IDENTIFIKASI BUKTI DIGITAL SISTEM PROPERTY PADA INSTAGRAM MENGGUNAKAN LIVE FORENSIK

Rizky Tri Amanah, Fahmi Fachri
Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen
Jl. Kutoarjo Km 05, Ds. Jatisari, Kab. Kebumen, Jawa Tengah 54317
rizkytriamanah07@gmail.com

ABSTRAK

Media sosial memiliki peran penting sebagai platform untuk mempromosikan dan menjual produk dagangan. Namun penggunaannya tidak hanya membawa dampak positif, tetapi juga dapat menimbulkan dampak negatif bagi pengguna, terutama jika dimanfaatkan sebagai sarana untuk melakukan tindak kejahatan, seperti penipuan melalui online. Salah satu penelitian yang digunakan untuk mengidentifikasi bukti kejahatan digital adalah dengan *Institut Standar dan Teknologi Nasional* (NIST). Penelitian ini bertujuan untuk mengungkap bukti digital yang telah dihapus menggunakan tools FTK Imager berdasarkan metode NIST. Selain itu, penelitian ini juga menunjukkan tingkat keberhasilan dalam mengungkap bukti digital menggunakan FTK Imager dalam kasus penipuan transaksi online. Bukti yang berhasil diperoleh berupa teks percakapan dan gambar antara tersangka dan korban, yang kemudian digunakan sebagai barang bukti digital terkait tindak pidana penipuan toko online. Proses pembuktian dilakukan dengan membandingkan dan menyinkronkan teks percakapan yang ditemukan pada laptop tersangka dengan percakapan yang terdeteksi.

Kata kunci : *Instagram, FTK Imager, Bukti Digital, NIST*

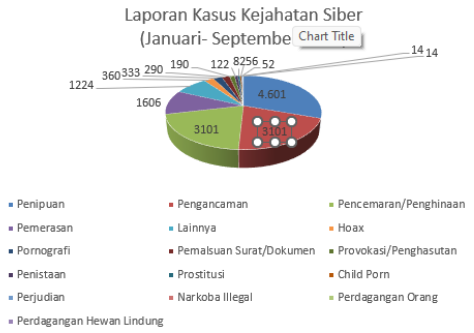
1. PENDAHULUAN

Perkembangan teknologi saat ini berlangsung dengan sangat cepat, membawa dampak signifikan terhadap berbagai aspek kehidupan manusia. Perkembangan yang pesat ini memberikan manfaat positif dengan meningkatkan efisiensi dan kemudahan dalam aktivitas sehari-hari. Seperti ada nya media sosial, media sosial adalah platform digital yang memungkinkan pengguna untuk berinteraksi, berbagi konten, dan membangun komunitas secara online. beberapa platform yang populer antara lain Facebook, Twitter, dan TikTok, Instagram. Media sosial digunakan untuk berbagai tujuan, baik untuk komunikasi pribadi, pemasaran, hingga berbagi informasi. Pengguna dapat berbagi berbagai jenis konten, seperti teks, gambar, video, dan audio.[1]

Aplikasi Instragram termasuk salah satu jenis media soial yang sangat banyak digunakan disetiap negara dan merupakan yang populer di dunia, secara umum instagram merupakan sebuah aplikasi yang dapat dipergunakan sebagai nedia berbagi foto dan video, tak hanya itu instagram juga dapat digunakan dalam kegiatan jual beli online yang tidak harus bertemu langsung dengan konsumen, namun kegiatan jual beli secara online dapat menimbulkan dampak positif maupun negatif, dampak negatif dari Jual beli online yaitu karena pembeli dan penjual tidak bertemu secara langsung dan tidak bisa melihat dan menyetuh barang secara langsung sering terjadi penipuan online. Contoh dari penipuan jual beli online biasanya barang yang datang ke pembeli tidak sesuai dengan apa yang ditampilkan di awal, atau tidak seperti yang pembeli inginkan [1].

Untuk memberikan hukum dalam mengatisipasi kejahatan cyber di Indonesia telah diberlakukan UU 11/2008 tentang Informasi dan Transaksi Elektronik (ITE) yang sudah berubah menjad.i UU 19/2016. Adanya Undang-Undang tersebut juga menjadi solusi dan pengakuan bahwa alat bukti elektronik dapat menjdai alat bukti yang sah dalam penyelidikan sebagaimana tertulia pada Pasal 54 Ayat(1) dan Legalitas dari alat bukti yang tertulis juga dalam Pasal 5 [2].

