....	7
B. Penelitian Terdahulu	7
BAB 3 METODE PENELITIAN	9
A. Metode Yang Digunakan	9
B. Fisnbone Diagram Penelitian	10
C. Analisa Kebutuhan / Kebutuhan Metode	11
1. Kebutuhan Perangkat Keras.....	12
2. Kebutuhan Perangkat Lunak	12
3. Kebutuhan Tahapan Uji Coba	12
4. Kebutuhan Metode / Tools	15
BAB 4 PEMBAHASAN HASIL PENELITIAN	21
A. Implementasi dan Uji Sistem	21
1. Bukti Foto dari Internet/Media Sosial.....	21
2. Bukti Foto dari Smartphone/Laptop	35
B. Analisa Hasil Perbandingan	52
1. Bukti Foto dari Internet/Media Sosial.....	52
2. Bukti Foto dari Smartphone/Laptop	54
BAB 5 PENUTUP	61
A. Kesimpulan	61
B. Saran	62
DAFTAR PUSTAKA	63
PROFIL PENULIS	66



PENDAHULUAN

A. LATAR BELAKANG

Indonesia setiap lima tahun sekali selalu menyelenggarakan pesta demokrasi yaitu PEMILU, PILEG dan PILKADA. Pesta demokrasi yang diselenggarakan lima tahun sekali ini akan memilih wakil-wakil rakyat yang akan duduk di kursi parlemen. Pemilu tahun 2019 misalnya menghadapi permasalahan yaitu gelombang hoax. Hoax muncul bertubi-tubi dalam berbagai konteks persebaran informasi, tidak hanya politik saja, tetapi dibidang lain seperti agama, suku, ras, ekonomi. pendidikan, kesehatan, sampai dari urusan publik hingga privat seseorang (Kominfo, 2018). Banyak sekali bermunculan konten-konten yang sifatnya ingin mempengaruhi para pemilih, baik untuk kebutuhan pileg maupun pilpres. Konten-konten tersebut ada yang menampilkan kelebihan-kelebihan calon dan adapula sampai menjelek-jelekkan calon dengan menampilkan keburukan-keburukan yang pernah dilakukan oleh salah satu calon. Semua ini tidak lain dilakukan dengan niat dan tujuan bagaimana bisa mempengaruhi para pemilih yang semula ada dikubu sebelah agar berpindah ke kubunya. Namun yang jadi perhatian adalah isi dari konten yang disebarkan oleh para penggiat tim sukses para calon atau orang yang menyebarkan suatu konten, seperti konten yang benar-benar asli adanya tanpa sebuah rekayasa yang sengaja dibuat atau kata fenomenalnya disebut informasi hoax.

Informasi hoax yang tersebar selama ini banyak berupa foto-foto yang sudah diedit dan dimanipulasi dari foto-foto yang sebenarnya, kemudian foto-foto tersebut menyebar secara berantai di dunia elektronik lewat situs-situs internet dan media sosial. Perkembangan foto yang semakin maju membuatnya memiliki banyak keunggulan untuk dijadikan berita hoax seperti

mudahnya dimanipulasi, mudah disebarkan secara massif dan luas serta mudah sekali membuat orang cepat percaya. Perubahan foto yang dapat dibuat atau diedit dengan mudah, sehingga dapat merubah informasi yang disampaikan menjadi berbeda dan membuatnya rawan digunakan untuk tindak kejahatan. Dunia internet kini dipenuhi banyak sekali informasi hoax, provokasi, fitnah, sikap intoleran dan anti agama. Keberadaan internet sebagai media *online* membuat informasi yang belum terverifikasi benar dan tidaknya tersebar begitu cepat. Hanya dalam hitungan detik, suatu peristiwa sudah bisa langsung tersebar dan diakses oleh pengguna internet lainnya yang berada jauh. Bahkan orang kadang belum sempat memahami materi informasi, reaksi atas informasi tersebut sudah lebih dulu terlihat.

Berdasarkan hasil penelitian Mastel (2017), jenis hoax yang paling sering diterima masyarakat adalah bidang sosial politik (Pilkada, pemerintah) dan masalah SARA. Kementerian Komunikasi dan Informatika (Kemenkominfo) mendata ada 1.000 berita hoax yang disebar dari awal masa kampanye sampai sekarang. Berita hoax itu menyerang kedua pasangan calon presiden dan calon wakil presiden. “Menurut mesin scrolling kami, ada 1.000 lebih konten hoax yang berkaitan dengan konten politik dan beberapa instrumen pendukungnya, terkait partai, kampanye menjelang pilpres dan pileg ini,” ucap Plt Kabiro Humas Kemenkominfo, Ferdinandus Setu, di Ibis Budget Hotel, Jalan Cikini Raya, Jakarta Pusat, Jumat (19/10/2018). Diantara konten-konten penyebaran informasi hoax yang tersebar selama ini banyak berupa foto-foto yang sudah diedit dan dimanipulasi dari foto-foto yang sebenarnya, kemudian foto-foto tersebut menyebar secara berantai di dunia elektronik lewat situs-situs internet dan media sosial. Dengan banyak foto-foto yang dijadikan sebagai sarana tindak kejahatan maka perlu dilakukan sebuah penelitian yang bisa dijadikan sebagai pedoman untuk bisa melihat foto mana yang asli dan yang palsu dengan menggunakan sebuah metode. Banyak sekali beredar sebuah metode yang bisa melihat keaslian dan kepalsuan foto tersebut. Namun dari banyak yang beredar, tidak jarang yang memiliki tingkat pengujian yang tidak mendekati kebenaran, karena kelayakan dan tingkat kebenaran dari metode tersebut masih belum bisa dipercaya.

Dengan banyak foto-foto yang dijadikan sebagai sarana tindak kejahatan maka perlu dilakukan sebuah penelitian yang bisa dijadikan sebagai pedoman untuk bisa melihat foto mana yang asli dan yang palsu dengan menggunakan sebuah metode. Banyak sekali beredar sebuah metode yang bisa melihat keaslian dan kepalsuan foto tersebut. Namun dari banyak yang beredar, tidak jarang yang memiliki tingkat pengujian yang tidak mendekati kebenaran, karena kelayakan dan tingkat kebenaran dari metode tersebut masih belum bisa dipercaya. Untuk itu didalam penelitian ini penulis mencoba untuk

membandingkan hasil analisa foto hoax dengan menggunakan metode exif/metadata, reverse image dan image *forensics*. Ketiga metode ini akan dijadikan contoh mana yang lebih mendekati kebenaran yang kemudian bisa dijadikan pedoman atau rujukan oleh orang-orang untuk membuktikan keaslian sebuah foto atau informasi yang sedang menyebar luas ditengah-tengah masyarakat khususnya pada musim pemilu, pileg dan pilkada.

B. TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah menghasilkan suatu metode/cara tepat yang bisa dijadikan pedoman atau rujukan dalam penentuan keaslian sebuah informasi berupa foto yang bisa dijadikan bukti valid dipersidangan misalnya atau pegangan bagi orang-orang sebelum mengambil keputusan untuk menyebarluaskan kembali foto tersebut atau tidak karena sudah ketahuan keaslian atau sebaliknya foto hoax.

C. LUARAN HASIL PENELITIAN

Output penelitian ini berupa sebuah metode yang tepat yang akan bermanfaat bagi orang banyak. Metode ini akan sangat membantu khususnya orang-orang yang sedang mengikuti pemilu, pileg dan pilkada. Mempermudah orang-orang dalam menganalisa sebuah informasi tersebar secara cepat dan tepat yang dapat membantu penekanan penyebaran sebuah informasi hoax.

BAB
2

TINJAUAN PUSTAKA

A. LANDASAN TEORI

1. Informasi Hoax

Penelitian yang dilakukan (Juliswara, 2017) bahwa kebhinnekaan sebagai pengikat sosial diuji karena kecenderungan praktik ujaran kebencian yang dipromosikan melalui media sosial. Kondisi itu diperparah oleh penyalahgunaan media sosial seperti persebaran berita bohong atau informasi palsu (hoax) yang dampaknya menimbulkan permusuhan dan tidak sesuai dengan budaya bangsa Indonesia yang mengutamakan toleransi.

Keberadaan internet sepaket dengan kebudayaan yang terbangun di dalam ruang publik baru membuat masyarakat sulit membedakan informasi faktual dan hoax. Jalan utama untuk mengantisipasi hoax adalah membangun kompetensi publik dalam menghadapi luapan banjir informasi. Upaya membangun kompetensi publik dilakukan melalui literasi media (Gumilar, Adiprasetio, & Maharani, 2017).

Dalam penelitiannya (Adhiarso, Utari, & Slamet, 2017) mengatakan Media online/internet mempunyai peranan penting yang terletak pada kemampuannya untuk menyajikan berita-berita tentang perkembangan masyarakat yang bisa mempengaruhi kehidupan modern pada saat ini. Oleh karena individu diyakini sangat terpengaruh oleh pesan-pesan media mengingat media dianggap sangat kuat dalam membentuk opini masyarakat.

Saat ini penyebaran informasi/berita bohong (hoax) makin marak. Survei Mastel 2017 mengungkapkan bahwa masyarakat menerima hoax setiap hari lebih dari satu kali. Saluran yang paling banyak digunakan dalam penyebaran hoax adalah media sosial. Fenomena hoax di Indonesia menimbulkan keraguan terhadap informasi yang diterima dan membingungkan masyarakat. Hal ini

dimanfaatkan pihak yang tidak bertanggung jawab untuk menanamkan fitnah dan kebencian. Karena itu, penelitian ini bertujuan untuk mendapatkan gambaran tentang interaksi komunikasi hoax di media sosial dan cara mengantisipasinya (Juditha, 2018).

Bahkan didalam pengambilan keputusan untuk pengembangan jiwa kewirausahaan mensyaratkan adanya kemampuan untuk mengambil keputusan dalam menghadapi berbagai resiko. Dimana dalam mengambil keputusan sangat dibutuhkan informasi dan kemampuan mendapatkan informasi yang tepat. Salah satu sumber informasi adalah media social dan lagi *trend* saat ini. Namun persoalan adanya kecenderungan masih lemahnya kemampuan menyaring berita menyebabkan perlunya adanya solusi untuk mengatasi masalah tersebut. Menilai kemampuan menilai kebenaran sebuah berita dari mahasiswa sangat berguna dalam menilai jiwa kewirausahaan mahasiswa dalam mengambil keputusan berwirausaha bahwa kemampuan menilai sebuah berita dapat dilihat dari: penilaian judul, penilaian situs, kontens, foto dan sumber berita (Fatkhurahman, 2018).

2. Manipulasi Foto

Perkembangan software pengolahan gambar sangat banyak dan bermacam-macam, dengan tersedianya beberapa program aplikasi yang ada mampu dapat merubah dan memodifikasi gambar asli menjadi gambar yang telah diubah bahkan gambar asli dan gambar termodifikasi nyaris tidak dapat dibedakan. Perubahan modifikasi tersebut dilakukan untuk tujuan mempercantik tampilan gambar, atau memperbaiki kualitas gambar agar lebih baik hasilnya. Pada kenyataannya memodifikasi gambar adapula dengan tujuan yang tidak baik. Memodifikasi dengan tujuan untuk menyamarkan data aslinya, atau membuat modifikasi gambar untuk kepentingan menyudutkan seseorang dengan gambar-gambar yang tidak layak, diubah bentuk dan terlebih-lebih banyak gambar artis yang dimodifikasi untuk kepentingan tertentu (Heriyanto, 2013).

Pertumbuhan pesat manipulasi citra digital telah mendorong para penulis di forensik gambar untuk mengungkapkan keasliannya. Manipulasi adalah biasanya ditemukan dalam format gambar seperti *Joint Photographic Kelompok Pakar* (JPEG). JPEG adalah format yang paling umum didukung oleh perangkat dan aplikasi (Riadi, Fadlill & Sari, 2017).

Perkembangan foto yang semakin maju membuatnya memiliki banyak keunggulan dan kekurangan, salah satunya adalah mudahnya dimanipulasi dengan software *editing*. Perubahan foto dapat dibuat atau diedit dengan mudah, sehingga dapat merubah informasi yang disampaikan menjadi berbeda

dan membuatnya rawan digunakan untuk tindak kejahatan (Riadi, Yudhana & Yuli Sulisty, 2019).

3. Metode / Tools

Berikut ada 3 jenis metode atau tools yang digunakan pada penelitian ini yaitu Exif/Metadata, Reverse Image dan Image *Forensics*.

Teknik pengamanan data dan informasi merupakan salah satu cara untuk menjaga kerahasiaan suatu obyek. *Exchangable Image File Format* (EXIF) Metadata adalah informasi data tentang citra digital. Dalam penyelidikan forensik digital, ini sangat berguna untuk keamanan hak cipta atau pengamanan bukti digital. (Wijiyanto, 2018).

Reverse image adalah salah satu teknik yang berhubungan dengan banyak teknik baru lainnya seperti menangani pengetahuan tersembunyi menggunakan ekstraksi, asosiasi data, menemukan pola tambahan. (Adrakatti, 2016).

Bidang ilmu forensik citra digital akan membantu para penegak hukum, intelijen, investigasi swasta dan media. Semakin majunya teknologi image pada saat ini mengangkat isu-isu baru dan tantangan dalam menentukan keaslian image. Forensik citra digital merupakan salah satu metode ilmiah pada bidang penelitian yang bertujuan untuk mendapatkan fakta-fakta pembuktian dalam menentukan keaslian image (Yuli Sulisty, Riadi, & Yudhana, 2018).

B. PENELITIAN TERDAHULU

State Of the Art atau beberapa penelitian yang pernah dilakukan sebelumnya yang berkaitan dengan hasil analisa foto hoax menjadi referensi dalam penulisan penelitian ini yaitu diantaranya:

1. Riadi, dkk (2017) melakukan penelitian dengan judul "*Image Forensic for detecting Splicing Image with Distance Function*". Mengungkapkan untuk menganalisis pengukuran kesamaan gambar forensik menggunakan metode *distance function*, sedangkan untuk manipulasi gambar digunakan *specially on image splicing*. Hasil penelitian ini menunjukkan *distance function* tersebut dapat berupa 2 gambar yang berbeda.
2. Ami D, dkk (2017) melakukan penelitian dengan judul "*Reverse Image Search Image retrieval using various techniques*". Teknik ini berhubungan dengan banyak teknik baru lainnya seperti menangani pengetahuan tersembunyi menggunakan ekstraksi, asosiasi data, menemukan pola tambahan. Disini kita memberikan gambaran umum tentang teknik Image Mining yang muncul dengan berbagai teknik deteksi gambar.

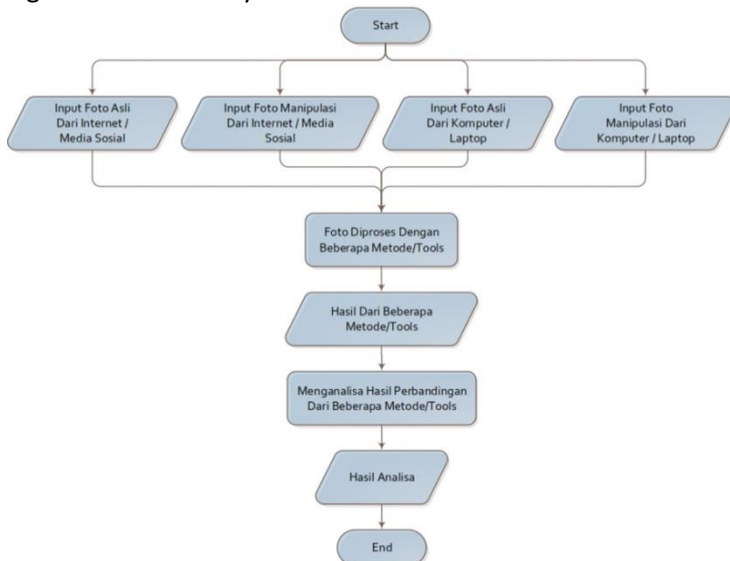
3. Imanda Putra, dkk (2018) melakukan penelitian dengan judul “Analisis Forensik Deteksi Keaslian Metadata Video Menggunakan Exiftool”. Dalam penelitian ini penulis akan menguji menganalisa metadata pada keaslian video dengan menggunakan exiftool. Hasil dari penelitian ini diharapkan dapat menunjukkan informasi perbandingan metadata yang baik.
4. Riadi, dkk (2019) melakukan penelitian dengan judul “Deteksi Pemalsuan Foto Digital Menggunakan Image *Forensics*”. Penelitian ini menggunakan analisa dengan 3 tools *forensics* yaitu *FotoForensics*, *ForensicallyBeta* dan *Opanda IExif*. Hasil yang didapat dari penelitian ini adalah terdeteksinya perbedaan metadata dan perbedaan kontras antara foto asli dan foto manipulasi yang menunjukkan adanya perubahan pada foto tersebut.

Dari beberapa penelitian sebelumnya, pada buku ini akan mengusulkan inovasi dan solusi yang terbaru yaitu terletak pada penggunaan banyak metode untuk penentuan keaslian sebuah informasi yang berupa foto. Buku ini di fokuskan untuk mempermudah orang-orang dalam menganalisa sebuah informasi tersebar secara cepat dan tepat yang dapat membantu penekanan penyebaran sebuah informasi hoax.

METODE PENELITIAN

A. METODE YANG DIGUNAKAN

Adapun tahapan metode buku ini menggunakan sebuah pembuatan metode sendiri untuk melakukan pendeteksian yang digunakan untuk menganalisa foto hoax. Skenario yang dibuat yaitu dengan mengambil sebuah foto di internet atau media sosial dan menyiapkan dua buah foto yang asli dan yang sudah dirubah, setelah itu dimasukkan kedalam metode/tools untuk diproses yang kemudian hasilnya akan dianalisa.



Gambar 1. Flowchart Menganalisa Hasil Foto

Berdasarkan gambar 1 flowchart alur proses menganalisa hasil foto diatas yang akan dibangun secara garis besar terbagi menjadi beberapa tahapan berikut:

1. File Foto

Beberapa file foto yang akan dijadikan sampel yaitu foto-foto yang tersebar di internet / media sosial dan file foto yang tersimpan pada komputer / laptop. Foto yang diambil yang akan dibuat percobaan ini terdiri dari dua jenis yaitu foto asli dan foto yang sudah dimanipulasi.

2. Metode/Tools

Jenis metode/tools yang akan digunakan ada tiga jenis yaitu exif/metadata, reverse image dan image *forensics*. Pertama menggunakan Metode Exif/Metadata yaitu melihat rekaman aktivitas foto. Kedua menggunakan Metode Reverse Image berarti melacak balik, mencocokkan sebuah foto dengan foto yang sudah ada di website dan media sosial. Selanjutnya yang ketiga menggunakan Metode Image *Forensics* yaitu merupakan salah satu metode ilmiah pada bidang penelitian yang bertujuan untuk mendapatkan fakta-fakta pembuktian dalam menentukan sebuah keaslian image.

3. Hasil

Dari beberapa metode/tools yang sudah di uji cobakan, maka akan muncul hasil prosesnya.

4. Analisa Hasil Perbandingan

Hasi-hasil tersebut di analisa untuk mendapatkan sebuah metode/tools yang tepat yang hasilnya mendekati kebenaran.

5. Hasil Analisa

Dari hasil analisa tersebut, maka bisa dipastikan sebuah metode/tools yang sudah bisa digunakan secara tepat dan cepat.

B. FISNBONE DIAGRAM PENELITIAN

Berikut ini adalah fishbone diagram penelitian yang telah disusun oleh penulis dalam melakukan penelitian ini, mulai dari identifikasi masalah, studi literatur, analisa kebutuhan, implementasi dan uji sistem, analisa hasil perbandingan, analisa hasil, penyusunan laporan sampai publikasi jurnal nasional terakreditasi.



Gambar 2. Fishbone Diagram Penelitian

1. Identifikasi Permasalahan

Pada tahapan awal penelitian ini akan merumuskan masalah untuk dijadikan sebagai objek penelitian. Perumusan masalah dilakukan terlebih dahulu melihat situasi di lapangan. Setelah masalah dirumuskan selanjutnya menentukan tujuan penelitian. Tujuan penelitian merupakan sasaran yang ingin di wujudkan dari penyelesaian permasalahan yang diteliti.

