Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

ANALISIS FORENSIK CITRA DI *PLATFORM* X MENGGUNAKAN METODE *DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS)*

Wicaksono Yuli Sulistyo[1*], Septia Ayu Pratiwi[2], Muhammad Haedar Zhafran Hidayatullah[3]

[1,2,3]Sistem Informasi, Fakultas Teknologi dan Ilmu Kesehatan, Universitas Siber Muhammadiyah, DI Yogyakarta, Indonesia
Email: [1*]wicaksono@sibermu.ac.id, [2]pratiwi@sibermu.ac.id, [3]zafran@sibermu.ac.id
(* : coressponding author)

Abstrak - Salah satu dampak negatif yang muncul adalah perilaku masyarakat yang kurang terkendali dalam menggunakan aplikasi pribadi, sehingga berpotensi menimbulkan kejahatan siber *(cybercrime).* Kasus *cybercrime* yang umum terjadi di media sosial meliputi pengunggahan foto untuk melakukan perundungan, menyebarkan informasi palsu, penipuan, dan pencemaran nama baik. Foto dapat dengan mudah diubah atau diedit, sehingga informasi yang disampaikan dapat dimanipulasi dan berpotensi digunakan untuk kejahatan. Saat ini, kemudahan mengunggah foto dan sulitnya mendeteksi keaslian foto merupakan faktor yang menjadi dasar utama dilakukannya penelitian ini, yang bertujuan untuk mendeteksi pemalsuan foto digital. Penelitian ini menggunakan *Digital Forensic Research Workshop (DFRWS)* untuk mengetahui adanya pemalsuan foto digital pada *platform X*. Tahapan penting yang digunakan dalam penelitian ini adalah identifikasi, pemeliharaan, pengumpulan, pemeriksaan, analisis, dan presentasi. Dari hasil penelitian, ditemukan bahwa terdapat perubahan piksel di area objek *smartphone* serta area lain yang menunjukkan adanya hasil manipulasi, sehingga terlihat berbeda dari foto yang asli. Selain itu, melalui *FotoForensic*, metadata foto berhasil diperoleh, dan diketahui bahwa foto kedua merupakan hasil edit dengan indikasi pernah dimodifikasi menggunakan *Adobe Photoshop* CC 2017. Dari hasil analisis menggunakan *ForensicallyBeta* juga terlihat perbedaan piksel di beberapa bagian yang menunjukkan adanya *noise* tambahan, yang mengindikasikan bahwa foto tersebut telah disunting di bagian-bagian tertentu, sehingga menunjukkan ketidakaslian foto.

Kata Kunci: *Digital Forensic Research Workshop, Cybercrime*, Pemalsuan Gambar

Abstract - *One of the negative impacts observed is the uncontrolled behavior of individuals in using personal applications, which has the potential to lead to cybercrimes. Common cases of cybercrime on social media involve posting photos for bullying purposes, spreading false information, fraud, and defamation. Photos can be easily altered or edited, enabling the manipulation of information that could be exploited for malicious activities. Nowadays, the ease of uploading photos and the difficulty in detecting their authenticity are key factors underlying this study, which aims to detect digital photo forgery in the platform X. The study adopts the Digital Forensic Research Workshop (DFRWS) framework to identify instances of digital photo forgery. The key stages implemented in this research include identification, preservation, collection, examination, analysis, and presentation. The findings revealed pixel alterations in the smartphone object area and other regions, indicating manipulation and making the image appear different from the original. Additionally, using FotoForensic, metadata from the photos was successfully retrieved, revealing that the second photo had been edited and previously modified using Adobe Photoshop CC 2017. Furthermore, analysis with ForensicallyBeta identified pixel discrepancies in several parts of the image, showing additional noise, which confirmed that the photo had been edited in specific areas, thus indicating its lack of authenticity.*

Keywords*: Digital Forensic Research Workshop, Cybercrime, Image Forgery*

1. PENDAHULUAN

Teknologi yang semakin berkembang memberikan dampak yang signifikan terhadap beberapa aspek, termasuk dalam bidang fotografi. Terdapat keunggulan dan kelemahan dari penggunaan foto digital seperti kemudahan untuk dimanipulasi menggunakan perangkat lunak pengeditan, yang dapat mengubah pesan yang ingin disampaikan melalui foto tersebut [1]. Kemajuan dalam perangkat lunak pengeditan membuat manipulasi foto menjadi semakin mudah bagi siapa pun, sehingga menimbulkan banyak kasus manipulasi foto yang beredar di internet. Seseorang dapat dengan mudah menyambung gambar, menyalin, dan mengubah gambar (*retouching*) yang mengakibatkan semakin sulitnya membedakan foto orisinil dengan foto hasil penyuntingan yang didukung oleh perkembangan teknik memanipulasi foto [2]. Kemudahan dalam membuat dan mengubah gambar menimbulkan tantangan terhadap kredibilitas keaslian foto di berbagai bidang, sehingga rentan digunakan untuk tindakan kriminal karena perubahan pada foto dapat mengubah informasi yang disampaikan [3].

Saat ini, telepon genggam modern atau *smartphone* dilengkapi dengan sistem operasi yang memungkinkan fungsi mirip komputer, termasuk akses internet. Indonesia memiliki jumlah pengguna Android yang tinggi, pengguna *smartphone* yang mengakses internet berbasis selain Android dan iOS ada sekitar 15%, sedangkan untuk *Apple iOS* ada 19% dan yang terbanyak yaitu sistem operasi Android sebesar 66%, hal tersebut membuat pengguna media sosial sangat tinggi yaitu mencapai 2,31 triliun di seluruh dunia [4]. *Retouching* adalah teknik manipulasi foto yang sering dijumpai di aplikasi media sosial seperti *Instagram, Facebook, dan X* dengan

Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

beragam tujuan, baik positif maupun negatif. Kejahatan berbasis teknologi terus meningkat dengan berbagai metode, sehingga diperlukan mekanisme ilmiah untuk melacak dan menganalisis bukti-bukti digital yang tersedia. Gambar atau foto dapat berfungsi sebagai barang bukti dalam ranah hukum atau pengadilan. Jika foto yang diajukan diketahui telah dimanipulasi, validitas foto tersebut akan hilang dan tidak dapat digunakan sebagai bukti sah di pengadilan [5].