Berikut data kasus kejahatan siber yang terjadi di Indoneisa dalam rentang waktu Sembilan bulan yaitu pada Januari hingga September tahun 2021.



Gambar 1. Diagram data kasus kejahatan siber yang (sumber dari Katadata.co.id)

Berdasarkan data yang diperoleh dari Katadata.co.id, pada tahun 2021, kasus penipuan menjadi jenis kejahatan yang paling banyak terjadi di Indonesia. Dalam rentang waktu sembilan bulan, yaitu dari Januari hingga September tahun 2021, tercatat sebanyak 4.601 kasus penipuan. Tingginya angka ini menunjukkan bahwa Indonesia sangat rentan terhadap kejahatan penipuan. Penipuan dapat terjadi karena berbagai faktor, diantaranya yaitu Kurangnya kewaspadaan dalam bertransaksi digital dan Rendahnya literasi teknologi masyarakat.

Contoh kasus Penipuan Toko Online Palsu modus ini melibatkan akun yang mengaku sebagai toko online terpercaya dan menjual berbagai produk dengan harga menarik. Korban diminta untuk mentransfer uang sebagai pembayaran, tetapi barang yang dijanjikan tidak dikirim. Setelah menerima uang, akun tersebut menghilang dan memblokir korbannya. Dalam penyelidikan kasusnya walaupun si penipu berusaha menghilangkan jejak dan bukti digital tetapi pembuktian tetap bisa ditampilkan [3]

Jejak dan bukti digital yang ditemukan pada kasus penipuan toko online palsu harus di analisa dengan menggunakan ilmu dan metode forensik. Analisa forensik terhadap jejak dan bukti digital di bidang teknologi juga dikenal *sebagai forensic digital*. *Forensic digital* pada dasarnya yaitu mencari bukti-bukti digital yang diperlukan untuk mengungkap kejahatan yang sedang diselidiki dan mengacu pada terjadiinya kejahatan. Biasanya bukti ditigal dapat di tersimpan pada penyimpanan yang bersifat permanen maupun sementara [4].

Adanya barang bukti yang kemudian dapat menunjukan peristiwa kejahatan yang telah terjadi sehingga dapat digunakan sebagai petunjuk dalam mengungkap kasus yang sedang di diusut dengan kronologis yang lengkap. Ada dua klasifikasi barang bukti yang dihasilkan dari forensic digital yaitu barang bukti digital dan barang bukti elektronik, barang bukti digital bersifat digital yang diekstrak atau di *recover* dari barang bukti elektronik, sedangkan barang bukti digital elektronik biasanya berupa penyimpanan yang dapat dilkenali secara visual, salah satu dari barang bukti elektronik yaitu bukti pesan *Instagram.*

Dalam melaksanakan analisis *forensik digital*, penggunaan aplikasi atau *tools* sangat penting untuk mendukung kelancaran proses investigasi dan menghasilkan data yang akurat. Berbagai aplikasi tersedia untuk mempermudah analisis *forensik digital*, baik yang bersifat gratis maupun berbayar. Beberapa contoh aplikasi yang dapat digunakan untuk membantu menemukan bukti digital meliputi *FTK Imager*, *Autopsy*, dan berbagai *tools* lainnya yang dirancang khusus untuk kebutuhan *forensik digital [5]*

2. TINJAUAN PUSTAKA

2.1. Digital Forensik

Digital forensik adalah ilmu yang mempelajari tentang bagaimana cara untuk menangani berbagai kejahatan yang melibatkan teknologi komputer, yang mana dalam hal ini untuk membuktikan kejahatan. *Digital forensic* pada dasarnya adalah untuk menemukan barang bukti digital yang bisa tersimpan pada penyimpanan komputer yang bersifat sementara maupun permanen [6].

Analisis forensik digital secara umum terbagi menjadi dua jenis, yaitu *dead forensics* dan *live forensics[7]*. *Dead forensics* adalah metode yang menganalisis data yang disimpan secara permanen di media penyimpanan. Sementara itu, *live forensics* merupakan teknik analisis yang fokus pada data yang sedang aktif atau berjalan dalam sistem, seperti data yang tersimpan di Random Access Memory (RAM) atau yang sedang bergerak melalui jaringan[8].