2. Studi Literatur

Pada tahapan ini mencari sumber-sumber literatur yang berada di internet yang berhubungan dengan informasi hoax, buku-buku teori dan praktek serta tools yang digunakan dalam penelitian ini, serta dijelaskan mengenai tools yang akan digunakan dalam mendeteksi sebuah informasi hoax yang berupa foto.

3. Analisis Kebutuhan

Analisis kebutuhan yaitu berupa bahan-bahan yang akan dibutuhkan untuk menganalisis sebuah system/tools yang akan di implementasi dan uji coba.

4. Implementasi dan Uji Sistem

Implementasi sistem merupakan proses dimana memastikan sebuah sistem atau tools yang akan diuji bisa menghasilkan kesimpulan dengan baik dan benar.

5. Analisa Hasil Perbandingan

Beberapa metode/tools yang sudah di uji cobakan, maka akan muncul hasil prosesnya. Kemudian hasil-hasil tersebut di analisa untuk mendapatkan sebuah metode/tools yang tepat yang hasilnya mendekati kebenaran.

6. Analisa Hasil

Kesimpulan dari semua hasil yang sudah didapatkan.

7. Penyusunan Laporan

Pada tahapan ini terdapat penyusunan laporan yang memuat semua hasil dari penelitian. Mulai dari latar belakang, tinjauan pustaka, metode penelitian, hasil dan pembahasan sampai pada tahap kesimpulan.

8. Publikasi

Pengiriman artikel ilmiah yang akan di publikasi dalam bentuk jurnal nasional terakreditasi.

C. ANALISA KEBUTUHAN / KEBUTUHAN METODE

Analisa kebutuhan yaitu kebutuhan-kebutuhan yang diperlukan oleh penulis selama melakukan kegiatan penelitian ini yang dapat berupa bahan-bahan yang akan dibutuhkan untuk menganalisis hasil dari metode/tools yang akan di implementasi dan uji sistem. Adapun kebutuhan itu berupa perangkat

keras (pc/laptop), perangkat lunak (tools/*aplication*), tahapan uji coba dan kebutuhan metode untuk mendukung penelitian ini.

1. Kebutuhan Perangkat Keras

Kebutuhan perangkat keras atau *hardware* yang diperlukan oleh penulis selama melakukan kegiatan penelitian ini yang terdiri dari:

- a. Laptop Acer Swift 3
- b. CPU intel Core i5 8 Gen
- c. Memory 12 GB
- d. SSD 256GB dan Hard Disk 1000 GB / 1 TB
- e. Monitor dengan Resolusi 1024 x 600 Pixel
- f. Keyboard dan Mouse
- g. Smartphone Infinix Hot 10

2. Kebutuhan Perangkat Lunak

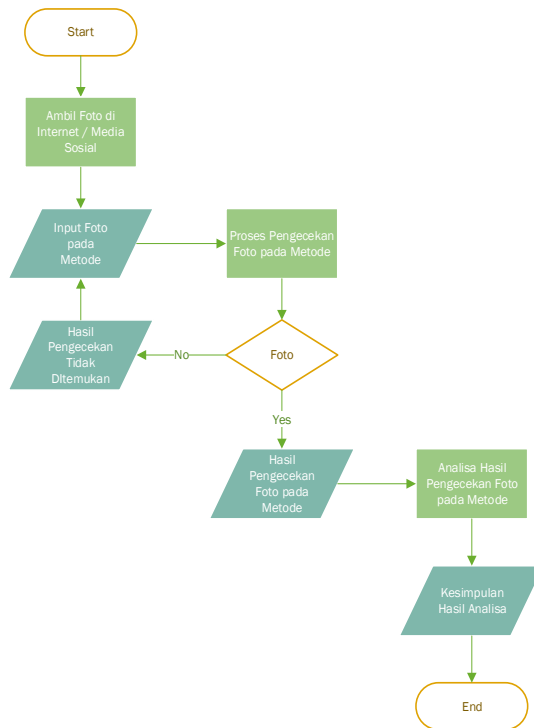
Kebutuhan perangkat lunak atau software yang diperlukan oleh penulis selama melakukan kegiatan penelitian ini yang terdiri dari:

- a. Sistem Operasi Windows 10
- b. Adobe Photoshop CC 2017
- c. Tools Exif/Metadata (Tools *Offline* dan *Online*)
- d. Reverse Image
- e. Image *Forensics*
- f. File Foto-foto

3. Kebutuhan Tahapan Uji Coba

Kebutuhan tahapan uji coba sistem yang diperlukan oleh penulis selama melakukan kegiatan penelitian ini yang terdiri dari:

- a. Fokus kebutuhan yang akan dilakukan dalam penelitian ini adalah mengambil sebuah file foto pada internet / media sosial yang asli dan yang sudah di edit untuk kemudian di analisa dengan ketiga metode (Tools Exif/Metadata, Reverse Image dan Image *Forensics*) dan hasilnya itu akan dibandingkan sesuai dengan kebutuhan permasalahan yang sedang di teliti yaitu foto hoax. Berikut tahapan yang dilakukan pada kebutuhan tahapan uji coba ini dalam bentuk flowchart / alur pengecekan foto:

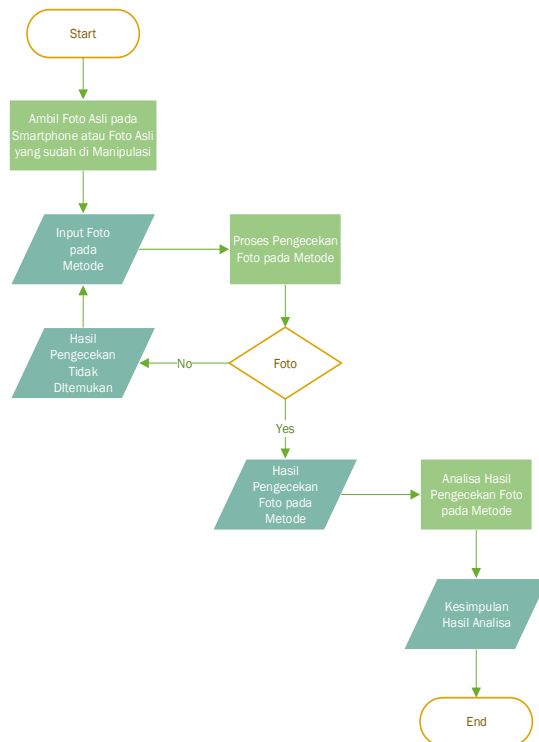


Gambar 3. Flowchart Uji Coba Foto yang diambil dari Internet / Media Sosial

Keterangan gambar 3:

- 1) Proses tahapan kebutuhan ini dimulai
- 2) Pertama yang dilakukan adalah mengambil sampel foto yang ada di internet/media sosial baik yang asli maupun yang sudah di manipulasi
- 3) Setelah itu dilakukan penginputan foto pada beberapa metode yang sudah disiapkan
- 4) Proses pengecekan akan dilakukan dari beberapa metode tersebut, dimana hasil pengecekannya akan ditampilkan kalau sudah berhasil. Namun jika hasilnya belum bisa di tampilkan, maka prosesnya akan di ulangi penginputan foto lagi pada metode tersebut
- 5) Hasil pengecekan yang sudah di tampilkan, akan dianalisa untuk dilakukan perbandingan dari foto asli yang belum di manipulasi dengan foto asli yang sudah di manipulasi
- 6) Akan diambil kesimpulan hasil dari analisa tersebut
- 7) Proses tahapan kebutuhan ini selesai

- b. Kebutuhan selanjutnya yaitu mengambil foto dari kamera Smartphone Infinix Hot 10, foto asli dari kamera tersebut dan yang sudah di manipulasi dengan Adobe Photoshop CC 2017 akan di analisa hasil perbandingannya dengan menggunakan ketiga metode diatas, seperti pada fokus kebutuhan yang pertama. Berikut tahapan yang dilakukan pada kebutuhan tahapan uji coba ini dalam bentuk flowchart / alur pengecekan foto:



Gambar 4. Flowchart Uji Coba Foto yang diambil dari Smartphone/Laptop

Keterangan gambar 4:

- 1) Proses tahapan kebutuhan ini dimulai
- 2) Pertama yang dilakukan adalah mengambil sampel foto yang ada di Smartphone Infinix Hot 10
- 3) Dipersiapkan foto yang asli dan foto yang sama dari foto yang asli namun sudah di manipulasi dengan Photoshop CC 2017
- 4) Setelah itu dilakukan penginputan foto pada beberapa metode yang sudah disiapkan

- 5) Proses pengecekan akan dilakukan dari beberapa metode tersebut, dimana hasil pengecekannya akan ditampilkan kalau sudah berhasil. Namun jika hasilnya belum bisa di tampilkan, maka prosesnya akan di ulangi penginputan foto lagi pada metode tersebut
- 6) Hasil pengecekan yang sudah di tampilkan, akan dianalisa untuk dilakukan perbandingan dari foto asli yang belum di manipulasi dengan foto asli yang sudah di manipulasi
- 7) Akan diambil kesimpulan hasil dari analisa tersebut
- 8) Proses tahapan kebutuhan ini selesai

4. Kebutuhan Metode / Tools

Kebutuhan metode/tools yang diperlukan oleh penulis selama melakukan kegiatan penelitian ini yang terdiri dari:

a. Kebutuhan Metode Tools Exif/Metadata

Teknik pengamanan data dan informasi merupakan salah satu cara untuk menjaga kerahasiaan suatu obyek. *exchangeable Image File Format* (EXIF) Metadata adalah informasi data tentang citra digital. Dalam penyelidikan forensik digital, ini sangat berguna untuk keamanan hak cipta atau pengamanan bukti digital (Wijiyanto, 2018).

Metadata dapat diartikan sebagai deskripsi mendasar tentang suatu data. Metadata merupakan informasi yang dapat mendeskripsikan data yang tertanam dalam suatu data, seperti konten halaman website, dokumen, atau file. Pada file berbentuk foto terdapat EXIF metadata atau Exchangeable Image File merupakan data yang memiliki informasi penting pada sebuah foto (Apriliani, A., Hijjayanti, K., & Suhairoh. 2020).

Citra merupakan sebuah gambar yang merepresentasikan suatu objek. Citra digital merupakan representasi objek yang dapat diolah di dalam perangkat komputer. Citra digital diperoleh dari peralatan digital seperti kamera digital sehingga dapat secara langsung diolah di dalam komputer. Penyebab citra yang dihasilkan dari peralatan digital dapat secara langsung diolah di dalam komputer adalah terdapat sistem sampling dan kuantisasi yang berguna untuk mengubah citra kontinu menjadi digital serta mengubah intensitas analog menjadi intensitas diskrit di dalamnya. Dalam proses sistem sampling dilakukan pembagian citra analog menjadi sejumlah m baris dan kolom sehingga menghasilkan citra digital. Sedangkan dengan melakukan proses sistem kuantisasi akan dihasilkan gradasi warna yang sesuai dengan kebutuhan (P. N. Andono, T. Sutojo och M. , 2017).

Sehingga penyelidikan keaslian citra ini menggunakan Algoritma EXIF Metadata agar informasi yang didapat terstruktur sehingga mendapatkan kesimpulan dari penyelidikan keaslian citra dengan adanya informasi software sebagai alat pemalsuan citra (Apriliani, A., Hijjayanti, K., & Suhairoh. 2020).

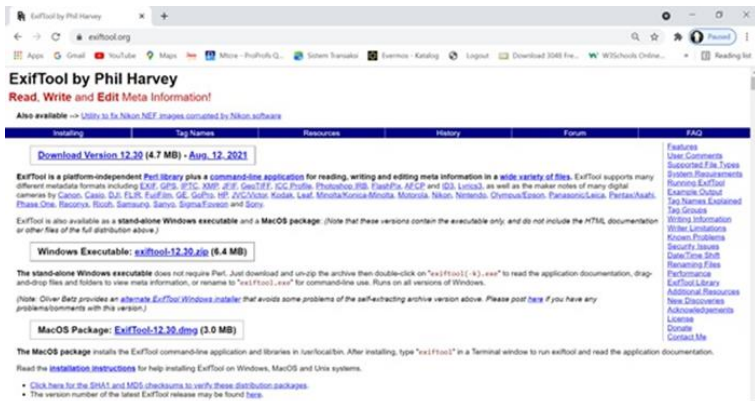
Sebuah foto mengandung informasi yang sangat jelas atau sering disebut dengan metadata file, yaitu identitas suatu file yang ada didalam foto, seperti nama, ukuran, tanggal dibuat, tanggal di edit, extensi sampai nilai hashngnya juga bisa dibaca pada file foto tersebut. Sehingga kalau sudah bisa dipahami tentang metadata foto ini, maka semua orang akan berhati-hati dalam menyebarkan suatu foto, terutama foto yang terkait mendeskritkan pribadi atau kelompok tertentu.

Berikut tools yang dibutuhkan pada metode ini ada 3 jenis yaitu 1 buah tools yang digunakan secara *offline* dan 2 buah tools yang digunakan secara *online*:

1) ExifTool by Phil Harvey (Tools *Offline*)

ExifTool adalah perpustakaan Perl platform-independen ditambah aplikasi baris perintah untuk membaca, menulis dan mengedit informasi meta dalam berbagai macam file. ExifTool mendukung banyak format metadata yang berbeda termasuk EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, Profil ICC, Photoshop IRB, FlashPix, ACP dan ID3, Lyrics3, serta catatan pembuat banyak kamera digital oleh Canon, Casio, DJI, FLIR, FujiFilm, GE, GoPro, HP, JVC/Victor, Kodak, Leaf, Minolta/Konica-Minolta, Motorola, Nikon, Nintendo, Olympus/Epson, Panasonic/Leica, Pentax/Asahi, Fase Satu, Reconyx, Ricoh, Samsung , Sanyo, Sigma/Foveon dan Sony. (Exiftool, 2021)

Exiftool ini sendiri bisa digunakan untuk membaca, menulis dan mengedit informasi metadata file, khususnya file foto. Untuk bisa menggunakan tools ini bisa akses dan download toolsnya secara free di website <https://exiftool.org/>. Berikut adalah tampilan websitenya dan silahkan di download sesuai dengan sistem operasi pc/laptop yang digunakan. Pada percobaan ini digunakan yang versi Windows Executable:



Gambar 5. Tools Exiftool

2) Tools Jeffrey's Image Metadata Viewer (Tools Online)

Tools ini bekerja dengan berbagai macam jenis file ini: 3FR, 3G2, 3GP, 3GP2, 3GPP, A, AA, AAE, AAX, ACFM, ACR, AFM, AI, AIF, AIFC, AIFF, AIT, AMFM, APE, APNG, ARQ, ARW, ASF, AVI, AZW, AZW3, BMP, BPG, BTIF, CHM, CIFF, COS, CR2, CR3, CRM, CRW, CS1, DC3, DCM, DCP, DCR, DFONT, DIB, DIC, DICM, DIVX, DJV, DJVU, DLL, DNG, DOC, DOCM, DOCX, DOT, DOTM, DOTX, DPX, DR4, DS2, DSS, DV, DVB, DVR-MS, DYLIB, EIP, EPS, EPS2, EPS3, EPSF, EPUB, ERF, EXE, EXIF, EXR, EXV, F4A, F4B, F4P, F4V, FFF, FLA, FLAC, FLIF, FLIR, FLV, FPF, FPX, GIF, GPR, GZ, GZIP, HDP, HDR, HEIC, HEIF, HTM, HTML, ICAL, ICC, ICM, ICS, IDML, IIQ, IND, INDD, INDT, INX, ISO, ITC, J2C, J2K, JNG, JP2, JPC, JPE, JPEG, JPF, JPG, JPM, JPX, JSON, JXR, K25, KDC, KUNCI, KTH, LA, LFP, LFR, LNK, M2T, M2TS, M2V, M4A, M4B, M4P, M4V, MAX, MEF, MIE, MIF, MIFF, MKA, MKS, MKV, MNG, MOBI, MODD, MOI, MOS, MOV, MP3, MP4, MPC, MPEG, MPG, MPO, MQV, MRW, MTS, MXF, NEF, BARU, NMBTEMPLATE, NRW, ANGKA, O, ODB, ODC, ODF, ODG, ODI, ODP, ODS, ODT, OFR, OGG, OGV, OPUS, ORF, OTF, PAC, PAGES, PB M, PCD, PCT, PDB, PDF, PEF, PFA, PFB, PFM, PGF, PGM, PICT, PLIST, PMP, PNG, POT, POTM, POTX, PPM, PPS, PPSM, PPSX, PPT, PPTM, PPTX, RRC, PS, PS2, PS3, PSB, PSD, PSDT, PSP, PSPFRAME, PSPIMAGE, PSPSHAPE, PSPTUBE, QIF, QT, QTI, QTIF, R3D, RA, RAF, RAM, RAR, RAW, RIF, RIFF, RM, RMVB, RPM, RSRC, RTF, RV, RW2, RWL, RWZ, SEQ, SKETSA, SO, SR2, SRF, SRW, SVG, SWF, THM, THMX, TIF, TIFF, TORRENT, TS, TTC, TTF, TUB, VCARD, VCF, VOB, VRD, VSD, WAV, WDP, WEBM, WEBP, WMA, WMV, WTV, WV, X3F, XCF, XHTML, XLA, XLAM, XLS, XLSB, XLSM, XLSX, XLT, XLTM, XLTX, XMP, dan ZIP (Jeffrey's Image Metadata Viewer, 2021).

Banyak sekali jenis file yang bisa dibaca metadata informasinya dengan menggunakan tools *online* ini. Untuk bisa menggunakan tools ini bisa akses dan digunakan secara *online* di website <http://exif.regex.info/exif.cgi>. Berikut

adalah tampilan websitenya dan pada percobaan ini langsung digunakan secara *online*:

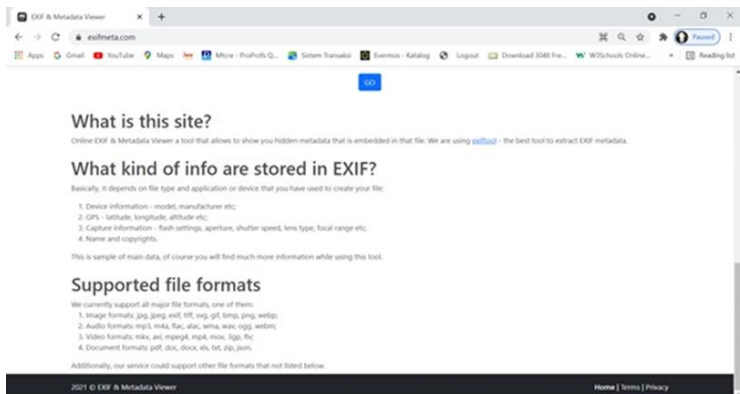


Gambar 6. Tools Jeffrey's Image Metadata Viewer

3) EXIF & Metadata Viewer (Tools Online)

EXIF & Metadata Viewer Online ini adalah tools yang memungkinkan untuk menampilkan metadata tersembunyi yang disematkan didalam *file* itu. Menggunakan Exiftool Online merupakan tools terbaik untuk mengekstrak metadata EXIF (Exif & Metadata Viewer, 2021).