Kemajuan dalam perangkat lunak pengeditan gambar memudahkan seseorang untuk memanipulasi gambar. Manipulasi citra bisa dikelompokkan menjadi tiga yaitu: *retouching*, *splicing* gambar, dan *copy-move*. Manipulasi gambar/citra sering dilakukan sebelum gambar dipublikasikan, biasanya dengan tujuan tertentu seperti menyindir seseorang atau memperbaiki penampilan. Teknik *Copy-move* merupakah salah satu teknik manipulasi gambar yang paling sering digunakan karena yang relatif mudah dan efektif. *Copy-move* merupakan teknik manipulasi dengan menyembunyikan objek dalam gambar menggunakan blok kecil yang disalin dari area lain dalam gambar yang sama. Kejahatan berbasis teknologi terus meningkat dengan berbagai modus, sehingga diperlukan mekanisme ilmiah untuk menganalisis dan melacak bukti digital yang tersedia [6].

Digital forensik adalah aktivitas yang mencakup pengumpulan bukti, identifikasi, dokumentasi, identifikasi, dan penyaringan bukti digital dalam kasus kejahatan komputer [7]. Digital forensik memiliki banyak kegunaan dan dapat diterapkan dalam berbagai konteks, bukan hanya untuk kasus kriminal yang melibatkan hukum, tetapi juga untuk rekonstruksi insiden penyelesaian masalah terkait perangkat keras, keamanan komputer, perangkat lunak, dan serta pemulihan sistem yang rusak [8]. Digital forensik menyediakan keahlian teknis dalam pengumpulan bukti digital yang dapat disajikan di pengadilan sesuai dengan hukum yang berlaku [9]. Digital forensik terdiri dari beberapa cabang, seperti *System Forensic*, *Mobile Forensic*, *Network Forensic*, dan *Image Forensic* [10]. Kejahatan siber atau *cybercrime* merupakan salah satu kasus umum yang membutuhkan forensik Digital. *Cybercrime* memiliki sifat yang cepat dan efisien, sehingga menyulitkan pihak berwenang dalam menangkap pelakunya. Hal ini sering disebabkan oleh kurangnya pemahaman dan pengetahuan dalam menangani kejahatan siber. Oleh karena itu, diperlukan pengaturan hukum dan pengawasan terhadap aktivitas yang diduga terkait dengan *cybercrime* [11].

Forensik citra digital membantu penegak hukum, intelijen, investigasi swasta, dan media dalam menangani kasus yang melibatkan keaslian gambar. Kemajuan teknologi gambar saat ini menimbulkan tantangan baru dalam memastikan keaslian gambar. Forensik citra digital adalah metode ilmiah dalam penelitian yang bertujuan mengungkap bukti untuk menilai keaslian gambar. Banyak kasus kriminal dan pornografi yang melibatkan *file* gambar, sehingga forensik gambar sebagai bukti menjadi kunci penting bagi pengadilan dalam membuat keputusan [12].

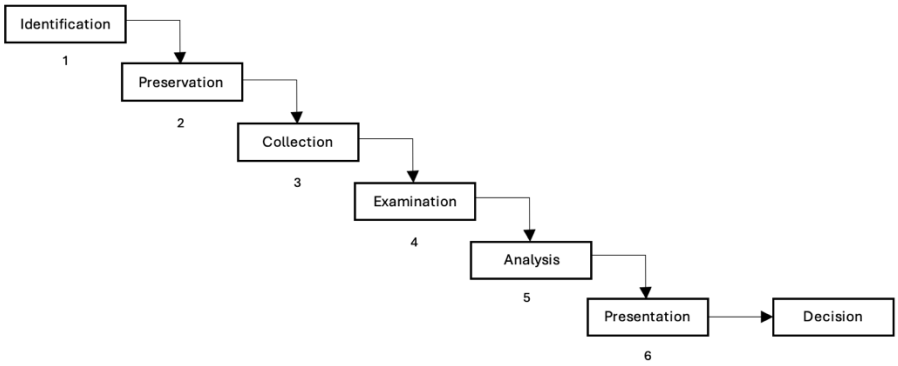
Metode *ELA (Error Level Analysis)* dapat digunakan sebagai salah satu tools untuk mendeteksi manipulasi pada sebuah citra digital dengan menampilkan area yang dicurigai [13]. Selain itu, *EXIF (Exchangeable Image File)* menyediakan informasi metadata teknis terkait citra digital, sedangkan metode *CD (Clone Detection)* melengkapi *ELA* dengan kemampuan memetakan area yang di-*copy-paste* [14]. Penelitian Hasan Bisri (2023) menunjukkan bahwa ketiga metode ini—*ELA*, *EXIF*, dan *CD*—yang digunakan dalam aplikasi *Forensically Beta*, efektif dalam mendeteksi manipulasi pada gambar digital. Hasil penelitian mencatat tingkat keberhasilan masing-masing metode: ELA 94,6% dalam mendeteksi perbedaan piksel yang mencurigakan, CD 94% dalam mengidentifikasi area yang di-*copy-paste*, dan EXIF 98,3% dalam memeriksa perubahan metadata teknis, sehingga ketiganya berkontribusi secara signifikan dalam forensik citra digital. Namun, metode ini juga memiliki kekurangan, seperti *ELA* yang kurang akurat pada gambar terkompresi, *CD* yang memerlukan waktu lebih lama untuk analisis, dan *EXIF* yang tidak berguna jika metadata telah dihapus atau diubah [15]. Penelitian lainnya menggunakan metode *NIST* yang sesuai dengan Standar Nasional Indonesia (SNI) 27037:2014 untuk mengidentifikasi keaslian gambar sebagai barang bukti. Aplikasi yang digunakan adalah *Metadata++*, alat *offline* untuk menganalisis metadata gambar. Penelitian ini menunjukkan adanya perbedaan metadata antara foto asli dan foto hasil manipulasi, seperti perubahan dalam atribut *ModifyDate* dan penggunaan perangkat lunak *Adobe Photoshop* untuk pengeditan, yang mengindikasikan gambar telah diedit [16].