2.2. Analisis Bukti Digital

Analisis bukti digital adalah proses yang bertujuan untuk memeriksa barang bukti digital guna mendukung investigasi dalam kasus-kasus kejahatan yang melibatkan teknologi. Langkah ini juga memiliki peran penting dalam memastikan keakuratan bukti yang ditemukan, sehingga dapat mempermudah penyelidikan terhadap pelaku [9].

2.3. Instagram

Instagram adalah platform media sosial berbasis gambar dan video yang memungkinkan penggunanya untuk berbagi konten secara pribadi atau publik. Pengguna dapat mengunggah foto dan video, memberikan "like," mengomentari unggahan orang lain, serta menggunakan fitur seperti hashtag untuk mengkategorikan dan mempermudah pencarian konten. Selain itu, Instagram juga memungkinkan pembentukan komunitas digital, baik untuk tujuan sosial, bisnis, maupun pemasaran. Fitur lain yang ada termasuk geotagging, cerita singkat (stories), dan interaksi langsung dengan pengikut melalui pesan dan komentar. Instagram telah menjadi salah satu platform terpopuler untuk berbagi kehidupan sehari-hari, mempromosikan produk, dan berinteraksi dengan orang-orang di seluruh dunia[10].

2.4. FTK Imager

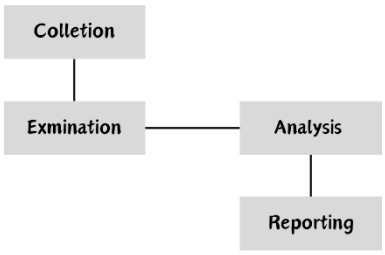
FTK Imager sebuah *software* yang digunakan untuk mendukung dalam mengoprasikan sistem akusisi data dalam dunia forensik digital yang di perbaharui oleh Perusahaan Access Data. Dalam pengumpulan data itu sendiri merupakan suatu sistem yang bertugas mengambil, mengumpulkan dan menyiapkan informasi yang cukup dan mengolah data untuk mendapatkan informasi yang dibutuhkan[11].

3. METODE PENELITIAN

3.1. Metode

Metode forensik salah satu factor penting dalam mendukung penyelidikan tindak kejahatan dengan lebih efesien dan efektif dalam menangani kasus[8] Metode NIST memiliki langkah dalam proses analisis data yaitu tahap pertama adalah identifikasi, di mana peneliti menentukan masalah atau tujuan yang akan diselesaikan dalam analisis, tahap kedua dimana pada tahap ini peneliti mengajukan solusi untuk menyelesaikan masalah hasil identifikasi pada tahap satu. Tahap ke tiga yaitu uji coba tahap untuk mendapatkan barang bukti digital dengan alat bantu dari *tools* forensik, tahap ke empat yaitu tahap evaluasi dimana peneliti mengevaluasi data yang sudah diperoleh dari tahap sebelumnya lalu menyimpulkannya hasil uji coba dari *tools* yang digunakan, untuk yang terakhir ada tahap laporan, dimana pada tahap ini peneliti membuat laporan hasil

evaluasi yang mencangkup metodologi forensik yang dilakukan , teknik dan *tools* yang digunakan[12]



Gambar 2. Tahapan Metode NIST

3.1.1. Pengumpulan (Collection)

Pencatatan spesifikasi barang bukti mencakup semua perangkat yang terlibat, yaitu laptop milik pelaku dan smartphone milik korban. Pengamanan barang bukti elektronik dan/atau digital harus dilakukan oleh orang yang memiliki kompetensi dibidang Forensik Digital. Barang bukti digital yang diamankan dalam bentuk berkas percakapan dalam bentuk raw data.

3.1.2. Pemeriksaan(Examination)

Tahap pemeriksaan dilakukan setelah data terkumpul. Data tersebut kemudian dianalisis untuk menemukan bukti-bukti yang berhubungan dengan tindakan kriminal yang dilakukan oleh pelaku.

3.1.3. Analisis(Analysis)

Pada tahap ini, hasil dari proses pemeriksaan dianalisis untuk mengidentifikasi konten atau file yang dapat dijadikan barang bukti. Dalam penelitian ini, bukti digital dianalisis menggunakan perangkat lunak FTK Imager, dengan fokus pada percakapan antara korban dan pelaku.