Berbagai macam jenis file yang bisa dibaca informasi metadatanya dengan menggunakan tools *online* ini. Untuk bisa menggunakan tools ini bisa akses dan digunakan secara *online* di website <https://exifmeta.com/>. Berikut adalah tampilan websitenya dan pada percobaan ini langsung digunakan secara *online*:



Gambar 7. Tools EXIF & Metadata Viewer

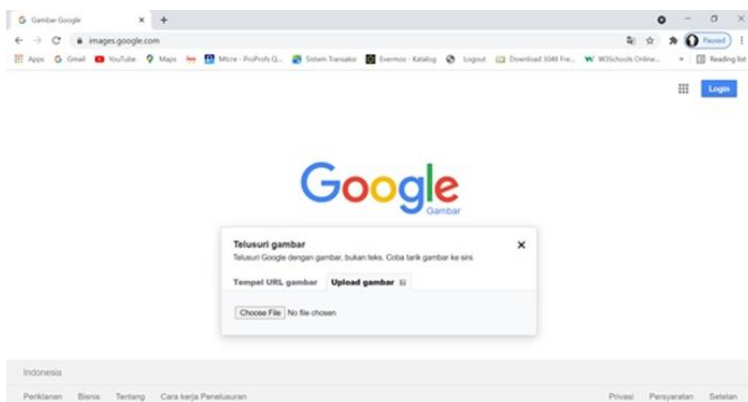
b. Menggunakan Metode Reverse Image

Reverse image adalah salah satu teknik yang berhubungan dengan banyak teknik baru lainnya seperti menangani pengetahuan tersembunyi menggunakan ekstraksi, asosiasi data, menemukan pola tambahan (Adrakatti, 2016).

Pengambilan foto pada internet/media sosial sangat menarik dan disebarkan lagi, sehingga banyak orang yang tidak mengetahui siapa pemilik asli dari foto tersebut. Seperti untuk apa foto itu dibuat dan digunakan untuk kebutuhan apa saja, orang-orang hanya menyebarkan tanpa punya kepentingan yang jelas dan tanpa mengetahui resiko dari penyebaran foto tersebut. Padahal kalau diselidiki lebih dalam lagi, foto itu sudah ada atau belum ada yang tersebar di dunia internet / media sosial dan informasi apa saja yang terkandung didalamnya, bisa menggunakan salah satu metode ini. Salah satu tools yang digunakan pada metode Reverse Image ini adalah menggunakan Google Images.

Google images adalah layanan pencarian yang dibuat oleh Google dan diperkenalkan pada bulan Juli 2001. Layanan ini memungkinkan pengguna mencari konten gambar di web. Kata kunci pencarian gambar didasarkan pada nama berkas gambar, teks tautan yang mengacu ke gambar, dan teks di dekat gambar (Google Images, 2021).

Untuk menggunakan tools ini silahkan akses websitenya di <https://images.google.com/> dan masuk pada menu upload gambar. Tampilan websitenya seperti pada gambar dibawah ini:



Gambar 8. Tools Reverse Image dengan Google Images

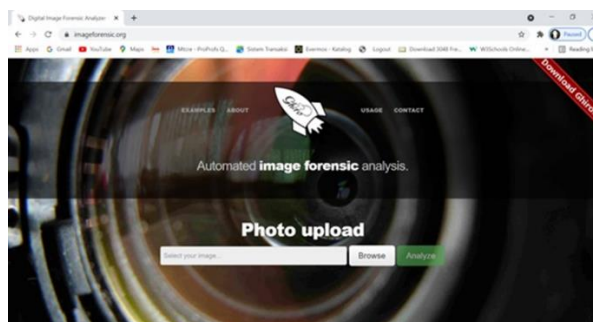
c. Menggunakan Metode Image Forensic

Bidang ilmu forensik citra digital akan membantu para penegak hukum, intelijen, investigasi swasta dan media. Semakin majunya teknologi image pada saat ini mengangkat isu-isu baru dan tantangan dalam menentukan keaslian image. Forensik citra digital merupakan salah satu metode ilmiah pada bidang penelitian yang bertujuan untuk mendapatkan fakta-fakta pembuktian dalam menentukan keaslian image (Yuli Sulisty, Riadi, & Yudhana, 2018).

Dampak negatif yang terjadi akibat mudahnya informasi menyebar salah satunya yaitu informasi dapat dengan mudahnya di manipulasi, salah satunya adalah informasi berbentuk foto yang telah direkayasa atau edit. Untuk mencegah hal tersebut dapat dilakukan analisis ke foto tersebut dengan image forensic. Dengan bantuan tools image forensic seperti Jpegsnoop bisa melihat metadata dari foto tersebut sehingga kita dapat dengan mudah mencari tahu sumber foto tersebut, dan dengan Forensically bisa dilakukan analysis dengan metode Error level analysis untuk melihat objek yang direkayasa (Rizky Al-Fajri, Caruddin & Yusup, 2021).

Salah satu cara yang valid digunakan untuk mengecek keaslian foto itu bisa digunakan dengan menggunakan image forensic. Metode image forensic merupakan salah satu cara dalam pemeriksaan bukti digital yang digunakan didalam sebuah persidangan. Pemeriksaan hasil image forensics bisa digunakan sebagai barang bukti yang berhubungan dengan bukti digital dan ini diakui oleh persidangan. Meskipun ada banyak alat untuk melakukan investigasi forensik pada gambar, mereka tidak memiliki fitur dan umumnya bermasalah. Situs ini dimaksudkan untuk mengatasi masalah ini dan menawarkan layanan yang stabil dan andal untuk penyelidikan forensik dan profesional keamanan (Imageforensic, 2021).

Untuk menggunakan tools ini silahkan akses websitenya di <https://www.imageforensic.org/> dan silahkan browser gambar yang ingin di analisa. Tampilan websitenya seperti pada gambar dibawah ini:



Gambar 9. Tools Image Forensic



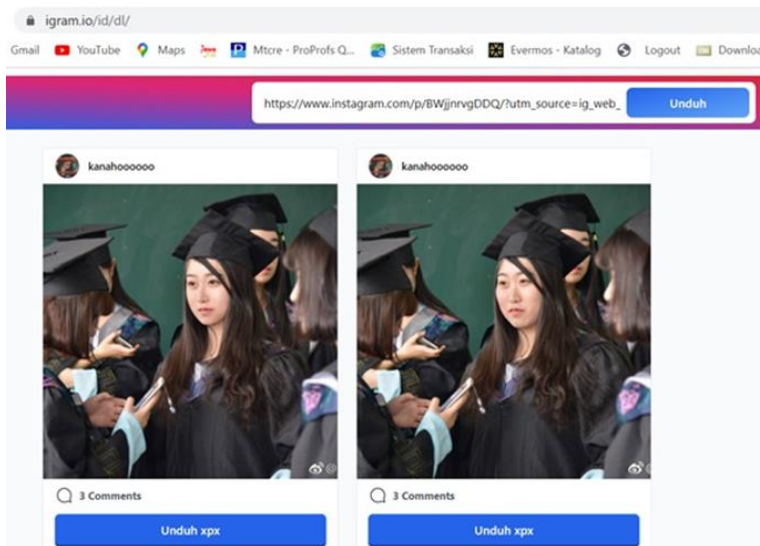
PEMBAHASAN HASIL PENELITIAN

A. IMPLEMENTASI DAN UJI SISTEM

Implementasi dan uji sistem merupakan proses dimana memastikan sebuah sistem atau tools yang akan diuji bisa menghasilkan kesimpulan yang sesuai dengan apa yang akan diharapkan, terutama dalam penelitian ini. Adapun tahapan implementasi dan uji sistem dilakukan dengan 2 jenis bukti foto yang sudah di persiapkan sebagai sampel dengan masing-masing menggunakan 3 metode yang telah dijelaskan pada analisa kebutuhan sebelumnya.

1. Bukti Foto dari Internet/Media Sosial

Sebelum melakukan implementasi dan uji sistem, terlebih dahulu mengambil sampel foto yang ada di Internet/Media Sosial. Foto yang diambil ada 2 jenis yaitu foto asli dan foto manipulasi. Kedua foto tersebut akan di uji coba pada tahap implementasi dan uji sistem ini. Foto diambil dari akun instagram @kanahooooo dengan link url <https://www.instagram.com/p/BWjjnrvGDDQ/> dan di download dengan bantuan link url <https://igram.io/id/dl/> dengan tampilan fotonya seperti gambar berikut:



Gambar 10. Sampel Foto Asli dan Manipulasi

File foto yang sudah di download berikut tampilan Name, Date Modified, Type dan Size jika dibuka pada PC/Laptop OS Windows 10.

View			
PC > Downloads			
Name	Date modified	Type	Size
Today (4)			
19985689_116897472268112_9054493905596186624_n.jpg	16/09/2021 13:01	JPG File	787 KB
19985654_489612018045740_4996359537318428672_n.jpg	16/09/2021 13:01	JPG File	797 KB

Gambar 11. Tampilan Informasi Foto

Keterangan gambar 11:

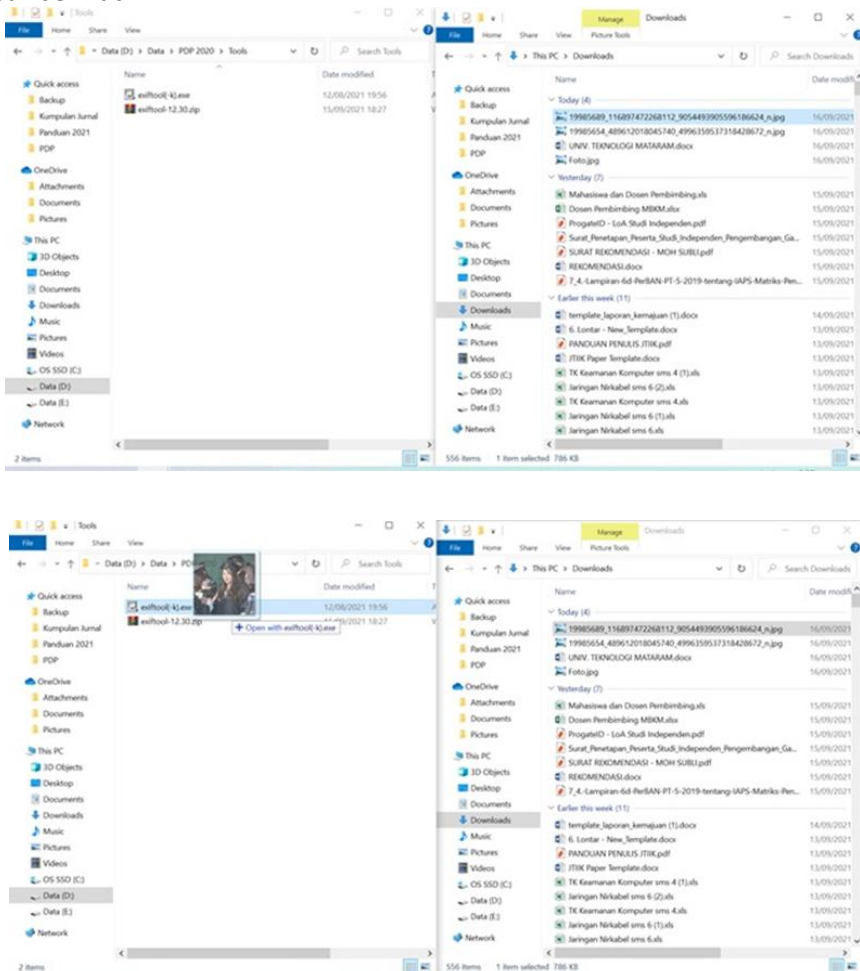
- 1) Foto asli dari internet/media sosial instagram @kanahoooooo
- 2) Dengan nama: 19985689_116897472268112_9054493905596186624_n.jpg (nama asli dari internet/media sosial tanpa dirubah kembali di pc/laptop)
- 3) Foto manipulasi dari internet/media sosial instagram @kanahoooooo
- 4) Dengan nama: 19985654_489612018045740_4996359537318428672_n.jpg (nama asli dari internet/media sosial tanpa dirubah kembali di pc/laptop)

Berikut implementasi dan uji sistem bukti foto ini dilakukan dengan menggunakan 3 metode/tools:

a. Metode Tools Exif/Metadata

1) ExifTool by Phil Harvey (Tools Offline)

Setelah selesai download Exiftool, selanjutnya dilakukan extract pada file rar/zip dan jalankan toolsnya dengan cara drag and drop file foto, seperti gambar berikut:



Gambar 12. Proses Drag and Drop File Foto pada Exiftool

Kemudian hasilnya akan muncul pada gambar 12 dan gambar 13 berikut:

```
ExifTool Version Number      : 12.30
File Name                    : 19980509_116897472268112_0054493905596186624_n.jpg
Directory                     : D:/Back Up/Downloads
File Size                     : 786 KiB
File Modification Date/Time   : 2021:09:16 13:01:55+07:00
File Access Date/Time        : 2021:09:16 13:38:25+07:00
File Creation Date/Time      : 2021:09:16 13:01:51+07:00
File Permissions              : -rwxrwxrwx-
File Type                     : JPEG
File Type Extension           : .jpg
MIME Type                     : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                   : 1
Y Resolution                   : 1
Current IPTC Digest           : 6804fa61419d410499053c009e0cc01
Special Instructions           : F80D2300096F0200001da0000ba23003004df05000430070000000002c4509000d0b00000cc2f0a0095490c00
Image Width                   : 1080
Image Height                  : 1080
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample               : 8
Color Components               : 3
Y Cb Cr Sub Sampling          : YCbCr4:4:4 (1 1)
Image Size                   : 1080x1080
Megapixels                    : 1.2
-- press ENTER --
```

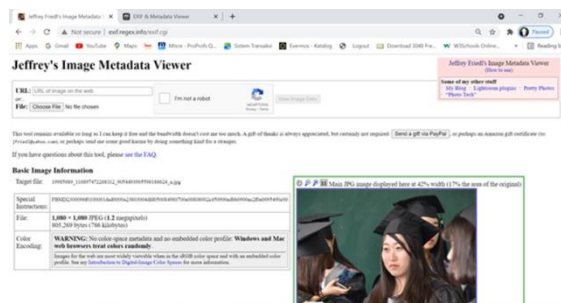
Gambar 13. Hasil Proses Exif/Metadata Foto Asli

```
ExifTool Version Number      : 12.30
File Name                    : 19980509_116897472268112_0054493905596186627_n.jpg
Directory                     : D:/Back Up/Downloads
File Size                     : 796 KiB
File Modification Date/Time   : 2021:09:16 13:01:20+07:00
File Access Date/Time        : 2021:09:16 13:39:40+07:00
File Creation Date/Time      : 2021:09:16 13:01:12+07:00
File Permissions              : -rwxrwxrwx-
File Type                     : JPEG
File Type Extension           : .jpg
MIME Type                     : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                   : 1
Y Resolution                   : 1
Current IPTC Digest           : 1af20b0f0c96f7b72f0b580ab243f0baa
Special Instructions           : F80D2300096F02000099af0000134b0300ff2f060041b0070072230800b15b090078d20900f0480a0072700c00
Image Width                   : 1080
Image Height                  : 1080
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample               : 8
Color Components               : 3
Y Cb Cr Sub Sampling          : YCbCr4:4:4 (1 1)
Image Size                   : 1080x1080
Megapixels                    : 1.2
-- press ENTER --
```

Gambar 14. Hasil Proses Exif/Metadata Foto Manipulasi

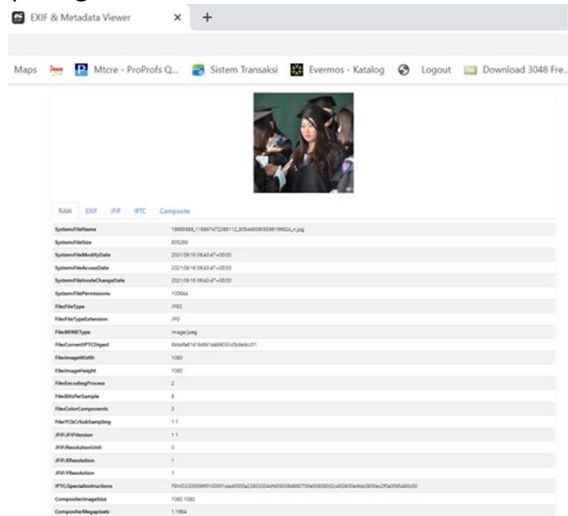
2) Tools Jeffrey's Image Metadata Viewer (Tools Online)

Uji coba tools ini harus terkoneksi internet, dan internet tidak boleh terputus selama melakukan proses uji coba tools ini. Caranya langsung saja akses link url <http://exif.regex.info/exif.cgi> kemudian *upload file* foto yang akan dianalisa dengan tampilan hasil proses pengecekannya seperti gambar berikut:



3) EXIF & Metadata Viewer (Tools Online)

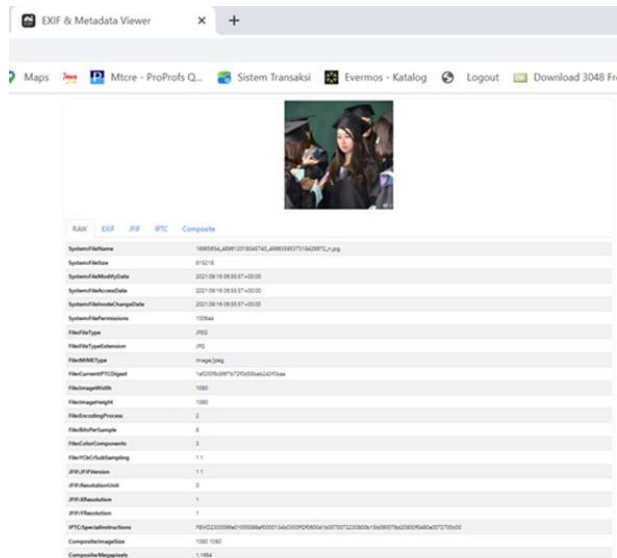
Sama seperti point b diatas, untuk uji coba tools ini harus terkoneksi internet juga, dan internet tidak boleh terputus selama melakukan proses uji coba tools ini. Caranya langsung saja akses link url <https://exifmeta.com/> kemudian *upload file* foto yang akan dianalisa dengan tampilan hasil proses pengecekannya seperti gambar berikut:



The screenshot shows the EXIF & Metadata Viewer interface with a photo of a woman in a graduation cap. The metadata table below the photo lists various EXIF data points.

RAW	EXIF	JPEG	IFD	Composite
System.FileName 18885854_1888747228171_C354483003818854_C.jpg				
System.FileSize 816216				
System.FileModifyDate 2021:08:16 08:42:47+00:00				
System.FileCreateDate 2021:08:16 08:42:47+00:00				
System.FileChangeDate 2021:08:16 08:42:47+00:00				
System.FilePermissions 100644				
File.FileName JPEG				
File.FileType JPEG				
File.FileTypeExtension .jpg				
File.FileNameType Image/JPEG				
File.FileNameOriginalImage 18885854_1888747228171_C354483003818854_C.jpg				
File.ImageWidth 1080				
File.ImageHeight 1080				
File.EncodingProcess 2				
File.ColorProfile 8				
File.ColorComponents 3				
File.FileColorSampling 1:1				
JPEG.JPEGVersion 1.1				
JPEG.ExifVersion 0				
JPEG.ExifThumbnail 1				
JPEG.ExifThumbnail 1				
IFD.ExifThumbnail 18885854_1888747228171_C354483003818854_C.jpg				
Composite.ImageWidth 1080 1080				
Composite.ImageHeight 1080 1080				

Gambar 17. Hasil Proses EXIF & Metadata Viewer Foto Asli



The screenshot shows the EXIF & Metadata Viewer interface with a manipulated photo of a woman in a graduation cap. The metadata table below the photo lists various EXIF data points.

