Indonesian Journal of Multidisciplinary on Social and Technology
Homepage: https://journal.ilmudata.co.id/index.php/ijmst
Vol. 4 No. 3 (2026) pp: 1164-1173
P-ISSN: 2986-6790, e-ISSN: 2986-6782

Analisis Forensik Barang Bukti Promosi Judi Online Tiktok Live Gift Menggunakan NIST

Kaffin Feri Handi Yuwono[1], Fahmi Fachri[2]
[1,2] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Ma'arif Nahdlatul Ulama Kebumen
[1]kaffinyuwono@gmail.com *, [2]fahmifachriumnu@gmail.com

Abstract
This study aims to evaluate the effectiveness of the NIST SP 800-86 method in identifying digital traces of online gambling promotion on the TikTok Live Gift feature. The primary challenge in TikTok application forensics lies in the rapid data dynamics and the lack of standardized acquisition procedures. This research employs a qualitative approach through the systematic stages of the NIST framework, including collection, examination, analysis, and reporting. Data were acquired via the official Download Your Data feature and analyzed using FTK Imager, Autopsy, and Python automation scripts. The results demonstrate that the NIST SP 800-86 framework was successfully implemented with an artifact identification success rate of 85%, successfully reconstructing 17 out of 20 target artifacts with high validity, evidenced by hash value consistency and metadata completeness. Although limitations were identified regarding the availability of specific metadata, such as username, gift name, and timestamp within the official export files, this research provides a significant contribution by establishing a valid technical forensic procedure for law enforcement agencies. These findings serve as a crucial foundation for developing more comprehensive data acquisition methods to address increasingly complex cybercrime cases. The study confirms that platform data limitations do not constitute a methodological failure, but rather indicate a need for deeper physical acquisition techniques in social media forensic investigations.

Keyword: Digital Forensics, NIST SP 800-86, Online Gambling, Tiktok Live, Digital Evidence.

Abstrak
Penelitian ini bertujuan untuk mengevaluasi efektivitas penerapan metode NIST SP 800-86 dalam mengidentifikasi jejak digital terkait promosi judi *online* pada fitur *TikTok Live Gift*. Tantangan utama dalam forensik aplikasi *TikTok* terletak pada dinamika data yang sangat cepat serta belum adanya prosedur akuisisi data standar yang diakui. Penelitian ini menggunakan pendekatan kualitatif dengan mengikuti tahapan sistematis kerangka kerja NIST, yakni *collection*, *examination*, *analysis*, dan *reporting*. Data diakuisisi melalui fitur *Download Your Data* resmi dan dianalisis secara mendalam menggunakan perangkat lunak forensik FTK *Imager*, *Autopsy*, serta otomasi skrip pemrograman *Python*. Hasil penelitian menunjukkan bahwa metode NIST SP 800-86 berhasil diterapkan secara sistematis dengan tingkat keberhasilan identifikasi artefak digital mencapai 85%, di mana 17 dari 20 target artefak berhasil direkonstruksi dengan validitas tinggi yang dibuktikan melalui konsistensi nilai *hash* dan kelengkapan metadata. Meskipun ditemukan keterbatasan pada ketersediaan data spesifik seperti *username*, *gift name*, dan *timestamp* dalam berkas ekspor resmi, penelitian ini tetap memberikan kontribusi signifikan berupa prosedur teknis forensik yang valid bagi aparat penegak hukum. Temuan ini menjadi landasan penting bagi pengembangan metode akuisisi data yang lebih komprehensif di masa depan untuk menangani kasus kejahatan siber yang semakin kompleks. Penelitian ini membuktikan bahwa keterbatasan data *platform* bukanlah kegagalan metode, melainkan indikator kebutuhan teknik akuisisi fisik yang lebih mendalam pada investigasi forensik media sosial.

Kata Kunci: Digital Forensik, NIST SP 800-86, Judi *Online*, *Tiktok Live*, Bukti Digital.