3.1.4. Pelaporan(Report)

Tahap pelaporan melibatkan rangkuman dari semua langkah yang telah dilakukan, mulai dari pencatatan waktu, proses pembuatan citra (imaging), hingga analisis. Proses ini juga mencakup perbandingan dan perhitungan antara file hasil ekstraksi dan file asli.

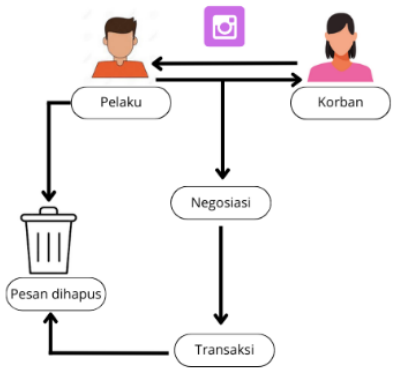
3.2. Alat dan Bahan

Alat yang digunakan pada penelitian ini yaitu berupa *Software* atau *Tools Forensic* serta *Hardware*. Berikut ini adalah spesifikasi dari setiap alat dan bahan yang digunakan.

Tabel 1. Alat dan bahan

Alat dan Bahan	Spesifikasi	Keterangan
Laptop	HP, Celeron(R), Windows 11, 64bit , RAM 4GB	Hardware
Smartphone	Redmi Note 12	Hardware
FTK imager	Versi 3.1.2.0	Software

3.3. Skenario Kasus



Gambar 3. Skenario Kasus Penipuan

Berikut merupakan alur simulasi kasusnya

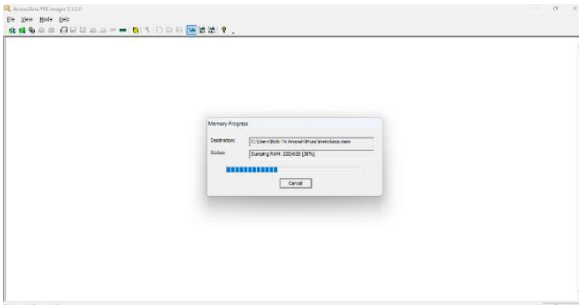
a. Korban melakukan chatting dengan pelaku
b. Korban melakukan negosiasi dengan pelaku
c. Korban melakukan transaski dan mengirim bukti transfer
d. Pelaku melakukan penipuan
e. Pelaku menghapus percakapan dengan korban
f. Korban merasa tertipu dan melapor kepada pihak berwajib.

Penelitian ini mengacu pada salah satu bentuk umum penipuan online shop, sebagaimana dijelaskan oleh Pratama Dahlian Persadha, pakar Riset Keamanan Siber. Skenario kasus akan dilakukan melalui simulasi percakapan antara pelaku dan korban. Dalam simulasi ini, pelaku menggunakan laptop, sementara korban menggunakan smartphone, untuk memungkinkan perbandingan. Percakapan yang sebelumnya dihapus oleh pelaku akan direkonstruksi menggunakan alat forensic.

4. HASIL DAN PEMBAHASAN

4.1. Collection

Pengumpulan barang bukti digital pada data yang tersimpan di RAM dilakukan menggunakan FTK Imager melalui fitur capture memory.



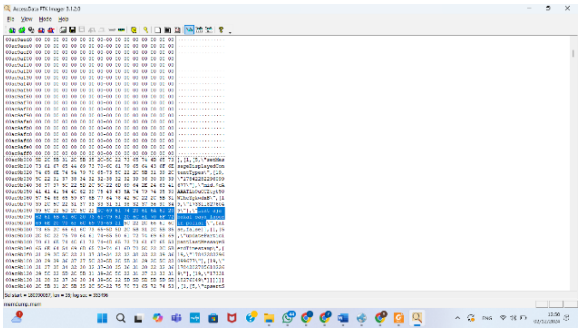
Gambar 4. Capture Memory

Pada Gambar 4 proses RAM Imaging digunakan untuk menyalin bukti digital tanpa mengubah data aslinya. Hasilnya berupa file dengan format .mem. Waktu yang dibutuhkan untuk proses ini dipengaruhi oleh kapasitas RAM semakin besar kapasitasnya,

semakin lama prosesnya, dan sebaliknya.