Penelitian ini berfokus pada analisis forensik citra di *platform X* menggunakan metode *Digital Forensic Research Workshop (DFRWS)*. Berbeda dari penelitian sebelumnya yang menggunakan metode forensik *NIST* dengan alat *Metadata++* untuk mengidentifikasi keaslian gambar berbasis *metadata*, penelitian ini menerapkan metode DFRWS yang mencakup tahap identifikasi, pemeliharaan, pengumpulan, pemeriksaan, analisis, dan presentasi untuk mendeteksi manipulasi pada gambar. Selain itu, penelitian ini menggunakan *platform online FotoForensic* yang memiliki fitur analisis lebih mendalam untuk mendeteksi perubahan pada gambar yang diunggah di media sosial, sehingga lebih sesuai dalam konteks *platform* dinamis seperti *X*. Teknik manipulasi yang sudah semakin berkembang, maka diperlukan suatu metode forensik yang dapat memecahkan masalah tersebut, salah satunya adalah menggunakan metode *Digital Forensic Research Workshop* (DFRWS). Beberapa *tools* yang dapat digunakan untuk proses tersebut adalah *MOBILedit Forensic Express*, *Fotoforensic* dan *ForensicallyBeta.*

Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

2. METODE PENELITIAN

Metode *Digital Forensic Research Workshop (DFRWS)* mencakup beberapa tahapan penting yang memungkinkan penyelidik mengikuti langkah-langkah yang konsisten dan dapat diandalkan saat melakukan investigasi. Tahapan ini bertujuan untuk mengidentifikasi, memelihara, mengumpulkan, memeriksa, menganalisis, dan menyajikan bukti digital. Setiap tahap memiliki peran dan fungsi khusus yang membantu memastikan bahwa seluruh proses forensik dilakukan dengan benar, mulai dari awal hingga akhir. Tahapan-tahapan ini disajikan dalam Gambar 1, yang memberikan gambaran visual mengenai alur kerja dari metode *Digital Forensic Research Workshop (DFRWS)* serta menunjukkan urutan setiap langkah yang harus diikuti selama investigasi berlangsung [17].



Gambar 1. Skema Metode *Digital Forensic Research Workshop* (DFRWS)

Metode ini terdiri dari enam tahapan penting: identifikasi, pemeliharaan, pengumpulan, pemeriksaan, analisis, dan presentasi. Tahap pertama, identifikasi, melibatkan pengenalan barang bukti dan sumber data yang relevan untuk menyelidiki kasus tertentu, sehingga penyelidik dapat menentukan informasi spesifik yang diperlukan dalam proses investigasi. Pemeliharaan, sebagai tahap kedua, bertujuan untuk melindungi keutuhan bukti digital, memastikan keasliannya, dan mencegah perubahan yang tidak diinginkan. Proses ini dilakukan dengan langkah-langkah seperti isolasi perangkat atau data yang berfungsi menjaga bukti tetap asli [18].

Tahap pengumpulan dilakukan dengan mengambil barang bukti dari perangkat atau sumber terkait secara hati-hati, didokumentasikan secara menyeluruh untuk menjaga jejak bukti dan memastikan data dapat ditelusuri kembali. Selanjutnya, tahap pemeriksaan adalah proses penyaringan data yang diambil sehingga penyelidik dapat berfokus pada informasi penting tanpa mengubah isi asli data, menjaga keaslian konten agar tetap valid [19].

Pada tahap analisis, data dianalisis mendalam untuk menentukan dari mana data berasal, siapa yang membuatnya, bagaimana dan mengapa data tersebut dihasilkan. Analisis ini bertujuan untuk memahami bukti dalam konteks kasus yang diselidiki dan memberikan wawasan yang diperlukan untuk rekonstruksi peristiwa. Tahap terakhir adalah presentasi, di mana hasil analisis disajikan dalam bentuk yang jelas dan sistematis, termasuk penjelasan alat dan metode yang digunakan. Pada tahap ini, juga diberikan rekomendasi untuk perbaikan kebijakan, metode, atau aspek-aspek lain yang mendukung proses forensik digital. Presentasi ini memastikan bahwa bukti dapat dipahami oleh pengunjung dan diterima dalam konteks hukum [20].

3. HASIL DAN PEMBAHASAN

Penelitian ini menggunakan metode *Digital Forensic Research Workshop (DFRWS)* yang mempunyai tahapan yang cukup lengkap untuk menjalankan proses forensik dan sering digunakan oleh penyidik forensik. DFRWS mempunyai pendekatan ilmiah yang didasarkan pada prinsip-prinsip yang terbukti efektif untuk melakukan pemeliharaan, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi, dan penyajian bukti digital dari sumber digital. Tujuannya adalah untuk membantu atau memfasilitasi rekonstruksi kejadian yang melibatkan tindak pidana, atau mendukung pencegahan tindakan ilegal yang dapat mengganggu operasi yang direncanakan.