1. Pendahuluan

Perkembangan teknologi informasi telah mengubah lanskap interaksi sosial dan transaksi digital masyarakat secara signifikan. Salah satu *platform* media sosial yang mengalami pertumbuhan pesat dan memiliki pengaruh besar adalah *TikTok*. Selain sebagai media berbagi video pendek, *TikTok* menyediakan fitur interaktif bernama *TikTok Live* yang memungkinkan pengguna melakukan siaran langsung secara *real-time*. Berdasarkan laporan terbaru dari *We Are Social* dan *Meltwater*, jumlah pengguna *TikTok* di Indonesia mencapai 194,37 juta orang per Juli 2025, angka ini menempatkan Indonesia di posisi teratas secara global (Nouvan, 2026). Namun, popularitas dan fitur interaktif *platform* ini juga membuka celah penyalahgunaan oleh pihak tidak bertanggung jawab, salah satunya sebagai media promosi ilegal, seperti situs judi *online*.

Dalam ekosistem *TikTok live*, terdapat fitur *gift* yang melibatkan transaksi virtual antar pengguna. Modus operandi yang marak terjadi saat ini adalah pelaku kejahatan memanfaatkan fitur tersebut dengan cara mengirimkan *gift* secara masif kepada penyiar (*streamer*). Alih-alih bertujuan sebagai apresiasi, pelaku sengaja mengubah nama akun (*username*) mereka menjadi nama situs judi *online* tertentu. Ketika *gift* dikirimkan, nama akun pelaku akan muncul secara otomatis di layar siaran, yang secara tidak langsung berfungsi sebagai ruang iklan/promosi gratis

bagi penonton siaran tersebut. Maraknya promosi ini sejalan dengan data Kementerian Komunikasi dan Informatika yang telah memblokir 2,6 juta situs judi *online* sejak 2018 hingga awal 2026 (Kemal, 2026). Hal ini menunjukkan bahwa pelaku terus mencari alternatif platform baru seperti *TikTok* untuk melancarkan promosinya. Meskipun aktivitas promosi ilegal melalui platform *TikTok* ini telah teridentifikasi, proses pembuktian digital pada aplikasi *TikTok* menghadapi tantangan teknis yang besar. *TikTok* mengumpulkan berbagai jenis data dari penggunanya. Data tersebut meliputi informasi akun, lokasi, riwayat pencarian, aktivitas saat menggunakan aplikasi, hingga preferensi terhadap jenis konten tertentu (Tulisan, 2026). Secara sepesifiknya *platform TikTok* menyimpan berbagai data aktivitas pengguna, termasuk riwayat pengiriman *gift*, interaksi pesan, dan *log* akun, di dalam basis data lokas penyimpanan (*local storage*) perangkat yang digunakan. Sayangnya, hingga saat ini belum ada prosedur standar yang jelas dan diakui secara luas dalam teknik pengambilan (*acquisition*) serta pengolahan data forensik khusus untuk aplikasi *TikTok*. Akibatnya, penegak hukum seringkali menghadapi kesulitan dalam menjaga aspek integritas, otentisitas, dan validitas data yang diperoleh agar dapat diakui sebagai alat bukti yang sah di pengadilan. Mengingat tingginya urgensi penanganan kasus kejahatan siber yang memanfaatkan *platform* digital, diperlukan sebuah metode investigasi forensik digital yang terstruktur dan terstandar pada platform *TikTok*. Untuk mengatasi tantangan teknis pada platform tersebut, penerapan metode forensik digital yang mengacu pada standar global sangat diperlukan. Penelitian ini menerapkan kerangka kerja NIST SP 800-86 (*National Institute of Standards and Technology Special Publication 800-86*). Metode ini menyediakan empat tahapan sistematis, yaitu: *collection* (pengumpulan), *examination* (pemeriksaan), *analysis* (analisis), dan *reporting* (pelaporan) (Kent et al., 2006). Melalui penerapan kerangka kerja NIST ini, proses ekstraksi data artefak digital dari aplikasi *TikTok* diharapkan dapat menjaga rantai barang bukti (*chain of custody*) secara ketat, sehingga hasil akuisisi data memiliki legalitas yang kuat.