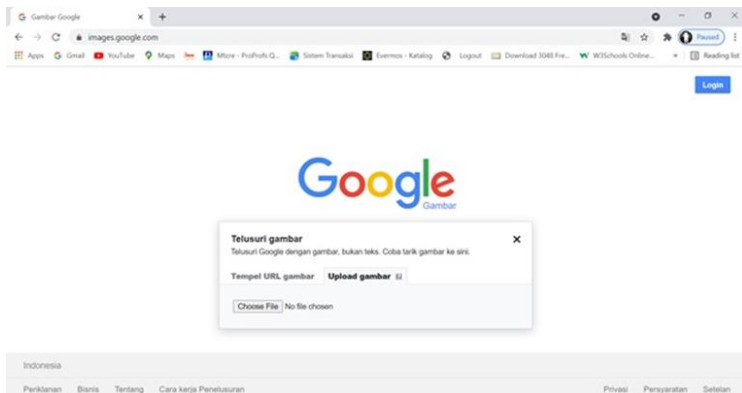
RAW	EXIF	JPEG	IFD	Composite
System.FileName 18885854_1888747228171_C354483003818854_C.jpg				
System.FileSize 816216				
System.FileModifyDate 2021:08:16 08:42:47+00:00				
System.FileCreateDate 2021:08:16 08:42:47+00:00				
System.FileChangeDate 2021:08:16 08:42:47+00:00				
System.FilePermissions 100644				
File.FileName JPEG				
File.FileType JPEG				
File.FileTypeExtension .jpg				
File.FileNameType Image/JPEG				
File.FileNameOriginalImage 18885854_1888747228171_C354483003818854_C.jpg				
File.ImageWidth 1080				
File.ImageHeight 1080				
File.EncodingProcess 2				
File.ColorProfile 8				
File.FileColorSampling 1:1				
JPEG.JPEGVersion 1.1				
JPEG.ExifVersion 0				
JPEG.ExifThumbnail 1				
JPEG.ExifThumbnail 1				
IFD.ExifThumbnail 18885854_1888747228171_C354483003818854_C.jpg				
Composite.ImageWidth 1080 1080				
Composite.ImageHeight 1080 1080				

Gambar 18. Hasil Proses EXIF & Metadata Viewer Foto Manipulasi

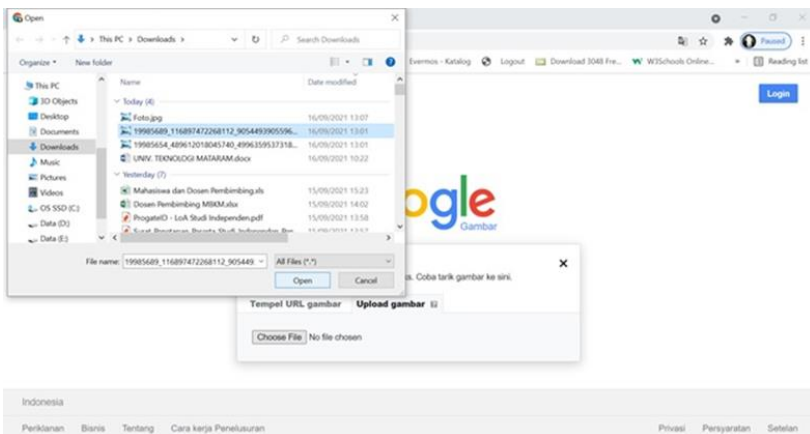
b. Metode Reverse Image

Metode ini dilakukan dengan mencocokkan dan mencari foto yang sama dari berbagai sumber link/situs yang sudah mempunyai file foto tersebut.

Langkah yang dilakukan sama seperti point 2) dan 3) diatas, untuk uji coba tools ini harus terkoneksi internet juga, dan internet tidak boleh terputus selama melakukan poroses uji coba tools ini. Caranya langsung saja akses link url <https://images.google.com/> kemudian upload file foto yang akan dianalisa dengan tampilan hasil proses pengecekannya seperti gambar-gambar berikut:

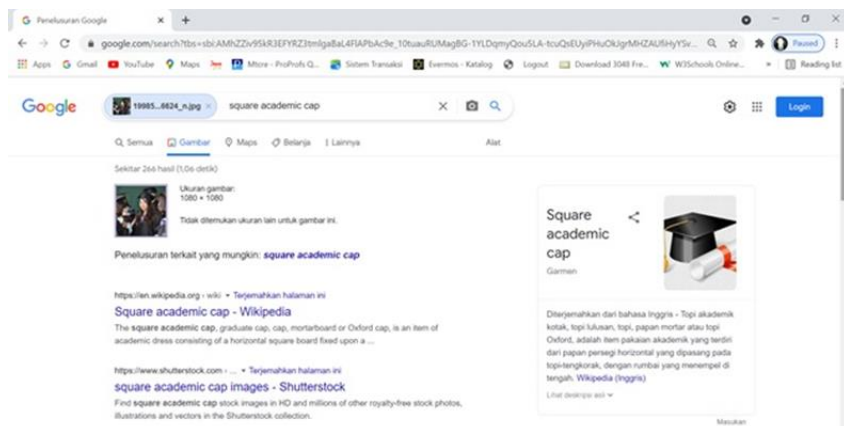


Gambar 19. Proses Upload Foto pada Metode Reverse Image

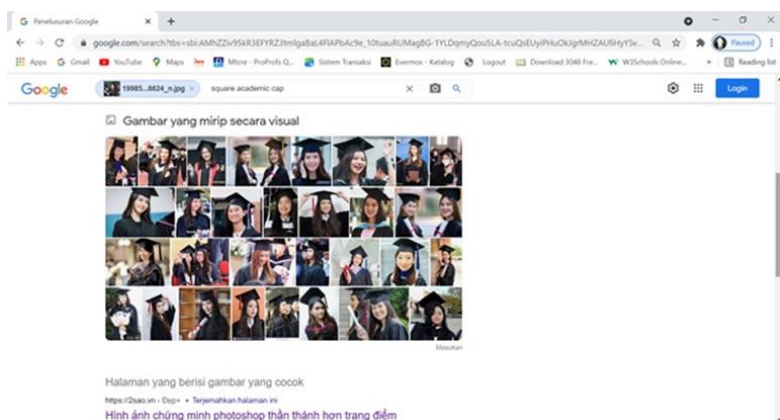


Gambar 20. Pilih Foto yang akan di upload pada Metode Reverse Image

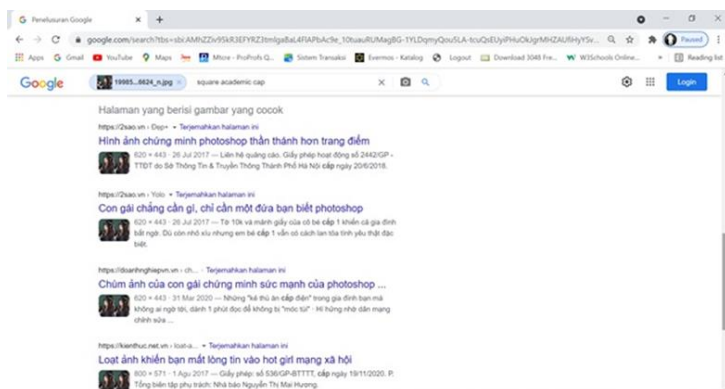
Disini di *upload* salah satu dari foto asli dan foto manipulasi, karena hasilnya akan melakukan pengecekan yang sama terhadap kedua foto tersebut. Berikut hasil penelusurannya seperti gambar-gambar berikut:



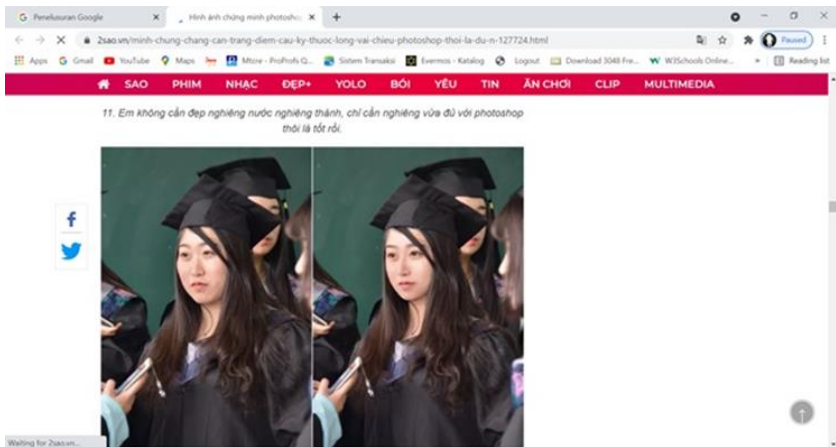
Gambar 21. Tampilan yang paling menonjol pada sebuah foto



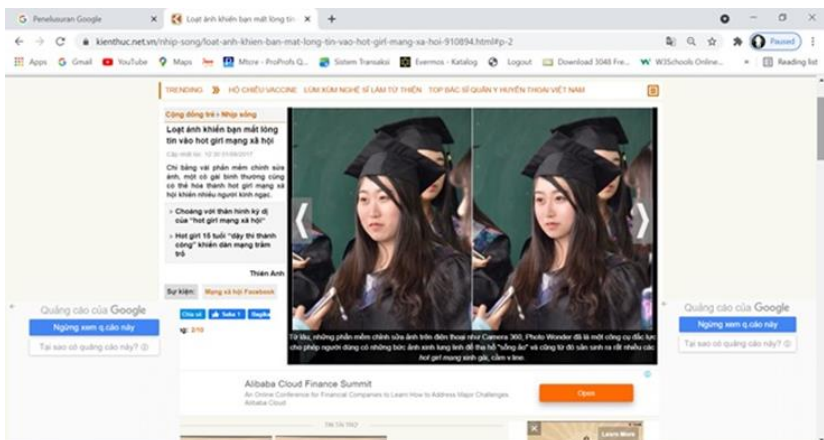
Gambar 22. Gambar yang serupa dengan foto



Gambar 23. Situs penyedia yang serupa dengan foto



Gambar 24. Contoh situs penyedia yang serupa dengan foto



Gambar 25. Contoh situs penyedia yang serupa dengan foto

c. Metode Image Forensic

Metode ini dilakukan dengan melihat semua informasi metada yang terkandung pada sebuah foto. Langkah yang dilakukan sama seperti point b , 2) dan 3) diatas, karena untuk melakukan uji coba metode ini sendiri harus terkoneksi internet juga, dan internet tidak boleh terputus selama melakukan proses uji coba metode ini. Caranya langsung saja akses link url <https://www.imageforensic.org/> kemudian *upload file* foto yang akan dianalisa dengan tampilan hasil proses pengecekannya seperti gambar berikut:

Image analysis: 50fbee4b8ed08cd8f312986dfdf356be
Submitted at: Sept. 16, 2021, 7:26 a.m.

Dashboard **Static** IPTC ELA

Static info File Type **Hashes**

Type	Value
SHA1	b259eccc3da1884e98f240cd25e0cc787a3d552
SHA224	8980c5e0cfd140c565eb594add1270e2705122af8aba0cb47f
SHA384	0f1a74899181332538963c2864d3c377967638cc18ba36f166a16f584ae38373193afaf5071d53c3a3c13033
CRC32	8623C236
SHA256	c90c1e5a539438e55480a1949cc04eac5ec94592d5339c2a6bcb13ab6a28a
SHA512	10448508690c2205e271867e56277c3c29da7ac0b84726279472b6c3cc3ac0c07569b61d7ec90e5058431185a451a15704001c2bdc35ab09a85c9af020
MD5	50fbee4b8ed08cd8f312986dfdf356be

Image analysis: 50fbee4b8ed08cd8f312986dfdf356be
Submitted at: Sept. 16, 2021, 7:26 a.m.

Dashboard **Static** IPTC ELA

Static info **File Type** Hashes

Type	Value
JPEG image data, JFIF standard 1.01	

Analyzed by imageforensic.org ver. 0.2
© 2012-2021 jekid and burkone

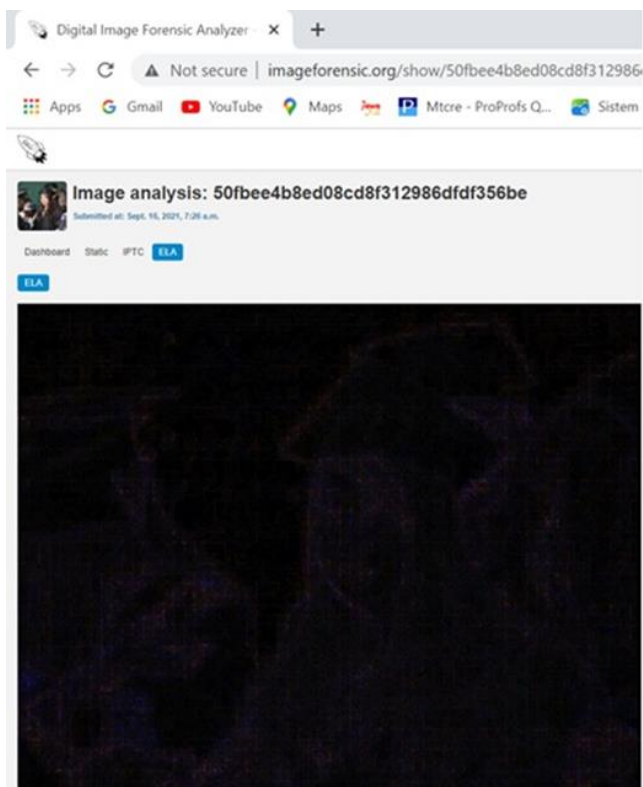
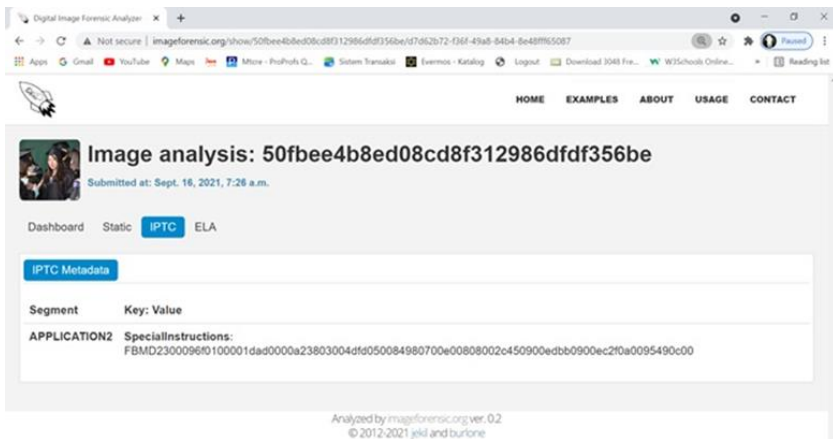
Image analysis: 50fbee4b8ed08cd8f312986dfdf356be
Submitted at: Sept. 16, 2021, 7:26 a.m.

Dashboard **Static** IPTC ELA

Static info File Type Hashes

Type	Value
Dimensions	[1080, 1080]
Analyzed at	Sept. 16, 2021, 7:26 a.m.

Analyzed by imageforensic.org ver. 0.2
© 2012-2021 jekid and burkone



Gambar 2.8 Hasil Pengecekan Foto Asli

Digital Image Forensic Analyzer

Not secure | imageforensic.org/show/55635b6a2bfeabcb89d3a8359746acca/0fb5766b-ed5e-4cef-85b6-fc48c9c97f6c

HOME EXAMPLES ABOUT USAGE CONTACT

Image analysis: 65635b6a2bfeabcb89d3a8359746acca

Submitted at: Sept. 16, 2021, 7:32 a.m.

Dashboard Static IPTC ELA

Analysis results (tagged as private)

Type	Result
Static analysis	Static data
EXIF metadata extraction	No EXIF metadata
IPTC metadata extraction	IPTC Metadata
XMP metadata extraction	No XMP metadata
Preview extraction from metadata	No Preview
Localization	No GPS data
Error Level Analysis (ELA)	Applicable
Signature check	No signature match

Digital Image Forensic Analyzer

Not secure | imageforensic.org/show/55635b6a2bfeabcb89d3a8359746acca/0fb5766b-ed5e-4cef-85b6-fc48c9c97f6c

HOME EXAMPLES ABOUT USAGE CONTACT

Image analysis: 65635b6a2bfeabcb89d3a8359746acca

Submitted at: Sept. 16, 2021, 7:32 a.m.

Dashboard Static IPTC ELA

Static info File Type Hashes

Type	Value
Dimensions	[1080, 1080]
Analyzed at	Sept. 16, 2021, 7:32 a.m.

Analyzed by imageforensic.org ver. 0.2
© 2012-2021 jsl and burton

Digital Image Forensic Analyzer

Not secure | imageforensic.org/show/55635b6a2bfeabcb89d3a8359746acca/0fb5766b-ed5e-4cef-85b6-fc48c9c97f6c

HOME EXAMPLES ABOUT USAGE CONTACT

Image analysis: 65635b6a2bfeabcb89d3a8359746acca

Submitted at: Sept. 16, 2021, 7:32 a.m.

Dashboard Static IPTC ELA

Static info File Type Hashes

Type
JPEG image data, JFIF standard 1.01

Analyzed by imageforensic.org ver. 0.2
© 2012-2021 jsl and burton

Digital Image Forensic Analyzer x +

Not secure | imageforensic.org/show/65635b6a2bfeabcb89d3a8359746acca/0b5766b-ed5e-4cef-85d6-fc48c9c9796c

HOME EXAMPLES ABOUT USAGE CONTACT

Image analysis: 65635b6a2bfeabcb89d3a8359746acca

Submitted at: Sept. 16, 2021, 7:32 a.m.

Dashboard Static IPTC ELA

Static info File Type Hashes

Type	Value
SHA1	820c76b89879a0e5115045a7a0565b16c310ca1
SHA224	03aa70517281d841d1145db1de097707e95098d2572d7040e73e5
SHA384	a5321e7a2085020572aed258055045262a1cc0c8777bba274f372785f84db3715784927de1d07ed0ab76a68647
CRC32	1CB18134
SHA256	1c145d3a8b8ec2e6ed85556d5c2b27a63ca1e02bd7b6f9e93414a9d9ae92d
SHA512	d2783e773aa35a8f8ca4dbaf0e27658415d8aed89ec38b9e957442ee77e74ca9e0521e218900fa09526275fawc404cc0bd506f16710c1ac1a259e1cd91d
MD5	65635b6a2bfeabcb89d3a8359746acca

Digital Image Forensic Analyzer x +

Not secure | imageforensic.org/show/65635b6a2bfeabcb89d3a8359746acca/0b5766b-ed5e-4cef-85d6-fc48c9c9796c

HOME EXAMPLES ABOUT USAGE CONTACT

Image analysis: 65635b6a2bfeabcb89d3a8359746acca

Submitted at: Sept. 16, 2021, 7:32 a.m.

Dashboard Static IPTC ELA

IPTC Metadata

Segment	Key: Value
APPLICATION2	SpecialInstructions: FBMD2300099e01000099a0000134b0300f2f060041b0070072230800b15b090078d20900f0480a0072700c00

Digital Image Forensic Analyzer x +

Not secure | imageforensic.org/show/65635b6a2bfeabcb89d3a8359746acca

HOME EXAMPLES ABOUT USAGE CONTACT

Image analysis: 65635b6a2bfeabcb89d3a8359746acca

Submitted at: Sept. 16, 2021, 7:32 a.m.