Metode *DFRWS* ini terdiri dari enam tahapan utama, yaitu identifikasi, pemeliharaan, pengumpulan, pemeriksaan, analisis, dan presentasi. Tahapan identifikasi dilakukan untuk mencari informasi dari kasus-kasus sebelumnya sebagai referensi untuk memahami barang bukti yang sedang dicari. Selanjutnya dilakukan identifikasi mengenai cara kerja dalam kasus pemalsuan gambar yang mungkin digunakan. Simulasi kasus pemalsuan gambar dilakukan untuk menemukan bukti digital yang relevan. Setelah bukti digital diperoleh,

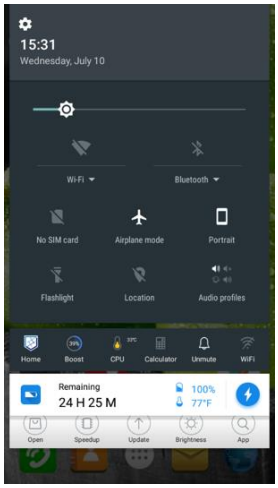
Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

proses identifikasi dilanjutkan ke tahap pemeliharaan sesuai dengan kerangka kerja metode *DFRWS*. Laporan pemalsuan gambar dideskripsikan pada Tabel 1.

Tabel 1. Laporan Pemalsuan Gambar

Tersangka/Korban	Kasus
Longki Djanggola	Dalam koran *Mercusuar*, terdapat tangkapan layar hasil seseorang menyunting judul sebuah artikel menjadi "Longki Djanggola Membiayai Aksi *People Power* di Sulteng"
Ahok	Dalam koran Kompas, seseorang menyunting judul sebuah artikel menjadi "Ahok: Kamu kira kami NIAT bangun masjid dan naikkan haji marbut?"

Tabel 1 merupakan contoh laporan pemalsuan gambar yang sudah pernah terjadi. Kemudian tahap kedua dalam metode forensik adalah *preservation*, yang berfokus pada pemeliharaan untuk menjaga keaslian barang bukti digital dan mencegah tuduhan menjadi bukti bahwa hasil gambar telah mengalami sabotase. Proses ini melibatkan langkah-langkah untuk memastikan integritas barang bukti tetap utuh dan tidak rusak, termasuk teknik isolasi barang bukti fisik dan pembuatan cadangan data dalam bentuk kloning atau *image file* dari barang bukti. Dalam konteks penyelidikan ini, langkah isolasi dilakukan dengan memisahkan perangkat *smartphone* dari segala bentuk komunikasi. Isolasi ini penting untuk mencegah hal-hal yang dapat merusak bukti digital atau memengaruhi integritas data yang tersimpan di dalamnya. Salah satu langkah isolasi yang dilakukan adalah dengan mengaktifkan *Mode* Pesawat pada perangkat, seperti ditunjukkan pada Gambar 2, untuk memastikan perangkat tidak terhubung dengan jaringan yang bisa mengubah data.



Gambar 2. Proses Isolasi koneksi *Smartphone*

Pada Gambar 2 dilakukan cara mengisolasi koneksi pada *smartphone* dengan tahapan mengumpulkan hasil identifikasi bagian barang bukti digital berbentuk *smartphone* yang dilakukan secara khusus serta mengidentifikasi sumber datanya. Proses identifikasi dan pengumpulan data ini menggunakan *smartphone merk Evercross* yang ditunjukkan pada Gambar 3.

Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

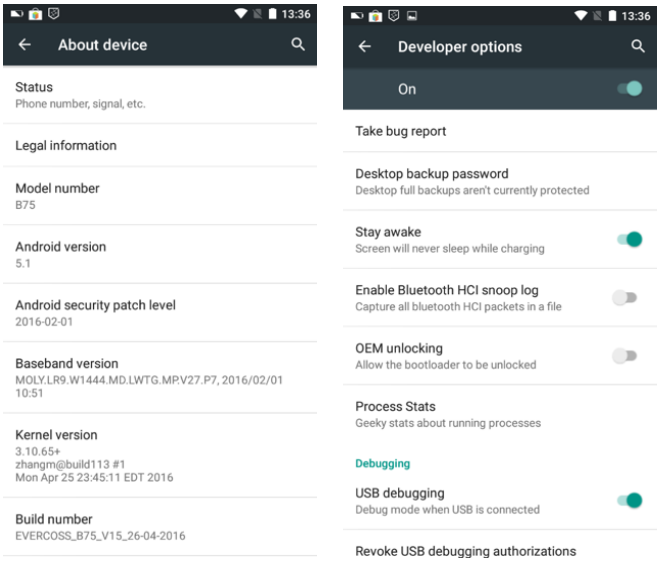
Gambar 3. Perangkat *Smartphone* yang digunakan

Pada Gambar 3, *smartphone* mempunyai spesifikasi yang khusus sehingga dapat digunakan dalam penelitian. Kekhususan pada *smartphone* ditunjukkan pada merek, seri, mode, dan *processor.* Adapun deskripsi khusus pada *smartphone* yang digunakan pada penelitian ini dideskripsikan pada Tabel 2.