Berdasarkan penelusuran literatur nasional terdahulu, penelitian forensik digital yang secara spesifik berfokus pada analisis artefak aplikasi *TikTok*, khususnya fitur *TikTok Live Gift* sebagai objek promosi ilegal, masih sangat terbatas. Sebagian besar penelitian forensik media sosial sebelumnya masih berfokus pada *platform* pesan instan atau forensik berbasis *web* umum. Oleh karena itu, penelitian ini penting untuk dilakukan guna memberikan kontribusi akademis dan praktis mengenai metodologi identifikasi bukti digital pada platform *TikTok.*

2. Kajian Teori

2.1. Digital Forensik

Digital forensik adalah salah satu bagian dari pada forensik yang membahas tentang bagaimana sistem digital mempengaruhi dan dapat meninggalkan data, dan sesuatu yang bisa digali kembali agar bisa dijadikan sebagai bukti pada sistem yang akan dicari (Yuadi, 2023). Tujuan utama digital forensik adalah merekonstruksi kejadian, mengidentifikasi pelaku, dan menjaga keabsahan barang bukti. Investigator mengandalkan teknik seperti pembuatan salinan identik (*imaging*) dan penghitungan nilai *hash* untuk menjamin bahwa data asli dari tempat kejadian perkara tetap utuh. Melalui prosedur ketat tersebut, hasil analisis yang diperoleh dapat dipertanggungjawabkan secara sah dan diterima sebagai alat bukti yang valid di dalam persidangan (Widiyasono, 2024).

2.2. Artefak Digital

Artefak digital adalah jejak atau sisa aktivitas pengguna yang tertinggal di dalam sistem operasi, perangkat keras, maupun aplikasi setelah suatu tindakan dilakukan pada perangkat elektronik. Dalam dunia digital forensik, komponen ini ibarat rekaman sidik jari atau puing-puing informasi yang sangat berharga untuk merekonstruksi kronologi peristiwa siber. Keberadaan artefak ini sering kali tidak disadari oleh pengguna biasa karena letaknya yang tersembunyi di dalam sistem, seperti pada berkas *registry*, *log file*, *cache* peramban, hingga metadata dari sebuah dokumen. Melalui analisis mendalam terhadap artefak-artefak tersebut, seorang investigator dapat membuktikan secara ilmiah mengenai siapa, kapan, dan bagaimana sebuah aset digital diakses atau dimanipulasi (Salim et al., 2025).

2.3. *TikTok*

TikTok adalah salah satu platform media sosial paling popular didunia. *TikTok* merupakan platform media sosial berbasis video pendek milik *ByteDance*. *TikTok* menyimpan berbagai aktivitas pengguna pada database lokal dan *server*, termasuk aktivitas *live*. *TikTok live* adalah fitur siaran langsung. Fitur *live gift* memungkinkan penonton mengirim hadiah virtual berupa koin yang kemudian dapat ditukar host menjadi uang. Fitur ini sering disalahgunakan sebagai media promosi judi *online*. Sesuai Kebijakan Privasi GDPR (*General Data Protection Regulation*), *TikTok* menyediakan fitur bagi pengguna untuk mengunduh salinan data pribadinya. File yang dihasilkan berupa *.zip* berisi folder *Activity*, *Direct Message*, *Profile*, dll dalam format *.json* dan *.html*. File *Activity*/*Live Gifts.json* berisi *array* objek dengan *field* seperti *Date*, *GiftName*, *CoinCount*, *Receiver*, dan *LiveId* (Reportal, 2025).

2.4. NIST SP 800-86

NIST SP 800-86 (*Guide to Integrating Forensic Techniques into Incident Response*) adalah panduan standar global yang diterbitkan oleh *National Institute of Standards and Technology* (NIST) untuk mengintegrasikan teknik

DOI: https://doi.org/10.69693/ijmst.v4i2.12395

digital forensik ke dalam proses penanganan insiden keamanan siber. Panduan ini dirancang agar organisasi tidak hanya mampu merespons serangan, tetapi juga dapat mengumpulkan bukti digital yang valid, akurat, dan dapat dipertanggungjawabkan secara hukum. Standardisasi ini membagi proses forensik menjadi empat tahapan utama yang saling berkesinambungan, yaitu *Collection*, *Examination*, *Analysis*, dan *Reporting* (Kent et al., 2006).