Dashboard Static IPTC ELA

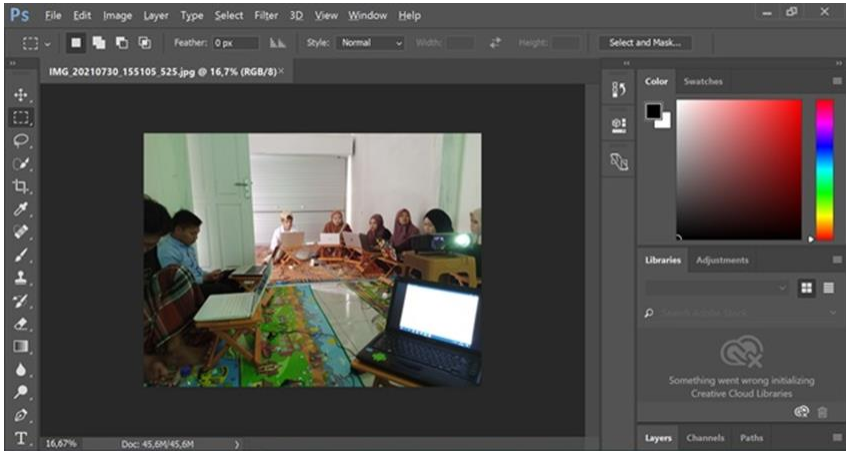
ELA



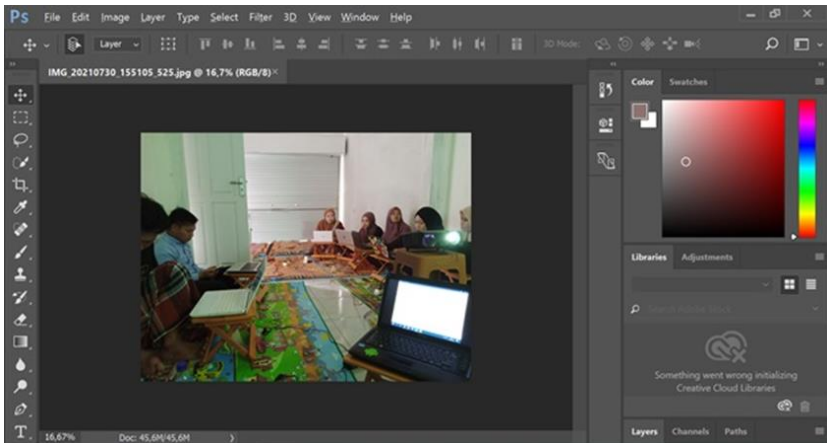
Gambar 29. Hasil Pengecekan Foto Manipulasi

2. Bukti Foto dari Smartphone/Laptop

Sebelum melakukan implementasi dan uji sistem, terlebih dahulu mengambil sampel foto yang ada di Smartphone Infinix Hot 10 kemudian di masukkan kedalam PC/Laptop. Foto yang akan di uji coba pada implementasi ini ada 2 jenis yaitu foto asli dan foto manipulasi dengan menghilangkan salah satu objek (orang) pada foto asli yang sudah di edit dengan Photoshop CC 2017. Tampilan fotonya seperti gambar berikut:



Gambar 30. Foto asli yang yang di edit dengan aplikasi photoshop



Gambar 31. Foto manipulasi yang sudah di edit dengan aplikasi photoshop



Gambar 32. Foto Asli



Gambar 33. Foto Manipulasi

Implementasi dan uji sistem bukti foto ini dilakukan dengan menggunakan 3 metode/tools, yang sebelumnya harus diperhatikan adalah langkah-langkahnya sama seperti point 1 diatas. Berikut yang ditampilkan adalah hasil pengecekan dari masing-masing metode:

a. Metode Tools Exif/Metadata

1) ExifTool by Phil Harvey (Tools Offline)

```

Select D:\Data\PDP 2020\Tools\exiftool(-k).exe
ExifTool Version Number      : 12.30
File Name                    : IMG_20210730_155105_525.jpg
Directory                   : D:\Data\PDP 2020\Tools\File Foto/Foto Sebelum Edit
File Size                    : 4.6 MiB
File Modification Date/Time  : 2021:07:30 15:51:05+07:00
File Access Date/Time       : 2021:09:16 20:48:13+07:00
File Creation Date/Time     : 2021:09:16 19:40:45+07:00
File Permissions             : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Image Description            :
Make                         : INFINIX MOBILITY LIMITED
Camera Model Name            : Infinix X682C
Orientation                  : Horizontal (normal)
X Resolution                  : 72
Y Resolution                  : 72
Resolution Unit               : inches
Software                     : MediaTek Camera Application
Modify Date                  : 2021:07:30 15:51:05
Y Cb Cr Positioning          : Co-sited
Exposure Time                 : 1/20
F Number                     : 1.9
Exposure Program              : Not Defined
ISO                           : 963
Exif Version                  : 0220
Date/Time Original            : 2021:07:30 15:51:05
Create Date                   : 2021:07:30 15:51:05
Offset Time                   : +08:00
Offset Time Original          : +08:00
Offset Time Digitized         : +08:00
Components Configuration     : Y, Cb, Cr, -
Exposure Compensation         : 0
Metering Mode                 : Center-weighted average
Light Source                  : Other
Flash                        : No Flash
Focal Length                  : 3.6 mm
Sub Sec Time                  : 46
Sub Sec Time Original         : 46
  
```

```

Select D:\Data\PD\ 2020\Tools\exiftool-kj.exe
Flashpix Version      : 0100
Color Space           : sRGB
Exif Image Width      : 4608
Exif Image Height     : 3456
Interoperability Index : R98 - DCF basic file (sRGB)
Interoperability Version : 0100
Exposure Mode         : Auto
White Balance         : Auto
Digital Zoom Ratio     : 1
Focal Length In 35mm Format : 0 mm
Scene Capture Type     : Standard
Compression           : JPEG (old-style)
Thumbnail Offset       : 1408
Thumbnail Length       : 49792
Image Width           : 4608
Image Height          : 3456
Encoding Process       : Baseline DCT, Huffman coding
Bits Per Sample        : 8
Color Components       : 3
Y Cb Cr Sub Sampling  : YCbCr4:2:0 (2 2)
Aperture              : 1.9
Image Size            : 4608x3456
Megapixels            : 15.9
Shutter Speed         : 1/20
Create Date           : 2021:07:30 15:51:05.46+08:00
Date/Time Original     : 2021:07:30 15:51:05.46+08:00
Modify Date           : 2021:07:30 15:51:05.46+08:00
Thumbnail Image        : (Binary data 49792 bytes, use -b option to extract)
Focal Length          : 3.6 mm
Light Value           : 2.8
-- press ENTER --

```

Gambar 34. Hasil Metode ExifTool by Phil Harvey dari Foto Asli

```

D:\Data\PD\ 2020\Tools\exiftool-kj.exe
ExifTool Version Number : 12.30
File Name                : IMG_20210730_155105_525.jpg
Directory                : D:\Data\PD\ 2020\Tools\File Foto\Foto Sudah Edit
File Size                : 4.6 MiB
File Modification Date/Time : 2021:09:16 20:29:49+07:00
File Access Date/Time     : 2021:09:16 20:51:59+07:00
File Creation Date/Time   : 2021:09:16 20:29:48+07:00
File Permissions          : -rw-rw-rw-
File Type                : JPEG
File Type Extension       : jpg
MIME Type                : image/jpeg
Exif Byte Order           : Little-endian (Intel, II)
Photometric Interpretation : RGB
Make                    : INFINIX MOBILITY LIMITED
Camera Model Name        : Infinix X682C
Orientation              : Horizontal (normal)
Samples Per Pixel        : 3
X Resolution             : 72
Y Resolution             : 72
Resolution Unit          : inches
Software                 : Adobe Photoshop CC 2017 (Windows)
Modify Date              : 2021:09:16 20:28:40
Y Cb Cr Positioning      : Co-sited
Exposure Time            : 1/20
F Number                 : 1.9
Exposure Program         : Not Defined
ISO                      : 963
Exif Version             : 0220
Date/Time Original       : 2021:07:30 15:51:05
Create Date              : 2021:07:30 15:51:05
Offset Time              : +08:00
Offset Time Original     : +08:00
Offset Time Digitized    : +08:00
Components Configuration : Y, Cb, Cr, -
Shutter Speed Value      : 1/20
Aperture Value           : 1.9
Exposure Compensation    : 0
Metering Mode            : Center-weighted average
Light Source              : Other
Flash                   : No Flash

```

```

D:\Data\POP 2020\tools\exiftool-kj.exe
Focal Length          : 3.6 mm
Sub Sec Time         : 46
Sub Sec Time Original : 46
Sub Sec Time Digitized : 46
Flashpix Version      : 0100
Color Space           : sRGB
Exif Image Width      : 4608
Exif Image Height     : 3456
Interoperability Index : 000 - DCF basic file (sRGB)
Interoperability Version : 0100
Exposure Mode         : Auto
White Balance         : Auto
Digital Zoom Ratio     : 1
Focal Length In 35mm Format : 0 mm
Scene Capture Type     : Standard
Compression           : JPEG (old-style)
Thumbnail Offset       : 1074
Thumbnail Length       : 6166
Current IPTC Digest    : eccb96e268c94f6924ab14edb385fdb
Coded Character Set    : UTF8
Application Record Version : 0
Time Created           : 15:51:05+00:00
IPTC Digest            : eccb96e268c94f6924ab14edb385fdb
Displayed Units X      : inches
Displayed Units Y      : inches
Print Style            : Centered
Print Position         : 0 0
Print Scale            : 1
Global Angle           : 30
Global Altitude        : 30
URL List               :
Slices Group Name      : IMG_20210730_155105_525
Num Slices             : 1
Pixel Aspect Ratio     : 1
Photoshop Thumbnail    : (Binary data 6166 bytes, use -b option to extract)
Has Real Merged Data   : Yes
Writer Name            : Adobe Photoshop
Reader Name            : Adobe Photoshop CC 2017
Photoshop Quality       : 11
Photoshop Format        : Standard

```

```

D:\Data\POP 2020\tools\exiftool-kj.exe
Progressive Scans      : 3 Scans
XMP Toolkit            : Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01
Creator Tool           : MediaTek Camera Application
Metadata Date          : 2021:09:16 20:28:40+07:00
Date Created           : 2021:07:30 15:51:05.046
Color Mode             : RGB
ICC Profile Name       : sRGB IEC61966-2.1
Document ID            : adobe:docid:photoshop:80c72cc1-16f1-11ec-b19f-b94362b428d5
Instance ID            : xmp.iid:df2d9f60-533b-1f4f-a99f-c9ed14b1e4b0
Original Document ID   : 00B8D50E9636C747BC469862739F05F1
Format                 : image/jpeg
History Action          : saved, saved
History Instance ID     : xmp.iid:37ecd01-4c70-974e-885f-f2c8327cc23d, xmp.iid:df2d9f60-533b-1f4f-a99f-c9ed14b1e4b0
History When           : 2021:09:16 20:26:24+07:00, 2021:09:16 20:28:40+07:00
History Software Agent  : Adobe Photoshop CC 2017 (Windows), Adobe Photoshop CC 2017 (Windows)
History Changed        : /, /
Profile CMYK Type       : Linotronic
Profile Version         : 2.1.0
Profile Class           : Display Device Profile
Color Space Data        : RGB
Profile Connection Space : XYZ
Profile Date Time       : 1998:02:09 06:49:00
Profile File Signature  : acsp
Primary Platform        : Microsoft Corporation
CMYK Flags              : Not Embedded, Independent
Device Manufacturer     : Hewlett-Packard
Device Model            : sRGB
Device Attributes       : Reflective, Glossy, Positive, Color
Rendering Intent         : Perceptual
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator          : Hewlett-Packard
Profile ID              : 0
Profile Copyright       : Copyright (c) 1998 Hewlett-Packard Company
Profile Description      : sRGB IEC61966-2.1
Media White Point        : 0.95045 1 1.08905
Media Black Point        : 0 0 0
Red Matrix Column        : 0.43607 0.22249 0.01392
Green Matrix Column      : 0.38515 0.71687 0.09708
Blue Matrix Column       : 0.14307 0.06061 0.7141

```

```

Select D:\Data\PDF 2020\Tools\exiftool-kj.exe
Green Matrix Column : 0.38515 0.71687 0.09708
Blue Matrix Column : 0.14307 0.06061 0.7141
Device Mfg Desc : IEC http://www.iec.ch
Device Model Desc : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc : Reference Viewing Condition in IEC61966-2.1
Viewing Cond Illuminant : 19.6445 20.3718 16.8089
Viewing Cond Surround : 3.92889 4.07439 3.36179
Viewing Cond Illuminant Type : D50
Luminance : 76.03647 80 87.12462
Measurement Observer : CIE 1931
Measurement Backing : 0 0 0
Measurement Geometry : Unknown
Measurement Flare : 0.999%
Measurement Illuminant : D65
Technology : Cathode Ray Tube Display
Red Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
Blue Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)
DCT Encode Version : 100
APP14 Flags 0 : [14]
APP14 Flags 1 : (none)
Color Transform : YCbCr
Image Width : 4608
Image Height : 3456
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)
Aperture : 1.9
Image Size : 4608x3456
Megapixels : 15.9
Shutter Speed : 1/20
Create Date : 2021:07:30 15:51:05.46+08:00
Date/Time Original : 2021:07:30 15:51:05.46+08:00
Modify Date : 2021:09:16 20:28:40.46+08:00
Thumbnail Image : (Binary data 6166 bytes, use -b option to extract)
Date/Time Created : 2021:07:30 15:51:05+00:00
Focal Length : 3.6 mm
Light Value : 2.8
-- press ENTER --

```

Gambar 35. Hasil Metode ExifTool by Phil Harvey dari Foto Manipulasi

2) Tools Jeffrey's Image Metadata Viewer (Tools Online)

The screenshot shows the 'Jeffrey's Image Metadata Viewer' website. The browser address bar shows 'exif.regex.info/ief/view'. The page title is 'Jeffrey's Image Metadata Viewer'. Below the title, there is a form to enter a URL or upload a file. The 'File' section shows 'D:\Data\PDF 2020\Tools\exiftool-kj.exe'. The 'Basic Image Information' section displays the following details:

- Target File: D:\Data\PDF 2020\Tools\exiftool-kj.exe
- Camera: Sanyo MOBILE LIMITED Sanyo MOBILE
- Lens: 3.6 mm
- Exposure: Auto exposure, Not Deflated, 1/20 sec, F1.85, ISO 963
- Flash: auto
- Date: July 30, 2021 15:51:05 (timezone not specified)
- File: 4,608 x 3,456 JPEG (15.9 megabytes)
- Color Encoding: WARNING: Color space tagged as sRGB, without an embedded color profile. Windows and Mac browsers and apps treat the colors as sRGB.

On the right side, there is a thumbnail image of a group of people sitting around a table, possibly in a meeting or classroom setting.

Exif Image Size	4,608 x 3,456
Image Description	
Make	INFINIX MOBILITY LIMITED
Camera Model Name	Infelix X60C
Software	MediaDR Camera Application
Modify Date	2021:07:30 17:51 (0)
	1 month, 17 days, 17 hours, 9 minutes, 9 seconds ago
Exif:0x0220 ← 0x0224	0 (0 items)
Exif:0x0222	
Exposure Time	1/20
F Number	1.85
Exposure Program	Not Defined
ISO	800
Exif Version	0220
Date Time Original	2021:07:30 17:51 (0)
	1 month, 17 days, 17 hours, 9 minutes, 9 seconds ago
Centre Date	2021:07:30 17:51 (0)
	1 month, 17 days, 17 hours, 9 minutes, 9 seconds ago
Offset Time	+08:00
Offset Time Original	+08:00
Offset Time Digitized	+08:00
Components Configuration	Y, Cb, Cr, -
Exposure Compensation	0
Metering Mode	Centre-weighted average
Light Source	Other

Flash	No Flash
Flash Length	0.0 mm
Sub Sec Time	40
Sub Sec Time Original	40
Sub Sec Time Digitized	40
Flashpix Version	0100
Color Space	sRGB
Interoperability Index	R98 - DCF basic file (v2.0)
Interoperability Version	0100
Exposure Mode	Auto
White Balance	Auto
Digital Zoom Ratio	1
Flash Length In 35mm Format	0 mm
Scene Capture Type	Standard
Compression	JPEG (old-style)
Orientation	Horizontal (normal)
Resolution	72 pixels/inch
Thumbnail Length	40762
YCbCr Processing	Co-sited
Thumbnail Image	(40762 bytes binary data)

File -- basic information derived from the file	
File Type	JPEG
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)

Bits Per Sample	8
Color Components	3
File Size	4.6 MB
File Type Extension	.jpg
Image Size	4,608 x 3,456
YCbCr Sub-Sampling	YCbCr4:2:0 (12:12:12)

Composite	
This block of data is computed based upon other items. Some of it may be wildly incorrect, especially if the image has been resized.	
Aperture	1.85
Megapixels	12.9
Shutter Speed	1/20
Centre Date	2021:07:30 17:51 (0) 40-08:00
	1 month, 17 days, 17 hours, 9 minutes, 9 seconds ago
Date Time Original	2021:07:30 17:51 (0) 40-08:00
	1 month, 17 days, 17 hours, 9 minutes, 9 seconds ago
Modify Date	2021:07:30 17:51 (0) 40-08:00
	1 month, 17 days, 17 hours, 9 minutes, 9 seconds ago
Flash Length	0.0 mm
Light Value	2.8

Exiftool	
Warning	[warning] Unkown APPS segment
Warning	[warning] Unkown APPS segment
Warning	[warning] Unkown APPS segment
Warning	[warning] Unkown APPS segment

Gambar 36. Hasil Tools Jeffrey's Image Metadata Viewer dari Foto Asli

Jeffrey Fried's Image Metadata Viewer

URL (URL of image on the web):
 File: [Choose File] No file chosen

☐ I'm not a robot

This tool remains available as long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. [Send a gift via PayPal] or perhaps via Amazon gift certificate (see: [privacy/faq.html](#)), or perhaps via some good karma by doing something kind for a stranger.

If you have questions about this tool, please see the [FAQ](#).

Basic Image Information

Target File:	D:\2021\76_111111_111.jpg
Camera:	Samsung M0651 LIMITED Edition S06C
Lens:	1.8 mm
Exposure:	Auto exposure, Not Default, 1/20 sec, F1.85, ISO 961
Flash:	on
Date:	July 26, 2021 1:51:11 PM (timezone not specified)
File:	4,408 x 3,446 JPEG (15.9 megapixels)
Color:	4,798,304 bytes (4.6 megabytes)
Color:	Embedded color profile: "sRGB"

Display image in window, which has been set to show thumbnails

Display image in window, which has been set to show thumbnails

Jeffrey Fried's Image Metadata Viewer

URL (URL of image on the web):
 File: [Choose File] No file chosen

☐ I'm not a robot

This tool remains available as long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. [Send a gift via PayPal] or perhaps via Amazon gift certificate (see: [privacy/faq.html](#)), or perhaps via some good karma by doing something kind for a stranger.

If you have questions about this tool, please see the [FAQ](#).

XMP

Date Created	2021-07-26 15:51:11 (UTC)
XMP Toolkit	Adobe XMP Core 3.0-c1311 79.139824, 2016-09-14-01-09-01
Creator Tool	Adobe Photoshop (Mac OS)
Modify Date	2021-09-14 20:28:40-07:00
Metadata Date	2021-09-14 20:28:40-07:00
Color Mode	RGB
ICC Profile Name	sRGB IEC61966-2.1
Document ID	adobe:docid:photoshop:00000000000000000000000000000000
Instance ID	adobe:docid:photoshop:00000000000000000000000000000000
Original Document ID	adobe:docid:photoshop:00000000000000000000000000000000
Process	Image (img)
History Actions	saved
History Instance ID	adobe:docid:photoshop:00000000000000000000000000000000
History When	2021-09-14 20:28:40-07:00
History Software Agent	Adobe Photoshop CC 2017 (Windows)
History Changed	1

Jeffrey Fried's Image Metadata Viewer

URL (URL of image on the web):
 File: [Choose File] No file chosen

☐ I'm not a robot

This tool remains available as long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. [Send a gift via PayPal] or perhaps via Amazon gift certificate (see: [privacy/faq.html](#)), or perhaps via some good karma by doing something kind for a stranger.

If you have questions about this tool, please see the [FAQ](#).

EXIF

Bits Per Sample	8 8 8
Photometric Interpretation	RGB
Make	INFINITUM MOBILE LIMITED
Camera Model Name	Infiniti M06C
Orientation	Horizontal (normal)
Samples Per Pixel	3
Software	Adobe Photoshop CC 2017 (Windows)
YCbCr Positioning	Co-sited
Exif Image ID	0x00224
Exif Image ID	0x00224
Exposure Time	1/20
F Number	1.85
Exposure Program	Not Default
ISO	961
Exif Version	0220
Date Time Original	2021-07-26 15:51:11 (UTC)
Offset Time	+08:00
Offset Time Original	+08:00
Offset Time Digitized	+08:00
Components Configuration	Y, Cb, Cr, -
Shutter Speed Value	1/20
Aperture Value	1.80
Exposure Compensation	0

Jeffrey Fried's Image Metadata - EXIF & Metadata Viewer

Not secure | exif.regex.info/exif.cgi

Apps Gmail YouTube Maps More - ProPhoto G. Sistem Transaksi Etermos - Katalog Logout Download 3048 Fre... W3Schools Online... Reading list

IFTC

Colored Character Set	UTF8
Application Based Version	0
Date Created	2021-07-30 1 month, 17 days, 7 hours, 7 minutes, 47 seconds ago
Time Created	15:51:00+00:00

File

Basic information derived from the file

File Type	JPEG
File Type Extension	.jpg
MIME Type	image/jpeg
Endianness	Little-endian (Intel, ID)
Bits Per Sample	8
Current IPTC Digest	ccccc0000000000000000000000000000
Coloring Process	Baseline DCT, Huffman coding
Color Components	3
File Size	4.6 KB
Image Size	4,000 x 3,456
Y-Ch-Cr Sub-Sampling	YCbCr4:4:4 (1:1:1)

Composite

This block of data is composed based upon other items. Some of it may be wildly incorrect, especially if the image has been resized.