Tabel 2. Spesifikasi *Smartphone*

Deskripsi	Spesifikasi
Merek	Evercross
Seri	Elevote
Model	Y3+
IMEI	358441061746404
OS	Android
Versi OS	5.1 (Lolipop)
Processor	Quad Core 1.0 GHz

Tabel 2 merupakan spesifikasi *smartphone* yang digunakan sebagai percobaan. Tahap berikutnya adalah pengumpulan, di mana dilakukan identifikasi secara spesifik terhadap bagian-bagian dari barang bukti digital dan penentuan sumber data. Barang bukti pada penelitian ini merupakan sebuah perangkat *smartphone* merek *Evercross*, seperti ditampilkan pada Gambar 3. Dalam tahap ini, diaktifkan *Developer Options* pada perangkat untuk memungkinkan proses forensik. Aktivasi *Developer Options* dilakukan dengan menekan opsi *"Build Number"* pada perangkat sebanyak tujuh kali, sebagaimana ditunjukkan dalam Gambar 4.



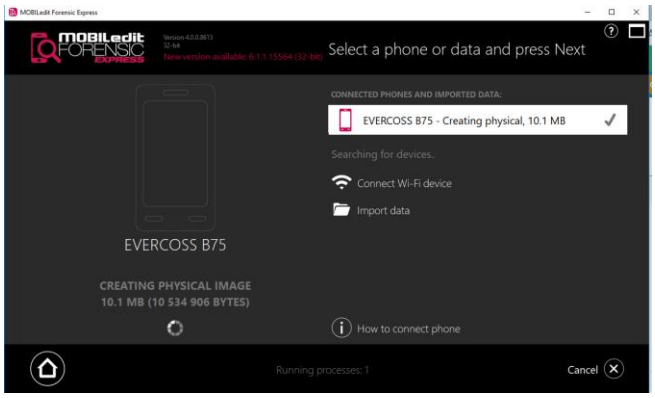
Gambar 4. *Build Number Smartphone*

Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

Setelah *Developer Options* diaktifkan, langkah selanjutnya adalah mengaktifkan opsi *Stay Awake* dan *USB Debugging*. Opsi *Stay Awake* bertujuan agar perangkat tetap aktif dan tidak masuk ke *mode sleep* saat proses forensik sedang berlangsung, karena *mode sleep* dapat mengaktifkan fitur keamanan perangkat. Sementara itu, *USB Debugging* memungkinkan perangkat *smartphone* untuk berkomunikasi dengan komputer *workstation* melalui kabel USB, menggunakan ADB *(Android Debug Bridge)* untuk akses forensik.

Gambar 4 merupakan *build number* pada *smartphone* yang digunakan untuk uji coba. Pada proses ini, keamanan bukti digital dari *smartphone* mempunyai resiko yang cukup berbahaya diakibatkan oleh kesalahan pengambilan bukti digital, seperti hilangnya data atau rusaknya bukti digital sehingga tidak bisa dibaca. Oleh sebab itu, perlu adanya proses mencadangkan data *smartphone* yang digunakan sebagai barang bukti, yang dapat disebut juga dengan *digital evidence preservation.* Selanjutnya, proses *logical acquistion* dibutuhkan untuk mencadangkan bukti digital dengan menggunakan *MOBILedit Forensic Express*. Alat ini mampu untuk membuat cadangan dari sistem *smartphone* dan mengekstrak data yang terdapat di dalamnya.

Gambar 5 menunjukkan tahapan *backup* pada perangkat *smartphone* dengan menggunakan *MOBILedit Forensic Express*, di mana proses ini dilakukan untuk mengamankan data sebelum analisis lebih lanjut.



Gambar 5. Proses Pencadangan *Smartphone*

Gambar 5 membahas tentang proses backup menggunakan *MOBILedit Forensic.* Dari proses ini dihasilkan file image dari *smartphone* yang memiliki ekstensi *.img* dengan ukuran *file* yang bervariasi tergantung pada jumlah data yang tersimpan di *smartphone* tersebut.

Gambar 6 menunjukkan hasil *backup* yang diperoleh dari proses ini. *File image* ini disimpan untuk keperluan analisis lebih lanjut tanpa mengubah data asli yang ada di perangkat.

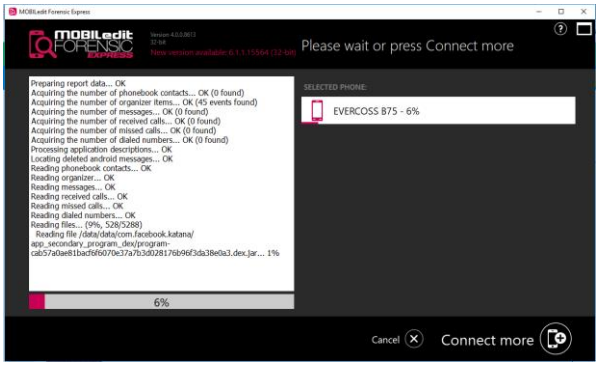
Name	Date modified	Type	Size
EVERCOSS B75 (2019-07-09 17h01m00s)	7/9/2019 5:30 PM	File folder	
samsung SM-G130H (2019-07-08 22h03...	7/8/2019 10:29 PM	File folder	
EVERCOSS B75	7/9/2019 4:53 PM	Disc Image File	15,267,840 ...
EVERCOSS B75.img_info	7/9/2019 4:53 PM	WinRAR ZIP archive	3 KB
samsung SM-G130H	7/8/2019 9:58 PM	Disc Image File	3,817,472 KB
samsung SM-G130H.img_info	7/8/2019 9:58 PM	WinRAR ZIP archive	2 KB

Gambar 6. Hasil proses *backup Smartphone*

Gambar 6 merupakan hasil *backup* yang berupa *file Disc* serta *folder* yang didalam berisi data-data *smartphone*. Setelah *backup* selesai dilakukan, langkah berikutnya adalah mengekstrak data dari *file image* tersebut menggunakan perangkat lunak *MOBILedit Forensic Express*. *Smartphone* terlebih dahulu dihubungkan dengan komputer yang sudah terinstal *MOBILedit Forensic Express*.