2.5. FTK *Imager*

FTK *Imager* adalah perangkat lunak gratis yang sangat populer digunakan oleh para investigator untuk menyalin data dari media penyimpanan digital secara aman pada tahap awal investigasi. Alat ini berfungsi untuk membuat salinan yang persis sama (identik) dengan data aslinya, sehingga investigator bisa memeriksa data tersebut tanpa khawatir akan merusak atau mengubah isi di dalam perangkat aslinya. Selain menyalin, alat ini juga bisa digunakan untuk melihat isi folder, menyelamatkan file yang tidak sengaja terhapus, serta menghitung nilai *hash* (sidik jari digital) untuk memastikan data tidak berubah. Karena kemudahan dan kemampuannya menghasilkan berbagai format file standar forensik, FTK *Imager* menjadi salah satu alat wajib yang sangat diandalkan dalam dunia forensik digital (Agustiono et al., 2024).

2.6. *Autopsy*

Autopsy adalah platform digital forensik berbasis sumber terbuka (*open-source*) yang dirancang dengan antarmuka grafis (GUI) yang intuitif untuk menganalisis berbagai jenis media penyimpanan. *Platform* ini bertindak sebagai *core engine* yang mengintegrasikan berbagai modul analisis, mulai dari pemeriksaan riwayat *web*, ekstraksi metadata, hingga analisis registri sistem operasi. Karena sifatnya yang modular dan didukung oleh komunitas global yang luas, investigator dapat dengan mudah menambahkan *plugin* pihak ketiga untuk memperluas kapabilitas investigasi. Keunggulan utama *Autopsy* terletak pada efisiensinya dalam mengotomatisasi pencarian kata kunci dan mengategorikan jenis file, sehingga mempercepat proses penemuan fakta hukum dari tumpukan data yang massif (Tamam et al., 2023).

2.7. *Hashing*

Hashing adalah sebuah algoritma matematika tunggal yang mengubah data input dengan ukuran apa pun menjadi *string* karakter dengan panjang tetap yang unik. Dalam ranah digital forensik, proses ini berfungsi sebagai sidik jari digital untuk mendeteksi perubahan sekecil apa pun pada berkas atau media penyimpanan. Jika satu *bit* data saja termodifikasi, maka nilai hash yang dihasilkan pada pengujian berikutnya akan berubah secara drastis, sebuah fenomena yang dikenal sebagai *avalanche effect*. Dua algoritma *hashing* yang paling umum digunakan dalam penegakan hukum dan analisis forensik adalah MD5 (*Message Digest 5*) dan SHA-256 (*Secure Hash Algorithm 256-bit*) (Hutagalung et al., 2023).

2.8. *Chain of Custody*

Chain of custody (rantai penyerahan barang bukti) merupakan dokumen kronologis yang mencatat secara ketat kronologi fisik dan elektronik dari suatu barang bukti sejak pertama kali ditemukan di tempat kejadian perkara hingga dipresentasikan di pengadilan. Dokumen ini harus mencantumkan informasi mendetail mengenai siapa yang mengumpulkan, kapan waktu pengambilannya, di mana lokasinya, serta siapa saja yang bertanggung jawab saat terjadi perpindahan tangan. Setiap celah atau kelalaian dalam pencatatan *chain of custody* dapat mengakibatkan barang bukti dianggap terkontaminasi atau tidak sah di mata hukum. Oleh karena itu, pemeliharaan dokumen ini sangat krusial untuk membuktikan bahwa barang bukti digital yang dianalisis di laboratorium adalah benar-benar barang bukti asli yang sama dari TKP tanpa mengalami rekayasa (Margono, 2026).

2.9. Integritas Data

Integritas data merupakan pilar paling krusial dalam forensik digital karena menentukan sah atau tidaknya suatu bukti di mata hukum. Jika data digital mengalami perubahan atau manipulasi selama proses investigasi, maka validitasnya akan langsung gugur di persidangan. Oleh karena itu, investigator wajib menerapkan prosedur perlindungan ketat, mulai dari isolasi perangkat hingga penggunaan fungsi hash sebagai sidik jari digital (Gani, 2023). Integritas data merupakan pilar paling krusial dalam forensik digital karena menentukan sah atau tidaknya suatu bukti di mata hukum. Jika data digital mengalami perubahan atau manipulasi selama proses investigasi, maka validitasnya akan langsung gugur di persidangan. Oleh karena itu, investigator wajib menerapkan prosedur perlindungan ketat, mulai dari isolasi perangkat hingga penggunaan fungsi *hash* sebagai sidik jari digital.