Aperture	1.85
Date/Time Created	2021-07-30 15:51:01+00:00 1 month, 18 days, 17 hours, 14 minutes, 37 seconds ago

Jeffrey Fried's Image Metadata - EXIF & Metadata Viewer

Not secure | exif.regex.info/exif.cgi

Apps Gmail YouTube Maps More - ProPhoto G. Sistem Transaksi Etermos - Katalog Logout Download 3048 Fre... W3Schools Online... Reading list

EXIF

File Size	4.6 KB
Image Size	4,000 x 3,456
Y-Ch-Cr Sub-Sampling	YCbCr4:4:4 (1:1:1)

Composite

This block of data is composed based upon other items. Some of it may be wildly incorrect, especially if the image has been resized.

Aperture	1.85
Date/Time Created	2021-07-30 15:51:01+00:00 1 month, 18 days, 17 hours, 14 minutes, 37 seconds ago
Megapixels	13.9
Shutter Speed	1/20
Create Date	2021-07-30 15:51:01+00:00 1 month, 17 days, 4 hours, 14 minutes, 37 seconds ago
Date/Time Original	2021-07-30 15:51:01+00:00 1 month, 17 days, 4 hours, 14 minutes, 37 seconds ago
Modify Date	2021-09-14 20:28:41+00:00 1 hour, 17 minutes ago
Focal Length	3.6 mm
Light Value	2.8

ICC_Profile

This block of data describes the color space used to render pixel colors.

[\[click to show profile data \]](#)

This application uses Phil Harvey's open-source Image::ExifTool library, version 11.11. Harigunapala created with ImageMagick.
 Before use modified this version on Feb 12, 2021.
 Photos and data derived with this service are not shared with anyone else, nor are they stored beyond the temporary period needed for the service to function.

Gambar 37. Hasil Tools Jeffrey's Image Metadata Viewer dari Foto Manipulasi

3) EXIF & Metadata Viewer (Tools Online)

Jeffrey Fried's Image Metadata - EXIF & Metadata Viewer

Not secure | exifmeta.com

Apps Gmail YouTube Maps More - ProPhoto G. Sistem Transaksi Etermos - Katalog Logout Download 3048 Fre... W3Schools Online... Reading list



EXIF

System.FileName	840_8510738_10108_525.jpg
System.FileSize	401630
System.FileModifyDate	2021/09/16 13:58:02+0000
System.FileAccessDate	2021/09/16 13:58:02+0000
System.FileCreateDate	2021/09/16 13:58:02+0000
System.FilePermissions	100644
File.FileType	JPEG
File.FileTypeExtension	.jpg
File.MIMEType	image/jpeg
File.ExifByteOrder	1
File.ImageWidth	4000
File.ImageHeight	3456
File.EncodingProcess	0

File:RawSample	8
File:ColorComponents	3
File:YCbCrSubsampling	2,2
File:ImageDescription	
File:Make	APRIMA MOBILITY LIMITED
File:Model	Index W54C
File:Orientation	1
File:XResolution	72
File:YResolution	72
File:XResolutionUnit	2
File:YResolutionUnit	2
File:Software	Module Camera Application
File:ModifyDate	2021:07:30 15:51:05
File:YCbCrPositioning	2
File:ExposureTime	0.048987
File:FNumber	1.85
File:ExposureProgram	9
File:ISO	960
File:ExposureIndex	6200
File:Date/TimeOriginal	2021:07:30 15:51:05
File:Date/TimeRawOriginal	2021:07:30 15:51:05
File:ColorProfile	+v200
File:ColorProfileName	+v2000
File:ColorProfileVersion	+v2000
File:ColorProfileDescription	+v2000
File:ColorProfileManufacturer	+v2000
File:ColorProfileCopyright	+v2000
File:ColorProfileConfiguration	1.2.0.0

File:RawSample	8
File:ColorComponents	3
File:YCbCrSubsampling	2,2
File:ImageDescription	
File:Make	APRIMA MOBILITY LIMITED
File:Model	Index W54C
File:Orientation	1
File:XResolution	72
File:YResolution	72
File:XResolutionUnit	2
File:YResolutionUnit	2
File:Software	Module Camera Application
File:ModifyDate	2021:07:30 15:51:05
File:YCbCrPositioning	2
File:ExposureTime	0.048987
File:FNumber	1.85
File:ExposureProgram	9
File:ISO	960
File:ExposureIndex	6200
File:Date/TimeOriginal	2021:07:30 15:51:05
File:Date/TimeRawOriginal	2021:07:30 15:51:05
File:ColorProfile	+v200
File:ColorProfileName	+v2000
File:ColorProfileVersion	+v2000
File:ColorProfileDescription	+v2000
File:ColorProfileManufacturer	+v2000
File:ColorProfileCopyright	+v2000
File:ColorProfileConfiguration	1.2.0.0

File:RawSample	8
File:ColorComponents	3
File:YCbCrSubsampling	2,2
File:ImageDescription	
File:Make	APRIMA MOBILITY LIMITED
File:Model	Index W54C
File:Orientation	1
File:XResolution	72
File:YResolution	72
File:XResolutionUnit	2
File:YResolutionUnit	2
File:Software	Module Camera Application
File:ModifyDate	2021:07:30 15:51:05
File:YCbCrPositioning	2
File:ExposureTime	0.048987
File:FNumber	1.85
File:ExposureProgram	9
File:ISO	960
File:ExposureIndex	6200
File:Date/TimeOriginal	2021:07:30 15:51:05
File:Date/TimeRawOriginal	2021:07:30 15:51:05
File:ColorProfile	+v200
File:ColorProfileName	+v2000
File:ColorProfileVersion	+v2000
File:ColorProfileDescription	+v2000
File:ColorProfileManufacturer	+v2000
File:ColorProfileCopyright	+v2000
File:ColorProfileConfiguration	1.2.0.0

Gambar 38. Hasil EXIF & Metadata Viewer dari Foto Asli

File:RawSample	8
File:ColorComponents	3
File:YCbCrSubsampling	2,2
File:ImageDescription	
File:Make	APRIMA MOBILITY LIMITED
File:Model	Index W54C
File:Orientation	1
File:XResolution	72
File:YResolution	72
File:XResolutionUnit	2
File:YResolutionUnit	2
File:Software	Module Camera Application
File:ModifyDate	2021:07:30 15:51:05
File:YCbCrPositioning	2
File:ExposureTime	0.048987
File:FNumber	1.85
File:ExposureProgram	9
File:ISO	960
File:ExposureIndex	6200
File:Date/TimeOriginal	2021:07:30 15:51:05
File:Date/TimeRawOriginal	2021:07:30 15:51:05
File:ColorProfile	+v200
File:ColorProfileName	+v2000
File:ColorProfileVersion	+v2000
File:ColorProfileDescription	+v2000
File:ColorProfileManufacturer	+v2000
File:ColorProfileCopyright	+v2000
File:ColorProfileConfiguration	1.2.0.0

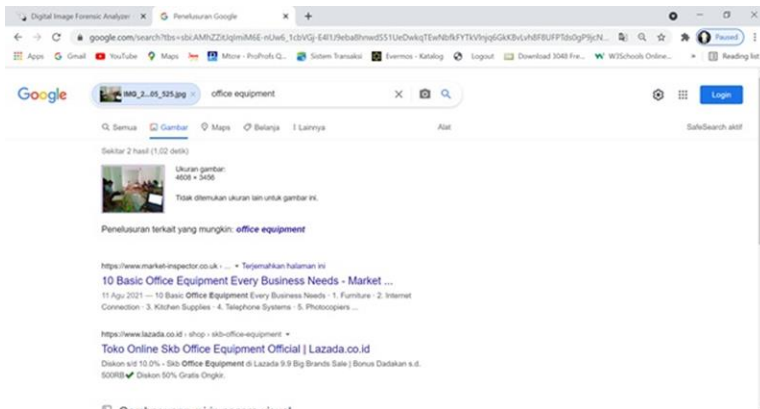
File:RawSample	8
File:ColorComponents	3
File:YCbCrSubsampling	2,2
File:ImageDescription	
File:Make	APRIMA MOBILITY LIMITED
File:Model	Index W54C
File:Orientation	1
File:XResolution	72
File:YResolution	72
File:XResolutionUnit	2
File:YResolutionUnit	2
File:Software	Module Camera Application
File:ModifyDate	2021:07:30 15:51:05
File:YCbCrPositioning	2
File:ExposureTime	0.048987
File:FNumber	1.85
File:ExposureProgram	9
File:ISO	960
File:ExposureIndex	6200
File:Date/TimeOriginal	2021:07:30 15:51:05
File:Date/TimeRawOriginal	2021:07:30 15:51:05
File:ColorProfile	+v200
File:ColorProfileName	+v2000
File:ColorProfileVersion	+v2000
File:ColorProfileDescription	+v2000
File:ColorProfileManufacturer	+v2000
File:ColorProfileCopyright	+v2000
File:ColorProfileConfiguration	1.2.0.0

File:RawSample	8
File:ColorComponents	3
File:YCbCrSubsampling	2,2
File:ImageDescription	
File:Make	APRIMA MOBILITY LIMITED
File:Model	Index W54C
File:Orientation	1
File:XResolution	72
File:YResolution	72
File:XResolutionUnit	2
File:YResolutionUnit	2
File:Software	Module Camera Application
File:ModifyDate	2021:07:30 15:51:05
File:YCbCrPositioning	2
File:ExposureTime	0.048987
File:FNumber	1.85
File:ExposureProgram	9
File:ISO	960
File:ExposureIndex	6200
File:Date/TimeOriginal	2021:07:30 15:51:05
File:Date/TimeRawOriginal	2021:07:30 15:51:05
File:ColorProfile	+v200
File:ColorProfileName	+v2000
File:ColorProfileVersion	+v2000
File:ColorProfileDescription	+v2000
File:ColorProfileManufacturer	+v2000
File:ColorProfileCopyright	+v2000
File:ColorProfileConfiguration	1.2.0.0

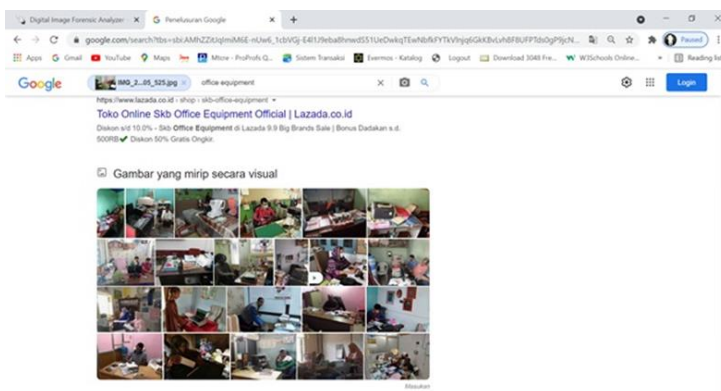
ICC_ProfileBaseTIC	(Binary data 2862 bytes, use -b option to extract)
KC-viewViewingConditions	15.040, 20.3714, 16.039
KC-viewViewingConditions	3.5089, 4.0749, 3.36179
KC-viewViewingConditionsType	1
KC-measMeasurementDimension	1
KC-measMeasurementDuration	0.0.0
KC-measMeasurementDuration	0
KC-measMeasurementDuration	0.0000
KC-measMeasurementDuration	2
Adobe DCTransformVersion	150
Adobe APPIFTag	16384
Adobe APPIFTag	0
Adobe Color Management	1
Composite Aperture	1.85
Composite ImageSize	4008 3436
Composite ImageSize	15.51248
Composite ShutterSpeed	0.040007
Composite SubDataCreationDate	2021:07:10 15:11:05.46+08:00
Composite SubDataCreationDate	2021:07:10 15:11:05.46+08:00
Composite SubDataCreationDate	2021:07:10 20:28:40.46+08:00
Composite SubDataCreationDate	2021:07:10 15:11:05+08:00
Composite SubDataCreationDate	280
Composite SubDataCreationDate	2.8267624020121

Gambar 39. Hasil EXIF & Metadata Viewer dari Foto Manipulasi

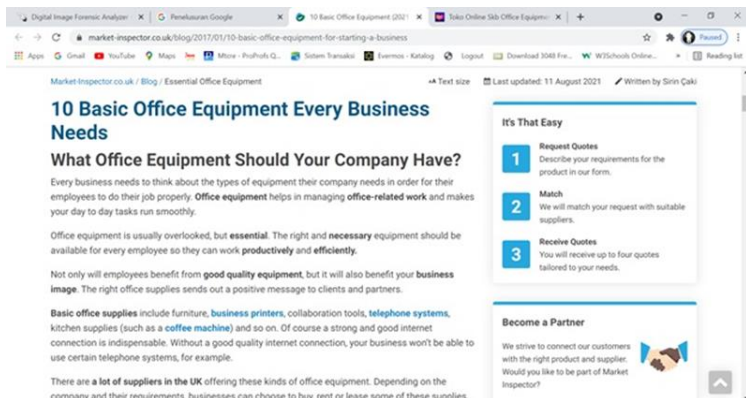
b. Metode Reverse Image



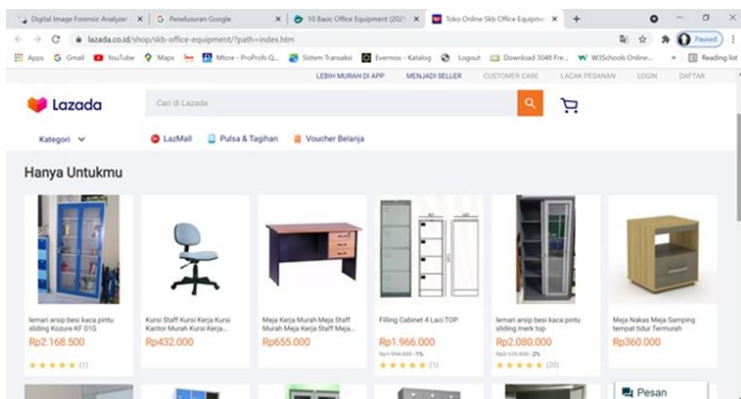
Gambar 40. Hasil yang serupa sesuai dengan foto



Gambar 41. Gambar dan situs yang serupa dengan foto

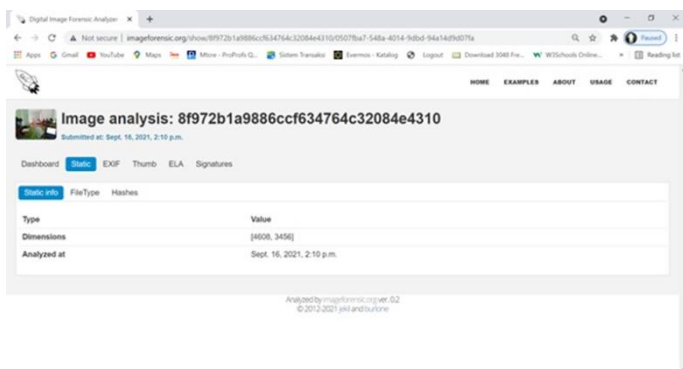


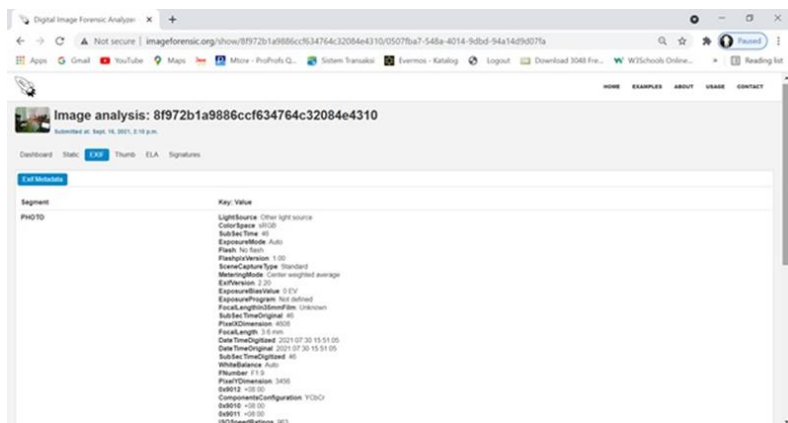
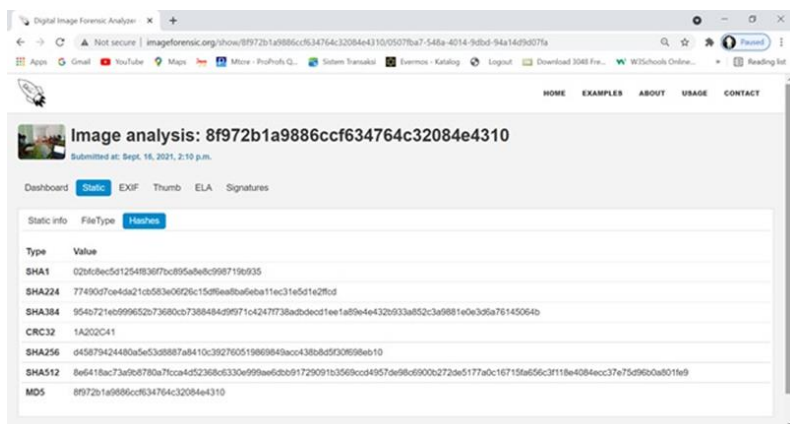
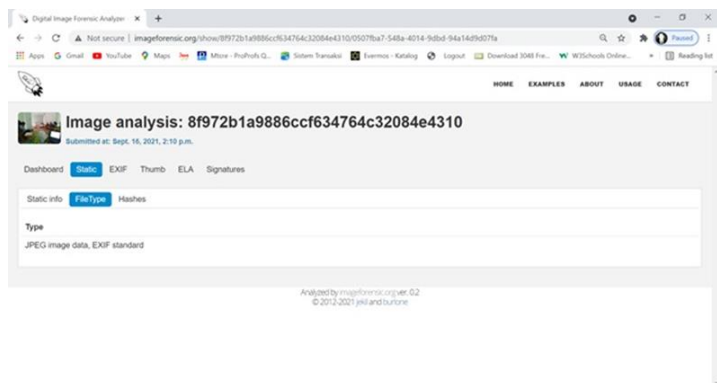
Gambar 42. Contoh situs penyedia yang serupa dengan foto

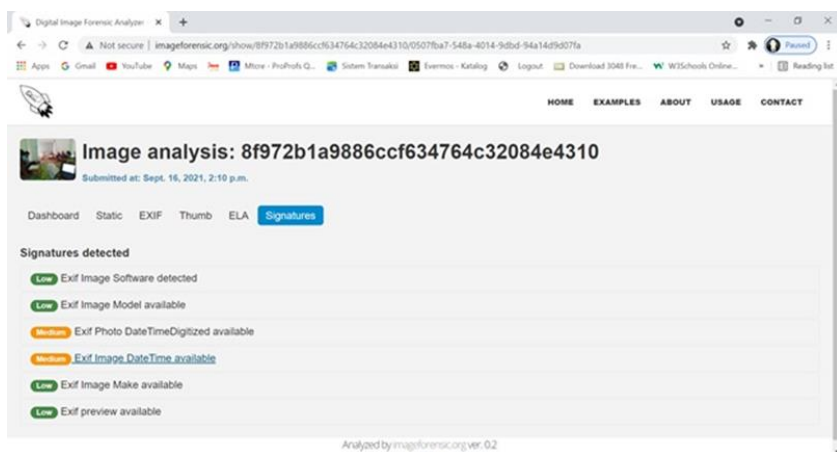
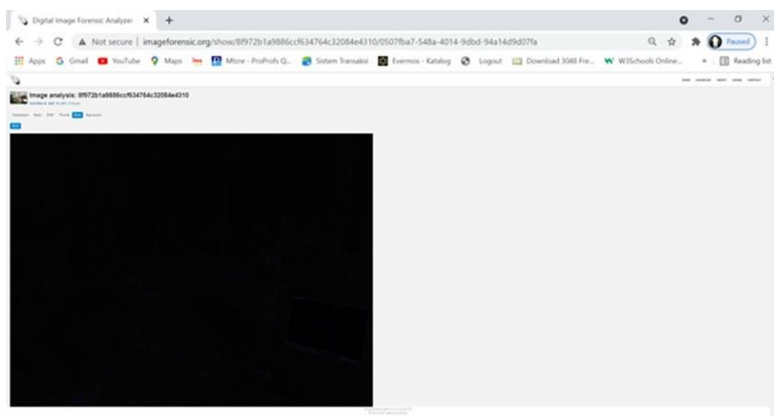
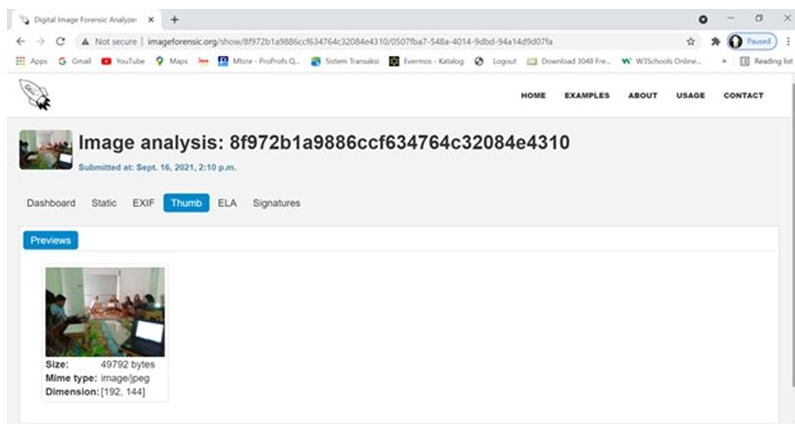


Gambar 43. Contoh situs penyedia yang serupa dengan foto

c. Metode Image Forensics







Gambar 44. Hasil Metode Image Forensics dari Foto Asli

Digital Image Forensic Analyzer

Not secure | imageforensic.org/show/86719959beb77746247c263a0bc06b50/d97c4c9-6655-4c5f-9d28-cb86427c1cb0

HOME EXAMPLES ABOUT USAGE CONTACT

Image analysis: 86719959beb77746247c263a0bc06b50

Submitted at: Sept. 16, 2021, 2:21 p.m.