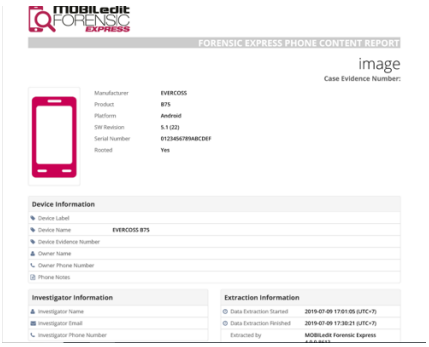
Gambar 7 memperlihatkan cara mengekstraksi data yang sedang berlangsung. Proses ini memungkinkan penyelidik untuk mengakses data yang ada di *smartphone* tanpa harus langsung berinteraksi dengan perangkat aslinya, sehingga keaslian data tetap terjaga.

Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index



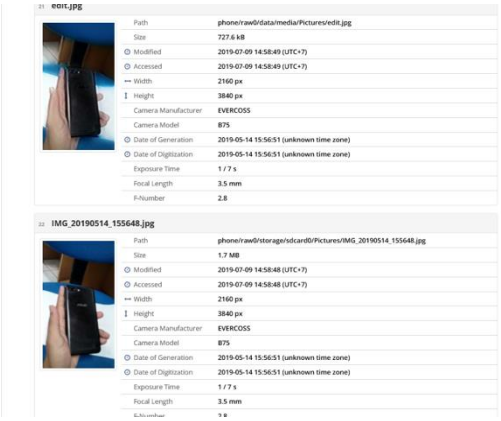
Gambar 7. Proses Ekstraksi Data *Smartphone*

Gambar 7 merupakan proses ekstraksi data menggunakan *MOBILedit Forensic*. Selanjutnya, laporan dibuat untuk menampilkan hasil dari proses ekstraksi data *smartphone. Format .pdf* digunakan untuk menampilkan hasil laporan akhir dengan tampilan bukti forensik pada Gambar 8.



Gambar 8. *Full Report MOBILedit Smartphone* 1

Pada Gambar 8 ditunjukkan tampilan laporan berupa *PDF* dari *MOBILedit*. Dari hasil proses esktraksi didapatkan laporan utuh bahwa terdapat 39 *file* gambar, seperti informasi spesifikasi *smartphone* dan *processor*. Gambar 8 menunjukkan informasi *file* yang lebih spesifik dan jelas.



Gambar 9. Contoh File Gambar yang Didapat

Setelah mendapatkan bukti gambar, seperti yang ditunjukkan pada Gambar 9, langkah selanjutnya adalah mencari gambar yang sesuai dengan unggahan pelaku di *X* dalam menjalankan aksinya. Contoh kasus dalam penelitian ini adalah penipuan penjualan *smartphone* dengan memperhalus tampilan *smartphone* sehingga terlihat tanpa kerusakan. Gambar 10 merupakan gambar dan postingan pelaku.

Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

Gambar 10. postingan pelaku

Gambar 10 merupakan contoh unggahan dari pelaku. Setelah melakukan analisis pada gambar yang diperoleh, ditemukan dua gambar yang memiliki kemiripan dengan gambar yang diunggah oleh pelaku di *X*. Selanjutnya, dilakukan analisis lebih mendalam terhadap kedua gambar ini untuk mengidentifikasi lebih lanjut kesamaan dan perbedaan yang mungkin ada. Gambar 11 menampilkan kedua gambar yang berhasil diidentifikasi sebagai hasil dari analisis tersebut. Analisis ini bertujuan untuk mencari tahu apakah kedua gambar ini adalah versi asli atau hasil manipulasi, serta memberikan wawasan lebih lanjut mengenai teknik atau metode yang mungkin digunakan pelaku dalam proses penyuntingan gambar sebelum diunggah di media sosial.

(a) Foto Pertama

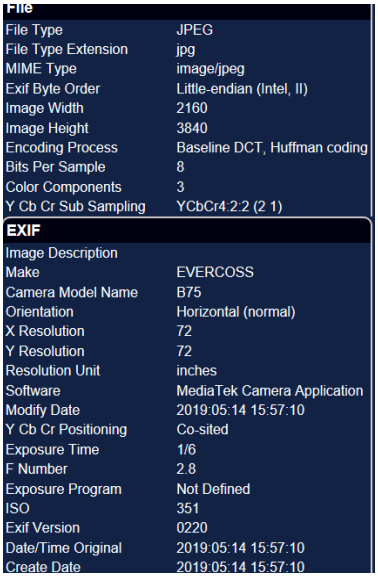
(b) Foto Kedua

Gambar 11. Foto yang Mirip dengan Unggahan

Gambar 11 merupakan 2 foto yang mirip dari hasil laporan. Tahap pertama dalam proses analisis keaslian sebuah gambar adalah dengan melakukan deteksi *metadata* pada gambar tersebut. *Metadata* adalah informasi tambahan yang tersimpan dalam *file* gambar dan dapat mencakup berbagai detail, seperti waktu pengambilan, jenis kamera, pengaturan lensa, hingga informasi perangkat lunak yang digunakan untuk mengedit gambar. Untuk mendeteksi metadata ini, digunakan alat khusus bernama *FotoForensic (fotoforensic.com)*, yang menyediakan fitur analisis metadata secara rinci. Melalui *FotoForensic*, dapat diketahui apakah gambar telah mengalami modifikasi atau manipulasi berdasarkan jejak digital yang tersimpan di *metadata.*

Pada penelitian ini, hasil analisis *metadata* dari dua gambar yang diuji terdapat pada Gambar 12 yang menunjukkan *metadata* foto pertama dan Gambar 12 menunjukkan *metadata* foto kedua. Kedua gambar tersebut diperiksa untuk mengidentifikasi perbedaan atau perubahan yang mungkin terjadi dalam proses penyuntingan. Pengecekan *metadata* pada kedua gambar ini memberikan petunjuk awal mengenai keaslian gambar, dengan informasi yang menunjukkan apakah gambar pernah disunting, perangkat lunak apa yang digunakan, serta detail teknis lain yang dapat mendukung proses investigasi lebih lanjut.

Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index



File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Little-endian (Intel, II)
Image Width	2160
Image Height	3840
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:2 (2 1)
EXIF	
Image Description	
Make	EVERCOSS
Camera Model Name	B75
Orientation	Horizontal (normal)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	MediaTek Camera Application
Modify Date	2019:05:14 15:57:10
Y Cb Cr Positioning	Co-sited
Exposure Time	1/6
F Number	2.8
Exposure Program	Not Defined
ISO	351
Exif Version	0220
Date/Time Original	2019:05:14 15:57:10
Create Date	2019:05:14 15:57:10

Gambar 12. *Metadata* Foto Pertama

Gambar 13. *Metadata* Foto Kedua

Gambar 12 memperlihatkan bahwa foto (a) merupakan foto asli karena *metadata* tidak menunjukkan adanya bukti penyuntingan. Sebaliknya, Gambar 13 menunjukkan *metadata* foto yang berisi informasi bahwa foto sudah melalui proses penyuntingan dengan *Adobe Photoshop* CC 2017. Informasi ini menunjukkan bahwa foto tersebut telah dimanipulasi.

Setelah keaslian kedua foto ditentukan, proses mencari bukti manipulasi dengan membandingkan kedua foto dengan alat *FotoForensic (fotoforensic.com)* dan *ForensicallyBeta (29a.ch/photo-forensik)* perlu dilakukan. Analisis terhadap foto pertama (asli) ditunjukkan oleh Gambar 14, sedangkan Gambar 15 menunjukkan analisis pada foto kedua (hasil penyuntingan). Gambar 15.a hanya tergambar warna hitam dengan sedikit goresan yang merupakan foto yang dianalisis, sedangkan Gambar 15.b merupakan hasil analisi *Forensic Beta* yang menunjukkan lebih banyak warna untuk mengidentifikasi keaslian foto.

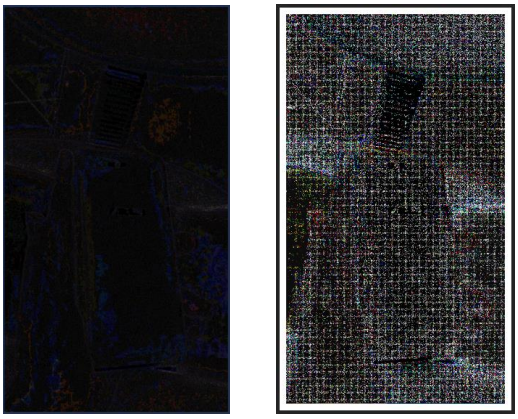
(a)*FotoForensic*

(b)*ForensicallyBeta*

Gambar 14. Analisis Foto Asli

Setelah kedua foto dianalisis menggunakan kedua alat tersebut, hasilnya terlihat pada Gambar 14 untuk foto asli dan Gambar 15 untuk foto yang sudah diedit. Dari perbandingan ini, perbedaan yang mencolok terlihat, khususnya dalam analisis menggunakan *FotoForensic* dengan teknik *Level Error Analysis (ELA).*

Idealis: Indonesia Journal Information System
Volume 8, Nomor 1, Januari 2025
ISSN 2684-7280 (*online*)
Halaman 10 - 20
available online at http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index



(a)*FotoForensic* (b)*ForensicallyBeta*

Gambar 15. Analisis Foto Asli

Perbedaan tersebut, salah satunya, dapat dilihat pada perubahan piksel di area objek *smartphone*, serta area lain yang berbeda dari foto asli, yang menunjukkan adanya manipulasi. Dalam analisis menggunakan *ForensicallyBeta*, juga terlihat perbedaan piksel di beberapa bagian yang menunjukkan adanya *noise* tambahan, yang mengindikasikan bahwa foto tersebut telah diedit di bagian-bagian tertentu.

4. KESIMPULAN

Analisis *image forensic* dengan metode *Digital Forensic Research Workshop (DFRWS)* memperoleh kesimpulan bahwa dari bukti digital didapatkan beberapa gambar yang terkait dengan simulasi kasus yang dibahas. Proses ekstraksi dilakukan dengan *tool MOBILedit Forensic Express* dan menggunakan perangkat *smartphone EVERCROSS*. Berdasarkan bukti digital melalui dua alat forensik diperoleh Kesimpulan bahwa *FotoForensic* mendapatkan isi metadata dari foto yang didapat, dimana foto kedua merupakan foto editan karena terdapat indikasi pernah diedit menggunakan *Adobe Photoshop* CC 2017. Selain untuk mengecek metadata, *FotoForensic* dapat digunakan untuk analisis bagian foto yang pernah dilakukan penyuntingan, sehingga dapat disimpulkan *FotoForensic* memiliki kinerja yang baik dalam mendeteksi keaslian foto. Sedangkan, *ForensicallyBeta* dapat digunakan untuk analisis bagian foto yang pernah diedit dengan berbagai teknik, seperti *Error Analysis Technique, Noise Analysis, Clone Detection dan JPEG Analysis*. Selanjutnya, untuk menemukan bukti forensic digital yang lebih kompleks, perlu dilakukan penelitian dengan menggunakan *device* dan *tools* yang lain untuk memberikan gambaran dan hasil yang berbeda, sehingga dapat diperoleh bahwa uji forensik dapat dilakukan secara variatif.