3. Metode Penelitian

Penelitian ini menggunakan metode kualitatif dengan pendekatan digital forensik untuk menganalisis artefak digital pada aplikasi *TikTok*. Pendekatan ini memungkinkan peneliti untuk memahami secara mendalam bagaimana platform *TikTok* mengelola dan menstrukturkan data aktivitas pengguna di dalam memori penyimpanan perangkat. Untuk menjamin proses perolehan, pemeriksaan, dan analisis bukti digital dilakukan secara sistematis serta dapat dipertanggungjawabkan secara hukum, penelitian ini menerapkan kerangka kerja NIST SP 800-86 yang terdiri atas empat tahapan operasional. Selain melakukan analisis secara kualitatif, penelitian ini juga melakukan evaluasi terhadap keberhasilan proses identifikasi artefak digital. Evaluasi dilakukan dengan membandingkan jumlah artefak digital yang berhasil ditemukan menggunakan *tools* forensik dengan jumlah artefak yang telah

DOI: https://doi.org/10.69693/ijmst.v4i2.12395

ditentukan pada skenario penelitian. Hasil evaluasi dinyatakan dalam bentuk persentase keberhasilan menggunakan persamaan sebagai berikut.

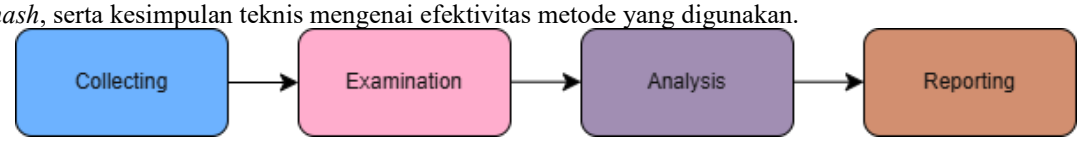
$$Presentase\ Keberhasilan(\%) = \frac{Jumlah\ Artefak\ yang\ Berhasil\ ditemukan}{Jumlah\ Artefak\ Awal} \times 100\% \quad (1)$$

Nilai persentase yang diperoleh digunakan untuk menunjukkan tingkat keberhasilan proses identifikasi artefak digital. Semakin tinggi nilai persentase yang dihasilkan, maka semakin baik kemampuan metode NIST SP 800-86 beserta *tools* yang digunakan dalam mengidentifikasi barang bukti digital pada kasus promosi judi *online* melalui fitur *TikTok Live Gift.*

3.1. Tahapan Penelitian

Tahapan pelaksanaan penelitian disesuaikan dengan ruang lingkup pemrosesan data ekspor resmi akun *TikTok* sebagai berikut:

1. *Collection* (Pengumpulan): Tahap pengumpulan *(collection)* data digital harus mengutamakan prinsip relevansi, otentisitas, dan minimalisasi risiko modifikasi terhadap barang bukti (Matondang et al., 2023). Tahap ini berfokus pada prosedur penarikan data ekspor resmi melalui fitur *Download Your Data* yang disediakan aplikasi *TikTok* sesuai kebijakan *platform*. Berkas arsip aktivitas akun dalam format *.zip* diunduh dan langsung diisolasi dalam stasiun kerja *(workstation)* untuk memastikan data aman dari modifikasi yang tidak disengaja.
2. *Examination* (Pemeriksaan): Tahap pemeriksaan *(examination)* berfokus pada penggunaan perangkat lunak forensik untuk mengidentifikasi, mengolah, dan memetakan arsitektur data tanpa mengubah karakteristik asli dari barang bukti tersebut (Runtuwene et al., 2024). Tahap ini merupakan proses teknis untuk memastikan integritas berkas sebelum dianalisis. Langkah pertama adalah memasukkan berkas ke dalam perangkat lunak FTK *Imager* untuk dihitung nilai *hash* (MD5 atau SHA-256) sebagai sidik jari digital awal. Selanjutnya, berkas dimuat ke dalam perangkat lunak *Autopsy* untuk memetakan struktur folder secara aman.
3. *Analysis* (Analisis): Tahap analisis *(analysis)* bertujuan untuk memeriksa hasil pemrosesan data secara mendalam guna menjawab pertanyaan investigasi melalui identifikasi pola dan rekonstruksi peristiwa terlarang (Purnama et al., 2023). Tahap ini bertujuan untuk membedah isi data JSON secara spesifik pada aktivitas fitur *TikTok Live Gift*. Proses analisis dilakukan dengan bantuan skrip pemrograman *Python* untuk membaca, menyaring, dan mengekstrak data kunci berupa *username* akun pelaku promosi judi *online*, jenis *gift*, serta catatan waktu *(timestamp)* untuk merekonstruksi bukti digital.
4. *Reporting* (Pelaporan): Tahap pelaporan *(reporting)* merupakan fase akhir dari siklus forensik digital yang bertujuan untuk menyajikan temuan teknis secara objektif, transparan, dan dapat direplikasi oleh investigator lain (Maulidal, 2026). Tahap akhir ini menyajikan temuan teknis secara objektif dan transparan. Peneliti menyusun laporan forensik formal yang menyajikan tabel *log* data hasil olahan *Python*, dokumentasi nilai *hash*, serta kesimpulan teknis mengenai efektivitas metode yang digunakan.