Dashboard **Static** EXIF IPTC XMP Thumb ELA Signatures

Static info **FileType** Hashes

Type	Value
Dimensions	[4608, 3456]
Analyzed at	Sept. 16, 2021, 2:21 p.m.

Analyzed by imageforensic.org ver. 0.2
© 2012-2021 jkrl and burton

Digital Image Forensic Analyzer

Not secure | imageforensic.org/show/86719959beb77746247c263a0bc06b50/d97c4c9-6655-4c5f-9d28-cb86427c1cb0

HOME EXAMPLES ABOUT USAGE CONTACT

Image analysis: 86719959beb77746247c263a0bc06b50

Submitted at: Sept. 16, 2021, 2:21 p.m.

Dashboard **Static** EXIF IPTC XMP Thumb ELA Signatures

Static info **FileType** Hashes

Type	Value
JPEG image data, EXIF standard	

Analyzed by imageforensic.org ver. 0.2
© 2012-2021 jkrl and burton

Digital Image Forensic Analyzer

Not secure | imageforensic.org/show/86719959beb77746247c263a0bc06b50/d97c4c9-6655-4c5f-9d28-cb86427c1cb0

HOME EXAMPLES ABOUT USAGE CONTACT

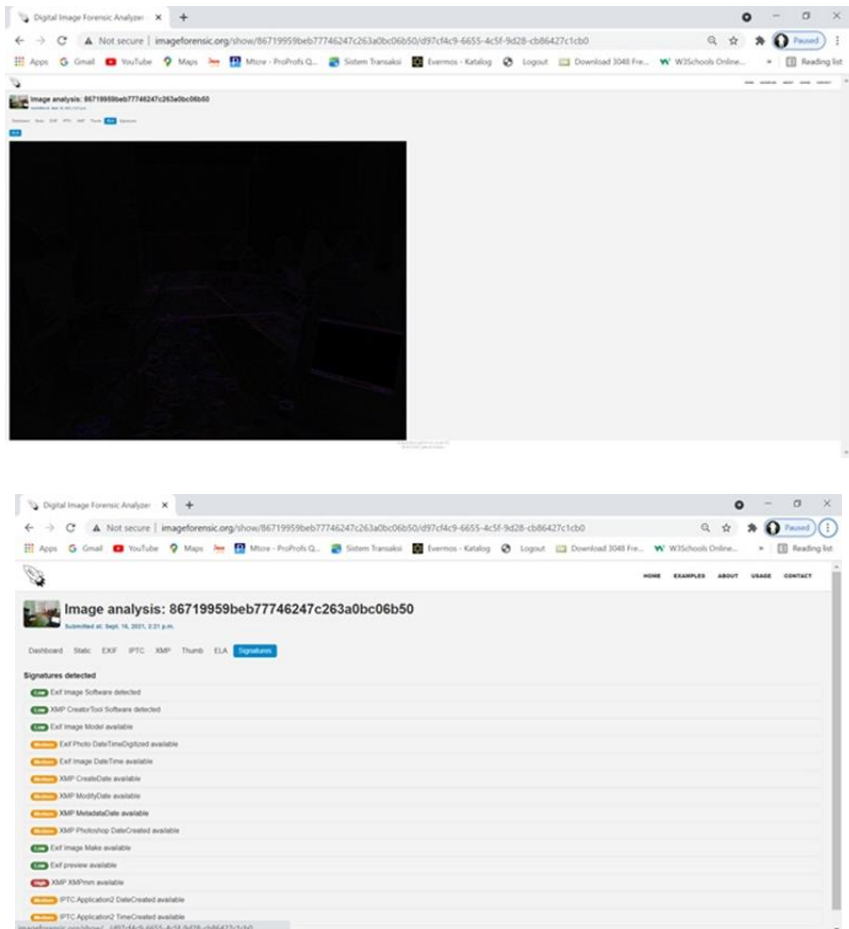
Image analysis: 86719959beb77746247c263a0bc06b50

Submitted at: Sept. 16, 2021, 2:21 p.m.

Dashboard **Static** EXIF IPTC XMP Thumb ELA Signatures

Static info **FileType** Hashes

Type	Value
SHA1	cfc319a66d94811e971c1eb0159630ec6d7c38
SHA224	8fc289330d0c029537d20999faae6030a0024aac19cb2a240be9
SHA384	05ee83acc0ba54e4499aae21311ecf864a0a1789f12eb2a43615642c12cb3ed063493689cb53f8317bf83afa10d5
CRC32	5E546854
SHA256	2a0b6442a2092068c8da24c51f49baa788c85a0c7664831cda115c86372f
SHA512	8b02845c77844b51601b0cc7edcbbaf85f672163ef879c01e895c3081d1d0556906eb7cb3832e5f671f5279397807463e6b97097da540d55c098e4df
MD5	86719959beb77746247c263a0bc06b50



Gambar 45. Hasil Metode Image *Forensics* dari Foto Manipulasi

B. ANALISA HASIL PERBANDINGAN

Beberapa metode/tools yang sudah di uji cobakan, maka akan muncul hasil prosesnya. Kemudian hasil-hasil tersebut di analisa untuk mendapatkan sebuah metode/tools yang tepat yang hasilnya mendekati kebenaran. Berikut analisa hasil perbandingan dari masing-masing metode dalam bentuk tabel dibawah ini:

1. Bukti Foto dari Internet/Media Sosial

Berikut analisa hasil perbandingan yang dilakukan dengan menggunakan 3 metode/tools:

a. Metode Tools Exif/Metadata

Fokus dari metode ini adalah dengan menampilkan berbagai macam metadata yang tersimpan pada sebuah file foto, baik yang ditemukan pada ExifTool by Phil Harvey yang toolsnya harus di download dulu baru kemudian dijalankan pada PC/Laptop tanpa harus menggunakan koneksi internet. Berbeda dengan 2 tools yang lainnya, yaitu fungsinya sama untuk Exif/Metadata juga namun harus menggunakan koneksi internet cara menjalankannya yaitu Tools Jeffrey's Image Metadata Viewer dan EXIF & Metadata Viewer. Berikut adalah perbedaan hasil metadata foto asli dan foto manipulasi yang di tampilkan dari ketiga tools ini:

1) ExifTool by Phil Harvey (Tools Offline)

Analisa hasil perbandingan foto asli dan foto manipulasi dari ExifTool by Phil Harvey (Tools Offline) yaitu value/nilai masing-masing metadatanya menampilkan sama antara foto asli dan foto manipulasi mulai dari File Name, Directory, File Size, File Modification Date/Time, File Access Date/Time, File Creation, File Permissions, File Type, Extension, MIME Type, JFIF Version, Image Size, Megapixels sampai yang lainnya.

2) Tools Jeffrey's Image Metadata Viewer (Tools Online)

Analisa hasil perbandingan foto asli dan foto manipulasi dari Tools Jeffrey's Image Metadata Viewer (Tools Online) yaitu value/nilai masing-masing metadatanya menampilkan sama antara foto asli dan foto manipulasi mulai dari Basic Image Information, IPTC, JFIF, FILE dan Composite

3) EXIF & Metadata Viewer (Tools Online)

Analisa hasil perbandingan foto asli dan foto manipulasi dari EXIF & Metadata Viewer (Tools Online) yaitu value/nilai masing-masing metadatanya menampilkan sama antara foto asli dan foto manipulasi mulai RAW, EXIF, JFIF, IPTC dan Composite.

Dapat disimpulkan dari pengecekan ini bahwa value/nilai antara foto asli dan foto manipulasi yang ditampilkan relatif sama dari ketiga tools ini, sehingga tidak bisa dibedakan antara foto asli dan foto manipulasi.

b. Metode Reverse Image

Jika ditelusuri lebih dalam lagi dari sampel foto asli dan manipulasi yang diambil dari internet/media sosial instagram ini, maka ditemukan kesamaan situs situs yang sudah memiliki foto tersebut, baik asli maupun yang sudah dimanipulasi dan bersebaran dimana-mana.

c. **Metode Image Forensic**

Analisa hasil perbandingan foto asli dan foto manipulasi dari Metode Image Forensic yaitu memiliki halaman hasil pengecekan yang ditampilkan dari foto asli dan foto manipulasi mulai dari Dashbord, Static, IPTC dan ELA yang masing-masing didalamnya mempunyai value/nilai yang berbeda-beda. Misal untuk Static didalamnya ada nilai hashes mulai dari SHA1, SHA224, SHA384, CRC32, SHA256, SHA512 dan MD5 menampilkan nilai yang berbeda dari foto asli dan foto manipulasi. Dapat disimpulkan dari pengecekan ini bahwa value/nilai antara foto asli dan foto manipulasi yang ditampilkan berbeda, sehingga bisa dibedakan antara foto asli dan foto manipulasi dengan catatan nilai hashes foto asli harus diketahui terlebih dahulu.

2. **Bukti Foto dari Smartphone/Laptop**

Berikut analia hasil perbandingan yang dilakukan dengan menggunakan 3 metode/tools:

a. **Metode Tools Exif/Metadata**

Berikut adalah perbedaan hasil metadata foto asli dan foto manipulasi yang di tampilkan dari ketiga tools yang ditampilkan dalam bentuk tabel:

1) **ExifTool by Phil Harvey (Tools Offline)**

Analisa hasil perbandingan foto asli dan foto manipulasi dari ExifTool by Phil Harvey (Tools Offline) ditampilkan dalam tabel 1 dan tabel 2 berikut:

Tabel 1. Analisa Hasil Foto Asli ExifTool by Phil Harvey

<i>Value</i>	<i>Description</i>
Nilai masing-masing deskripsi ada pada gambar 34 diatas.	<i>File Name, Directory, File Size, File Modification Date/Time, File Access Date/Time, File Creation, File Permissions, File Type, Extension, MIME Type, JFIF Version, Image Size, Megapixels, File Inode Change Date, Exif Byte Order, Image Width, Image Height, Encoding Process, Bits Per Sample, Color Components, YcbCr Sub Sampling, Image Description, Make, Model, Orientation, XResolution, YResolution, ResolutionUnit, Software, Modify Date, YcbCr Positioning, Exposure Program, ISO, Exif Version, Date Time Original, Create Date, OffsetTime, OffsetTimeOriginal, Offset Time Digitized, Components Configuration, Digital Zoom Ratio, Focal Length in 35 mm Format, Scene Capture Type, Compression, Orientation, XResolution, YResolution, ResolutionUnit, Thumbnail Offset, Thumbnail Length, YcbCr Positioning, Thumbnail Image, Aperture, ImageSize, Megapixels, ShutterSpeed, Sub Sec Create Date, Sub Sec Date Time Original, SubSec Modify Date, Focal Length 35 efl, LightValue.</i>

Tabel 2. Analisa Hasil Foto Manipulasi ExifTool by Phil Harvey

Value	Description
Nilai masing-masing deskripsi ada pada gambar 34 dan gambar 35 diatas.	<i>File Name, Directory, File Size, File Modification Date/Time, File Access Date/Time, File Creation, File Permissions, File Type, Extension, MIME Type, JFIF Version, Image Size, Megapixels, ExifByteOrder, ImageWidth, ImageHeight, EncodingProcess, BitsPerSample, ColorComponents, YcbCrSubSampling, ImageDescription, Make, Model, Orientation, XResolution, YResolution, ResolutionUnit, Software, ModifyDate, YcbCrPositioning, ExposureProgram, ISO, ExifVersion, DateTimeOriginal, CreateDate, OffsetTime, OffsetTimeOriginal, OffsetTimeDigitized, ComponentsConfiguration, DigitalZoomRatio, FocalLengthin35mmFormat, SceneCaptureType, Compression, Orientation, XResolution, YResolution, ResolutionUnit, ThumbnailOffset, ThumbnailLength, YCbCrPositioning, ThumbnailImage, CodedCharacterSet, ApplicationRecordVersion, DateCreated, TimeCreated, IPTCDigest, XResolution, DisplayedUnitsX, YResolution, DisplayedUnitsY, PrintStyle, PrintPosition, PrintScale, WriterName, ReaderName, PhotoshopQuality, Toolkit, CreatorTool, ModifyDate, CreateDate, MetadataDate, Format, ProfileCMType, ProfileVersion, ProfilClass, ColorSpaceData, ProfileDateTime, ProfilFileSignature, ProfilCreator, ProfileCopyright, ProfileDescription, DCTEncodeVersion, APP14Flags0, APP14Flags1, ColorTransform, Aperture, Aperture, ImageSize, Megapixels, ShutterSpeed, SubSecCreateDate, SubSecDateTimeOriginal, SubSecModifyDate, FocalLength35efl, LightValue.</i>

Untuk analisa hasil perbandingan dari metode exiftool by phil harvey adalah bisa dilihat dengan jelas dari tabel 1 dan tabel 2, dimana tabel 2 lebih banyak memberikan informasi seperti IPTC, Photoshop, XMP, ICC-header. Sudah sangat jelas bahwa gambar 31 merupakan foto yang sudah di manipulasi, karena informasinya memunculkan salah satu tools yang digunakan untuk mengedit memanipulasi foto tersebut yaitu Photoshop.

2) Tools Jeffrey's Image Metadata Viewer (Tools Online)

Analisa hasil perbandingan foto asli dan foto manipulasi dari Tools Jeffrey's Image Metadata Viewer (Tools Online) ditampilkan dalam tabel 3 dan tabel 4 berikut:

Tabel 3. Analisa Hasil Foto Asli Tools Jeffrey's Image Metadata Viewer

No	Menu	Description
1	Basic Image Information	<i>Camera, Lens, Exposure, Flash, Date, File, Color Encoding</i>
2	EXIF	<i>Exif Image Size, Make, Camera Model Name, Software, Modify Date, Exposure Time, F Number, ISO, Exif Version, Date/Time Original, Create Date, Color SPace, Digital Zoom Ratio, Scene Capture Type, Compression, Orientation, Resolution, Thunmbnail Length, Thumbnail Image.</i>
3	File	<i>File Type, MIME Type, Exif Byte Order, Bits Per Sample, Color Components, File Size, Extension, Image Size, Y Cb Cr Sub Sampling.</i>
4	Composite	<i>Aperture, Megapixels, Shutter Speed, Create Date, Date/Time Original, Modify Date, Focal Length, Light Value.</i>
5	ExifTool	<i>Warning: [minor] Unknown APP6 - APP8 segment</i>

Tabel 4. Analisa Hasil Foto Manipulasi Tools Jeffrey's Image Metadata Viewer

No	Menu	Description
1	Basic Image Information	<i>Camera, Lens, Exposure, Flash, Date, File, Color Encoding</i>
2	XMP	<i>Date Created, XMP Toolkit, Creator Tool, Modify Date, Metadata Date, Color Mode, ICC Profile Name, Document ID, Instance ID, Original Document ID, Format, History Action, History Instance ID, History When, History Software Agent, History Changed.</i>
3	EXIF	<i>Bits Per Sample, Photometric Interpretation, Make, Camera Model Name, Software, Modify Date, Exposure Time, F Number, ISO, Exif Version, Date/Time Original, Create Date, Color SPace, Digital Zoom Ratio, Scene Capture Type, Compression, Orientation, Resolution, Thunmbnail Length, Thumbnail Image.</i>
4	Photoshop	<i>IPTC Digest, Print Info 2, Print Style, X Y Resolution, Displayed Units X Y, Resolution, Print Position, Print Scale, Flags, Global Angle, Altitude, Pixel, Writer Name, Reader Name, Version, Quality, Format, Proressive Scans.</i>

5	APP14	<i>DCT Encode Version, Flags 0, Flags 1, Color Transform.</i>
6	IPTC	<i>CodedCharacterSet, ApplicationRecordVersion, DateCreated, TimeCreated</i>
7	File	<i>File Type, MIME Type, Exif Byte Order, Bits Per Sample, Color Components, File Size, Extension, Image Size, Y Cb Cr Sub Sampling.</i>
8	Composite	<i>Aperture, Megapixels, Shutter Speed, Create Date, Date/Time Original, Modify Date, Focal Length, Light Value.</i>

Untuk analisa hasil perbandingan dari metode tools jeffrey's image metadata viewer adalah bisa dilihat dengan jelas dari tabel 3 dan tabel 4, dimana tabel 4 lebih banyak memberikan informasi seperti Photoshop, APP14 dan IPTC. Sudah sangat jelas bahwa gambar 37 merupakan foto yang sudah di manipulasi, karena informasinya memunculkan salah satu tools yang digunakan untuk mengedit memanipulasi foto tersebut yaitu Photoshop.