4.2. Examination

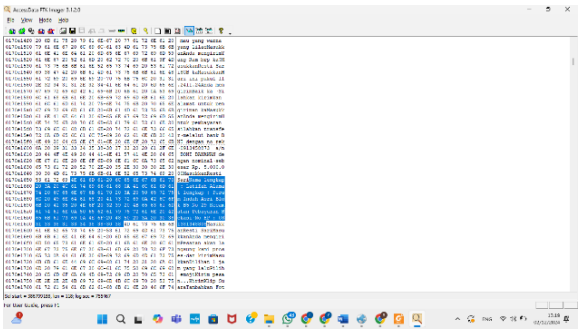
Pada tahap ini, berdasarkan pemeriksaan proses pencarian teks percakapan, penyidik menemukan rekaman data percakapan yang dilakukan dengan korban menggunakan FTK Imager. Alat ini membantu dalam proses pengumpulan bukti digital dengan cara mengekstraksi data secara menyeluruh dari perangkat yang digunakan.



Gambar 5.Bukti Digital yang ditemukan

4.3. Analysis

Pada tahap ini berdasarkan hasil yang diperoleh dari proses pengambilan data pada RAM. Beberapa bukti berupa teks percakapan berhasil ditemukan melalui FTK Imager.



Gambar 6. Bukti Data Digital

Berdasarkan hasil analisis data teks digital percakapan yang telah ditemukan akan dibandingkan dengan smartphone milik korban. Hasil menunjukkan percakapan Instagram Web yang dilakukan di laptop tersangka dengan smartphone korban. Dari perbandingan tesebut disimpulkan bahwa teks percakapan sama, sehingga penyidik menjadikan data percakapan tersebut sebagai bukti digital kasus penipuan.

Tabel 2. Bukti Digital

Isi Percakapan	Hasil
Samsung A55 ready ka?	✓
Ready ka mau yang type apa?	✓
Saya mau yang warna lilac Ram 8GB	✓
Baik ka Silahkan kirimkan alamat untuk pengiriman ka	✓
Untuk pembayaran silahkan transfer melalui bank BNI dengan no rek 0913458873 a/n DONI DANAWAN dengan nominal sebesar Rp. 5.000.000	✓
Nama lengkap : Latifah Alamat lengkap : Perum Indah Asri Blok B5 No 29 Kecamatan Pebayuran Bekasi No HP : 081381348808	✓
Pesanan akan langsung kami proses dan kirim	✓
Barangnya ko belum sampai ka udah 5 hari coba minta resinya	✓
Gaada resinya udah dikasih ke kurirnya	✓
Ko bisa gaada resinya? coba minta nomer hp kurirnya	✓
ya sabar lah kalo ga sabar gausah order disini	✓
Ko jadi sewot sih? Saya kan Cuma tanya barang yang saya pesen	✓
BALES WOY! Masukkan	✓
Penipuan ini namanya!	✓
BALIKIN UANG SAYA!	✓
Liat aja bakal saya laporin polisi!	✓

Pada Tabel 3 menampilkan sebuah percakapan yang terdapat pada laptop pelaku dan smartphone korban. Hasil yang diperoleh berupa bukti percakapan. Bukti digital yang ditemukan merupakan hasil dari perolehan menggunakan tools forensik yang membantu penyidik dalam menguak kasus penipuan online shop pada instagram web ini.

4.4. Reporting

Berdasarkan penipuan online shop di Instagram dibuktikan melalui analisis bukti digital, seperti percakapan di Instagram lewat windows yang di-cache. Informasi yang ditemukan meliputi waktu kejadian, akun Instagram pelaku dan korban, nomor HP korban, serta detail akun pelaku.

Tabel 3. Hasil Ideintifikasi Bukti Digital

Jenis Data	Ditemukan
Waktu kejadian	✓
Nama korban	✓
Nama Akun Korban	✓
Nama Ig Korban	✓
Nama Ig Pelaku	✓
Nomor Hp Korban	✓
Nomor Rekening Pelaku	✓
Nama Rekening Pelaku	✓
Total Kerugian Korban	✓

Pelaku dapat dijerat Pasal 378 KUHP tentang penipuan, dengan ancaman pidana penjara hingga empat tahun. Selain itu, sesuai Pasal 48 Ayat 1 sebagaimana Pasal 32 Ayat 1, pelaku yang menghilangkan barang bukti digital dapat dikenakan hukuman penjara hingga delapan tahun dan/atau denda maksimal Rp2 miliar.