DAFTAR PUSTAKA

[1] W. Y. Sulistyo, I. Riadi, and A. Yudhana, "Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital," *JUITA J. Inform.*, vol. 8, no. 2, p. 179, 2020, doi: 10.30595/juita.v8i2.6602.

[2] I. Riadi, A. Yudhana, and W. Y. Sulistyo, "Analisis Perbandingan Nilai Kualitas Citra pada Metode Deteksi Tepi," *Rekayasa Sist. dan Teknol. Inf.*, vol. 4, no. 2, pp. 345–351, 2020.

[3] Rizal Adi Saputra, Jumadil Nangi, Ika Purwanti Ningrum, M. F. Almaliki, and La Ode Rahmat Andre Pratama, "Deteksi Uang Palsu Rupiah dengan Menggunakan Metode Deteksi Tepi Laplacian of Gaussian (LoG) dan Algoritma K-Means Clustering," *J. Buana Inform.*, vol. 13, no. 02, pp. 85–92, 2022, doi: 10.24002/jbi.v13i02.5448.

[4] D. Ulag, S. A. S. Sekeon, and B. T. Ratag, "Hubungan Antara Kecanduan *Smartphone* Dengan Kualitas Tidur Peserta Didik Smp Negeri 12 Dumoga," *J. KESMAS*, vol. 11, no. 4, pp. 14–21, 2022.

[5] W. Y. Sulistyo *et al.*, "Analisis Perbandingan Kualitas Kompresi Citra Digital pada Media Sosial," *J. Ris. Teknol. Inf. dan Komput.*, vol. 2, no. 1, pp. 1–6, 2022, doi: 10.53863/juristik.v2i1.473.

[6] Wicaksono Yuli Sulistyo, Imam Riadi, and Anton Yudhana, "Comparative Analysis of Image Quality Values on Edge Detection Methods," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 2, pp. 345–351, 2020, doi: 10.29207/resti.v4i2.1827.

[7] I. Zuhriyanto, Anton Yudhana, and Imam Riadi, "Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 829–836, 2020, doi: 10.29207/resti.v4i5.2152.

[8] I. Sudianto and N. Anwar, "Analisa Forensik Citra Menggunakan Metode Error Level Analysis dan Block Matching," *JSTIE (Jurnal Sarj. Tek. Inform.*, vol. 11, no. 1, p. 40, 2023, doi: 10.12928/jstie.v11i1.25714.

[9] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di

Indonesia (Systematic Review)," *J. Telekomun. dan Komput.*, vol. 9, no. 3, p. 186, 2020, doi: 10.22441/incomtech.v9i3.7210.

[10] Muhammad Abdul Aziz, Wicaksono Yuli Sulistyo, and Sri Rahayu Astari3, "Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO)," *JURISTIK (Jurnal Ris. Teknol. Inf. dan Komputer)*, vol. 1, no. 01, pp. 8–15, 2021, doi: 10.53863/juristik.v1i01.341.

[11] M. Ali Diko Putra, A. Wirawan Muhammad, B. Parga Zen, R. Yunita Kisworini, and T. Rohayati, "Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86," *J. Sist. Inf. Galuh*, vol. 2, no. 1, pp. 44–54, 2024, doi: 10.25157/jsig.v2i1.3695.

[12] K. Eka Purnama, C. Rozikin, and A. Ali Ridha, "Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode Nist," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 2, pp. 1100–1107, 2023, doi: 10.36040/jati.v7i2.6660.

[13] P. N. Candra and A. Prapanca, "Klasifikasi Gambar Asli dan Manipulasi Menggunakan Error Level Analysis (ELA) Sebagai Proses Komputasi Metode Convolutional Neural Network (CNN)," *J. Informatics Comput. Sci.*, vol. 2, no. 01, pp. 9–18, 2020, doi: 10.26740/jinacs.v2n01.p9-18.

[14] A. Apriliani, K. Hijjayanti, and S. Suhairoh, "Analisis Keaslian Citra Dengan Menggunakan Exif Metadata," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 5, no. 1, p. 84, 2020, doi: 10.24114/cess.v5i1.15600.

[15] H. Bisri and M. I. Marzuki, "Forensik Citra Digital Menggunakan Metode Error Level Analysis, Clone Detection dan Exif Untuk Deteksi Keaslian Gambar," *G-Tech J. Teknol. Terap.*, vol. 7, no. 2, pp. 586–595, 2023, doi: 10.33379/gtech.v7i2.2363.

[16] M. Fransiskus and N. P, "Analisis Digital Forensik Metadata pada Rekayasa Digital Image sebagai barang bukti Digital," *J. Sains Dan Komput.*, vol. 8, no. 01, pp. 1–5, 2024, doi: 10.61179/jurnalinfact.v8i01.439.

[17] I. Riadi, H. Herman, and I. A. Rafiq, "Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensik Research Workshop Framework," *Int. J. Artif. Intell. Res.*, vol. 6, no. 2, 2022, doi: 10.29099/ijair.v6i2.311.

[18] I. Riadi, H. Herman, and N. H. Siregar, "Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 3, pp. 489–502, 2022, doi: 10.30812/matrik.v21i3.1620.

[19] Sunardi, I. Riadi, and M. Hajar Akbar, "Penerapan Metode Static Forensik untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 3, pp. 576–583, 2020.

[20] I. Riadi, Herman, and N. H. Siregar, "Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework," *Ing. des Syst. d'Information*, vol. 27, no. 6, pp. 903–913, 2022, doi: 10.18280/ISI.270606.