3) EXIF & Metadata Viewer (Tools Online)

Analisa hasil perbandingan foto asli dan foto manipulasi dari EXIF & Metadata Viewer (Tools Online) ditampilkan dalam tabel 5 dan tabel 6 berikut:

Tabel 5. Analisa Hasil Foto Asli EXIF & Metadata Viewer

No	Menu	Description
1	System	<i>FileName, FileSize, FileModifyDate, FileAccessDate, FileNodeChangeDate, FilePermissions</i>
2	File	<i>FileType, FileTypeExtension, MIMEType, ExifByteOrder, ImageWidth, ImageHeight, EncodingProcess, BitsPerSample, ColorComponents, YcbCrSubSampling</i>
3	IFD0	<i>ImageDescription, Make, Model, Orientation, XResolution, YResolution, ResolutionUnit, Software, ModifyDate, YcbCrPositioning</i>
4	ExifIFD	<i>ExposureProgram, ISO, ExifVersion, DateTimeOriginal, CreateDate, OffsetTime, OffsetTimeOriginal, OffsetTimeDigitized, ComponentsConfiguration, DigitalZoomRatio, FocalLengthin35mmFormat, SceneCaptureType</i>
5	IFD1	<i>Compression, Orientation, XResolution, YResolution, ResolutionUnit, ThumbnailOffset, ThumbnailLength, YCbCrPositioning, ThumbnailImage</i>

6	Composite	Aperture, ImageSize, Megapixels, ShutterSpeed, SubSecCreateDate, SubSecDateTimeOriginal, SubSecModifyDate, FocalLength35efl, LightValue
---	-----------	---

Tabel 6. Analisa Hasil Foto Manipulasi EXIF & Metadata Viewer

No	Menu	Description
1	System	FileName, FileSize, FileModifyDate, FileAccessDate, FileInodeChangeDate, FilePermissions
2	File	FileType, FileTypeExtension, MIMEType, ExifByteOrder, ImageWidth, ImageHeight, EncodingProcess, BitsPerSample, ColorComponents, YcbCrSubSampling
3	IFD0	ImageDescription, Make, Model, Orientation, XResolution, YResolution, ResolutionUnit, Software, ModifyDate, YcbCrPositioning
4	ExifIFD	ExposureProgram, ISO, ExifVersion, DateTimeOriginal, CreateDate, OffsetTime, OffsetTimeOriginal, OffsetTimeDigitized, ComponentsConfiguration, DigitalZoomRatio, FocalLengthin35mmFormat, SceneCaptureType
5	IFD1	Compression, Orientation, XResolution, YResolution, ResolutionUnit, ThumbnailOffset, ThumbnailLength, YCbCrPositioning, ThumbnailImage
6	IPTC	CodedCharacterSet, ApplicationRecordVersion, DateCreated, TimeCreated
7	Photoshop	IPTCDigest, XResolution, DisplayedUnitsX, YResolution, DisplayedUnitsY, PrintStyle, PrintPosition, PrintScale, WriterName, ReaderName, PhotoshopQuality
8	XMP	Toolkit, CreatorTool, ModifyDate, CreateDate, MetadataDate, Format
9	ICC-header	ProfileCMIMType, ProfileVersion, ProfilClass, ColorSpaceData, ProfileDateTime, ProfilFileSignature, ProfilCreator, ProfileCopyright, ProfileDescription
10	Adobe	DCTEncodeVersion, APP14Flags0, APP14Flags1, ColorTransform, Aperture
11	Composite	Aperture, ImageSize, Megapixels, ShutterSpeed, SubSecCreateDate, SubSecDateTimeOriginal, SubSecModifyDate, FocalLength35efl, LightValue

Untuk analisa hasil perbandingan dari metode tools exif/metadata adalah bisa dilihat dengan jelas dari tabel 5 dan tabel 6, dimana tabel 6 lebih banyak memberikan informasi seperti IPTC, Photoshop, XMP, ICC-header. Sudah sangat jelas bahwa gambar 39 merupakan foto yang sudah di manipulasi, karena informasinya memunculkan salah satu tools yang digunakan untuk mengedit memanipulasi foto tersebut yaitu Photoshop.

b. Metode Reverse Image

Analisa hasil perbandingan dari metode reverse image adalah menampilkan OfficeEquipment atau peralatan kantor yang sesuai dan berhubungan dengan apa yang ada di gambar, baik dari foto asli maupun yang sudah dimanipulasi, sehingga pada saat muncul banyak gambar-gambar yang berupa peralatan kantor dan link website yang ditampilkan juga berisi tentang peralatan kantor semua. Foto asli yang diambil dari Smartphone dan yang sudah di manipulasi dengan Photoshop ini juga tidak ditemukan gambar persis yang sama di internet, karena memang foto sampel ini belum pernah di *upload* di media sosial dan website. Berbeda dengan kasus sampel 3.1 Bukti Foto dari Internet/Media Sosial diatas, banyak yang tersebar di internet karena memang foto sampel tersebut diambil di Internet/Media Sosial.

c. Metode Image Forensics

Analisa hasil perbandingan foto asli dan foto manipulasi dari metode image *forensics* ditampilkan dalam tabel 7 dan tabel 8 berikut:

Tabel 7. Analisa Hasil Foto Asli Image Forensics

No	Menu	Description
1	Dashboard	Static analysis, EXIF metadata extraction, Preview extraction from metadata, Localization, Error Level Analysis, Signature check
2	Static	Static info, FileType, Hashes
3	EXIF	Segment, PHOTO, IMAGE, THUMBNAIL, IOP
4	Thumb	Size, Mime type, Dimension
5	ELA	Black Striped Drawing
6	Signatures	Low, Medium

Tabel 8. Analisa Hasil Foto Manipulasi Image Forensics

No	Menu	Description
1	Dashboard	<i>Static analysis, EXIF metadata extraction, IPTC extraction, XMP extraction, Preview extraction from metadata, Localization, Error Level Analysis, Signature check</i>
2	Static	<i>Static info, FileType, Hashes</i>
3	EXIF	<i>Segment, PHOTO, IMAGE, THUMBNAIL, IOP</i>
4	IPTC	<i>Segment, APPLICATION2, ENVELOPE</i>
5	XMP	<i>Segment, XMPMM, PHOTOSHOP, XMP, DC</i>
6	Thumb	<i>Size, Mime type, Dimension</i>
7	ELA	<i>Black Striped Drawing</i>
8	Signatures	<i>Low, Medium, High</i>

Untuk analisa hasil perbandingan dari Metode Image Forensics adalah dengan membandingkan tabel 7 dan tabel 8, dimana tabel 8 lebih banyak memberikan informasi seperti IPTC, XMP. Sudah sangat jelas juga bahwa gambar 45 merupakan foto yang sudah di manipulasi, karena informasinya memunculkan salah satu tools yang digunakan untuk mengedit memanipulasi foto tersebut yaitu Photoshop sama seperti metode tools exif/metadata, bedanya Metode Image Forensics bisa memunculkan Error Level Analysis (ELA) untuk mendeteksi perbedaan error pada seluruh bagian foto yang disimpan dengan kompresi lossy seperti JPEG. Algoritma ELA mempermudah pengguna untuk mengetahui apakah sebuah foto sudah asli atau hasil dari manipulasi. Dari hasil analisis ELA sendiri bahwa gambar 31 memiliki daerah dan tepian yang berbeda pada bagian gambar 30 yang asli, sehingga bisa disimpulkan gambar 31 merupakan gambar hasil manipulasi.



BAB 5

PENUTUP

A. KESIMPULAN

Kesimpulan yang bisa diambil dari penelitian ini adalah adanya sebuah pilihan metode yang bisa digunakan oleh para pengguna internet/media sosial dalam menyaring sebuah informasi yang berhubungan foto hoax, dimana para pengguna bisa melakukan analisa terlebih dahulu sebelum menyebarkan kembali informasi/foto tersebut. Dengan melihat hasil analisa foto asli dan foto manipulasi dari ketiga metode diatas bisa ditarik kelebihan dan kekurangan dari masing-masing metode tersebut. Metode Tools Exif/Metadata banyak menampilkan metadata file yang tersembunyi pada sebuah foto yang bisa di analisa informasi kebenaran apa saja yang terkandung didalamnya, Metode Reverse Image bisa menelusuri foto-foto serupa yang mirip atau yang aslinya sehingga akan muncul foto-foto yang pernah di upload dan dimiliki oleh siapa saja dan yang terakhir dengan Metode Image *Forensics* juga banyak menampilkan metadata file yang ada didalam foto sampai memunculkan Error Level Analysis (ELA) foto dimana daerah dan tepian yang mirip pada foto aslinya akan terlihat mirip pula, jika tidak mirip, besar kemungkinan foto tersebut hasil manipulasi.

B. SARAN

Pengembangan selanjutnya dalam penelitian ini bisa dengan menggunakan metode lain dari ketiga metode yang sudah di uji cobakan itu, dengan melihat kemudahan dan efektivitasnya dari sisi pengguna. Untuk foto juga bisa mengambil sampel yang ada di PC/Laptop untuk kemudian di upload terlebih dahulu di internet/media sosial. Bukti foto yang sudah di upload kemudian di download kembali lalu melakukan manipulasi, sehingga hasil analisisnya dengan menggunakan metode yang dilakukan diatas atau yang lainnya bisa dibandingkan dengan sampel foto yang ada di PC/Laptop yang belum pernah di *upload*.

DAFTAR PUSTAKA

- Kementerian Komunikasi Dan Informatika. (2018, October 4). 1000 Berita Hoax Selama Masa Kampanye Pemilu 2019. Retrieved From Detik.Com: <https://news.detik.com/berita/4264513/kemenkominfo-ada-1000-berita-hoax-selama-masa-kampanye-pemilu>
- Mastel. (2017, February 13). Hasil Survey Mastel Tentang Wabah Hoax Nasional. Retrieved From Mastel.Id: <https://mastel.id/infografis-hasil-survey-mastel-tentang-wabah-hoax-nasional>
- Juliswara, V. (2017). Mengembangkan Model Literasi Media Yang Berkebhinnekaan Dalam Menganalisis Informasi Berita Palsu (Hoax) Di Media Sosial. Jurnal Pemikiran Sosiologi Volume 4 No. 2, 142-164.
- Gumilar, G., Adiprasetyo, J., & Maharani, N. (2017). Literasi Media: Cerdas Menggunakan Media Sosial Dalam Menanggulangi Berita Palsu (Hoax) Oleh Siswa Sma. Jurnal Pengabdian Kepada Masyarakat Vol. 1, No. 1 Issn 1410 - 5675, 35-40.
- Adhianto, D. S., Utari, P., & Slamet, Y. (2017). Pemberitaan Hoax Di Media Online Ditinjau Dari Konstruksi Berita Dan Respon Netizen. Jurnal Ilmu Komunikasi, Volume 15, Nomor 3, September - Desember, 215-225.
- Juditha, C. (2018). Interaksi Komunikasi Hoax Di Media Sosial Serta Antisipasinya. Jurnal Pekommas, Vol. 3 No. 1, April, 31-44.
- Fatkhurrahman. (2018). Kemampuan Mahasiswa Tempatan Menilai Berita Palsu Atau "Hoax" Dalam Media Sosial Dalam Upaya Pengembangan Jiwa Kewirausahaan. Jurnal Benefita 3(3) Oktober, 417-426.
- Heriyanto. (2013). Analisa Gambar Bitmap Termodifikasi Atau Tidak Termodifikasi Dengan Memadukan Metode Deviasi Pixel, Rgb (Red Green Blue) Dan Histogram. Seminar Nasional Informatika 2013 (Semnasif 2013). Issn: 1979-2328.
- Riadi, I., Fadlil, A., & Sari, T. (2017). Image *Forensic* For Detecting Splicing Image With Distance Function. International Journal Of Computer Applications (0975 – 8887). Volume 169 – No.5.
- Riadi, I., Yudhana, A., & Yuli Sulisty, W. (2019). Deteksi Pemalsuan Foto Digital Menggunakan Image *Forensics*. Jurnal Mobile And *Forensics* (Mf). Vol. 1, No. 1, Pp. 13-21. P-Issn: 2656-6257, E-Issn: 2714-6685.
- Imanda Putra, A., Umar, R., & Fadlil, A. (2018). Analisis Forensik Deteksi Keaslian Metadata Video Menggunakan Exiftool. Seminar Nasional Informatika 2018 (Semnasif 2018). Issn: 1979-2328.

- Lad Ami D., Mori Shilpa I., Raulji Urvashi K., & Shaikh Saliha H. (2017). Reverse Image Search: Image Retrieval Using Various Techniques. Scientific Journal Of Impact Factor (Sjif): 4.72. Volume 4, Issue 4, E-Issn (O): 2348-4470.
- Wijayanto, H., Ady Prabowo, I., & Harsadi, P. (2018). Optimalisasi Penyusutan Exif Metadata Dengan Teknik Substitusi Null Value Pada Kasus Keamanan Citra Digital. Jurnal Ilmiah Sinus 16(1).
- Adrakatti, A .F., Wodeyar, R. S., & Mulla, K. R. (2016). Search By Image: A Novel Approach To Content Based Image Retrieval System. International Journal Of Library Science™. Volume 14; Issue No. 3; Issn 0975-7546.
- Yuli Sulistyo, W., Riadi, I., & Yudhana, A. (2018). Analisis Deteksi Keaslian Citra Menggunakan Teknik Error Level Analysis Dengan *Forensicallybeta*. Seminar Nasional Informatika 2018 (Semnasif 2018). Issn: 1979-2328.
- Wijayanto, H., Ady Prabowo, I., & Harsadi, P. (2018). Optimalisasi Penyusutan Exif Metadata Dengan Teknik Substitusi Null Value Pada Kasus Keamanan Citra Digital. Jurnal Ilmiah Sinus 16(1).
- Apriliani, A., Hijjayanti, K., & Suhairoh. (2020). Analisis Keaslian Citra Dengan Menggunakan Exif Metadata. Cess (Journal Of Computer Engineering System And Science), 84-88
- P. N. Andono, T. Sutojo Och M. , Pengolahan Citra Digital, Yogyakarta: Andi, 2017.
- Exiftool By Phil Harvey (2021, July 30). Metode Tools Exif/Metadata. Retrieved From Exiftool.Org: [Https://Exiftool.Org/](https://Exiftool.Org/)
- Jeffrey's Image Metadata Viewer (2021, July 30). Metode Tools Exif/Metadata. Retrieved From Exif.Regex.Info: [Http://Exif.Regex.Info/Exif.Cgi](http://Exif.Regex.Info/Exif.Cgi)
- Exif & Metadata Viewer (2021, July 30). Metode Tools Exif/Metadata. Retrieved From Exifmeta.Com: [Https://Exifmeta.Com/](https://Exifmeta.Com/)
- Adrakatti, A .F., Wodeyar, R. S., & Mulla, K. R. (2016). Search By Image: A Novel Approach To Content Based Image Retrieval System. International Journal Of Library Science™. Volume 14; Issue No. 3; Issn 0975-7546.
- Google Images (2021, July 30). Metode Reverse Image. Retrieved From Images.Google.Com: [Https://Images.Google.Com/](https://Images.Google.Com/)
- Yuli Sulistyo, W., Riadi, I., & Yudhana, A. (2018). Analisis Deteksi Keaslian Citra Menggunakan Teknik Error Level Analysis Dengan *Forensicallybeta*. Seminar Nasional Informatika 2018 (Semnasif 2018). Issn: 1979-2328.

Rizky Al-Fajri, M., Caruddin & Yusup, D. (2021). Analisis Image *Forensic* Dalam Mendeteksi Rekayasa File Image Dengan Metode Nist. Jurnal Sistem Dan Teknologi Informasi (Justindo). Volume 6, No. 2; E-Issn: 25541-5735, P-Issn: 2502-5724.

Image *Forensic* (2021, July 30). Metode Image *Forensics*. Retrieved From Imageforensic.Com: <https://www.imageforensic.org/>

PROFIL PENULIS

Moh. Subli



Moh. Subli lahir pada tahun 1989 di Kertasari sebuah dusun yang ada di Desa Sukarema Kecamatan Aikmel Kabupaten Lombok Timur Nusa Tenggara Barat. Penulis yang menempuh pendidikan S1 dan S2 bidang Komputer ini fokus ke bidang Network, Cyber Security dan *Forensic Digital*. Beberapa penelitiannya pun berhubungan dengan bidang tersebut, seperti Design of *Forensic* Metadata System to Support the Digital Investigation Processes

pada International Journal of Computer Science and Information Security tahun 2020 dan ditahun yang sama juga membuat jurnal publikasi karya ilmiah tentang Penerapan Spanning Tree Protocol Untuk Mencegah Terjadinya Looping Pada Frame Ethernet dan pada tahun 2021 melakukan penelitian tentang Perbandingan Hasil Analisa Foto Hoax Menggunakan Metode Exif/Metadata, Reverse Image dan Image *Forensics*. Penulis juga sering mengikuti seminar-seminar, workshop dan mengambil pelatihan sertifikat profesionalnya, mulai dari Certified Ethical Hacker (CEH) dan Computer Hacking *Forensic* Investigator (CHFI) yang diselenggarakan oleh The International Council Of E-Commerce Consultants (Ec-Council), Asesor Kompetensi Bidang Network Designer dari Badan Nasional Sertifikasi Profesi (BNSP), MikroTik Certified Network Associate (MTCNA) dan MikroTik Certified Routing Engineer (MTCRE) dari Mikrotik Certified Training Programs, Pelatihan Training Of Trainer Cisco Devnet Associate dari Cisco, Pelatihan Cyber Security Analyst oleh Thematic Academy Kominfo Digital Talent. Kerjaan sehari-hari penulis mengajar disalah satu Perguruan Tinggi yang di Mataram dan aktif membina UKM Cyber Security Universitas Teknologi Mataram.

Email : subli.kerta@gmail.com

Muhamad Masjun Efendi



Penulis lahir pada tahun 1991 di Dasan Re, sebuah Dusun yang berada di Kalijaga Timur Kecamatan Aikmel Kabupaten Lombok Timur Nusa Tenggara Barat. Penulis menempuh pendidikan S1 Desain Komunikasi Visual dan S2 di bidang Forensik digital fokus di image processing. Beberapa penelitiannya yang berhubungan dengan bidang tersebut, “Metode Deteksi Tepi Block JPEG Terkompresi untuk Meningkatkan Akurasi Analisis Manipulasi Splicing pada Citra Berekstensi JPEG”, “The Implementation of Extraction Feature Using GLCM and Back-Propagation Artificial Neural Network to Clasify Lombok Songket Woven Cloth” dan Penerapan Digital Signature Scheme dengan Metode Schnorr Authentication. Kerjaan sehari hari mengajar di salah satu kampus yang di Mataram dan untuk usaha tambahan, juga membuka studio yang bergerak di bidang Jasa Digital Skerching, Animasi, Desain, Interior / Exterior, Fotografer dan Video Shooting.

Email : creativepio@gmail.com

Perbandingan Hasil Analisa **FOTO HOAX**

Menggunakan Metode Exif/Metadata Reverse Image & Image Forensics



Berkembangnya teknologi menyebabkan sebuah informasi dapat dengan mudahnya menyebar secara luas dan juga cepat. Dampak negatif yang terjadi akibat mudahnya informasi menyebar salah satunya yaitu informasi dapat dengan mudahnya di manipulasi, salah satunya adalah informasi berbentuk foto yang telah di rekayasa atau edit. Untuk mencegah hal tersebut dapat dilakukan analisis ke foto tersebut dengan image forensic. Dengan bantuan tools image forensic seperti Jpegsnoop kita dapat melihat metadata dari foto tersebut sehingga kita dapat dengan mudah mencari tahu sumber foto tersebut, dan dengan Forensically beta dapat dilakukan analysis dengan metode Error level analysis untuk melihat objek yang direkayasa. Dengan menerapkan metodologi NIST (Nasional Institute of Standart and Technology) dalam tahapannya akan dilakukan simulasi dengan melakukan analysis perbandingan ke pada dua foto yang diantaranya terdapat foto asli dan yang sudah direkayasa.

Dari perbandingan yang dilakukan akan diketahui bahwa terdapat perbedaan metadata yang dihasilkan dan juga error level analysis yang dihasilkan dapat membuktikan bahwa foto tersebut sudah di rekayasa. Berdasarkan hal tersebut maka, buku ini menyajikan segala yang dibutuhkan oleh para penganalisa dalam menganalisa suatu foto atau gambar, sehingga perbandingan hasil analisa foto hoax menggunakan metode exif/metadata, reverse image dan image forensics menjadi lebih efektif dan efisien. Oleh sebab itu buku ini hadir dihadapan sidang pembaca sebagai bagian dari upaya diskusi sekaligus dalam rangka melengkapi khazanah keilmuan dibidangnya, sehingga buku ini sangat cocok untuk dijadikan bahan acuan bagi kalangan intelektual di lingkungan perguruan tinggi ataupun praktisi yang berkecimpung langsung dibidangnya.