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa analisis forensik digital menggunakan metode NIST dan tools FTK Imager berhasil mengungkap bukti-bukti digital dalam kasus penipuan online shop di Instagram. Melalui proses pengumpulan (collection), pemeriksaan (examination), analisis (analysis), dan pelaporan (reporting), peneliti berhasil menemukan dan merekonstruksi percakapan yang telah dihapus oleh pelaku melalui RAM imaging. Bukti digital yang ditemukan meliputi riwayat percakapan antara pelaku dan korban, detail transaksi, informasi rekening pelaku, serta informasi pribadi korban. Temuan ini membuktikan bahwa meskipun pelaku berusaha menghilangkan jejak digital dengan menghapus percakapan, data tersebut masih dapat diakses dan digunakan sebagai barang bukti. Pelaku dapat dikenakan sanksi hukum berdasarkan Pasal 378 KUHP tentang penipuan dengan ancaman pidana penjara hingga empat tahun, serta Pasal 48 Ayat 1 jo Pasal 32 Ayat 1 dengan ancaman hukuman penjara hingga delapan tahun dan/atau denda maksimal Rp2 miliar karena telah berusaha menghilangkan barang bukti digital.

DAFTAR PUSTAKA

[1] Vengga and Ariawan, "Pertanggungjawaban Platform Media Sosial Instagram sebagai Penyedia Layanan Iklan dalam Perkara Penipuan Berkedok Online Shop," *Jurnal Hukum Adigama*, vol. 4, no. 2, pp. 989–1012, 2021.

[2] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime," *Cyber Security dan Forensik Digital*, vol. 3, no. 2, pp. 12–21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[3] A. R. Thalib, F. A. Rabani, and A. L. K. Mufidah, "Proteksi Masyarakat Dalam Menyikapi Penipuan Giveaway di Media Sosial Instagram," *Prosiding Seminar Nasional Ilmu Ilmu Sosial (SNIIS)* , vol. 2, pp. 1403–1412, 2023, [Online]. Available: https://proceeding.unesa.ac.id/index.php/sniis/article/view/916

[4] N. Fatmah and R. Indrayani, "Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD," vol. 5, pp. 185–192, 2022.

[5] D. Julian, A. Wijaya, and T. Sutabri, "Perbandingan Kinerja Aplikasi Pengembalian Data Untuk Digital Forensik Dengan Metode National Institute of Standards and Technology," vol. 3, no. 1, pp. 210–218, 2023.

[6] R. A. Ramadhan, Abdul Kudus Zaini, and Jerika Mardafora, "Pelatihan Investigasi Digital Forensik," *Jurnal Pengabdian Masyarakat dan Penerapan Ilmu Pengetahuan*, vol. 3, no. 2, pp. 1–6, 2022, doi: 10.25299/jpmpip.2022.11003.

[7] W. Agustiono, D. Wulan Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," *Jurnal Teknologi dan Informasi (JATI)*, vol. 14, 2024, doi: 10.34010/jati.v14i2.

[8] M. H. Akbar and I. Riadi, "ANALISIS BUKTI DIGITAL PADA FLASH DISK DRIVE MENGGUNAKAN METODE GENERIC COMPUTER FORENSIC INVESTIGATION MODEL (GCFIM)," pp. 715–723, 2019.

[9] A. R. Triyanto and F. Fachri, "Analisis forensik bukti digital pada kejahatan pembunuhan berencana menggunakan metode national institute of justice," vol. 9, no. 2, pp. 1031–1042, 2024.

[10] I. D. Aryani and D. Murtiariyati, "Instagram Sebagai Media Promosi Dalam Meningkatkan Jumlah Penjualan Pada a.D.a Souvenir Project," *Jurnal Riset Akuntansi dan Bisnis Indonesia*, vol. 2, no. 2, pp. 466–477, 2022, doi: 10.32477/jrabi.v2i2.479.

[11] Amalia Yunia Rahmawati, "済無No Title No Title No Title," no. July, pp. 1–23, 2020.

[12] I. Riadi, Nasirudin, and Sunardi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 1, pp. 89–94, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/informatika89