Gambar 1. Alur Penelitian

3.2. Skenario

Skenario penelitian ini dirancang dalam bentuk simulasi terkontrol untuk merekonstruksi modus operandi promosi judi *online* pada fitur *TikTok live gift* tanpa melakukan aktivitas perjudian secara riil.

1. Langkah awal simulasi dilakukan dengan menyiapkan dua buah akun *TikTok* buatan yang bertindak sebagai akun penyiar (*streamer*) dan akun penonton sekaligus pelaku promosi (target investigator). Pada akun pelaku, dilakukan modifikasi profil di mana nama pengguna (*username*) dan nama tampilan (*display name*) diubah secara sengaja menggunakan nama situs judi *online* tiruan yang telah ditentukan untuk kebutuhan riset.
2. Skenario dilanjutkan dengan masuk ke tahap interaksi, di mana akun penyiar memulai sesi siaran langsung melalui fitur *TikTok live*. Di tengah jalannya siaran langsung tersebut, akun pelaku masuk sebagai penonton dan secara masif mengirimkan sejumlah hadiah virtual (*live gift*) kepada akun penyiar. Pengiriman *gift* ini memicu sistem *TikTok* untuk menampilkan notifikasi visual secara otomatis di layar siaran berupa nama akun pelaku beserta ikon hadiah yang dikirimkan. Kemunculan nama akun judi *online* di layar siaran langsung inilah yang menjadi objek utama promosi ilegal yang disaksikan oleh penonton lain secara *real-time*. setelah seluruh rangkaian simulasi interaksi tersebut selesai, sesi siaran langsung diakhiri oleh penyiar.
3. Prosedur pengumpulan bukti digital dimulai tepat setelah simulasi selesai dilakukan. Peneliti mengakses pengaturan privasi pada akun *TikTok* penyiar yang menerima *gift* untuk mengajukan permintaan unduh data melalui fitur resmi *Download Your Data* dengan memilih format keluaran JSON. Setelah permintaan diproses dan dokumen siap oleh pihak *TikTok*, berkas arsip data berbentuk *.zip* diunduh ke komputer investigator untuk memasuki tahapan forensik menggunakan *tools* yang telah ditentukan.

DOI: https://doi.org/10.69693/ijmst.v4i2.12395

Skenario pencarian bukti di dalam berkas JSON ini difokuskan penuh untuk melacak jejak digital aktivitas *live gift*, mencakup identifikasi nama akun judi *online* milik pelaku yang muncul saat siaran, jenis *gift* yang dikirimkan, serta catatan waktu (*timestamp*) terjadinya pengiriman untuk membuktikan validitas transaksi visual tersebut..

3.3. Alat dan Bahan

Alat yang digunakan dalam penelitian ini meliputi *hardware* berupa satu unit laptop sebagai *workstation* investigator, serta *software* forensik yakni FTK *Imager* untuk verifikasi integritas, *Autopsy* untuk analisis struktur data, dan *Python* untuk parsing data JSON. Bahan penelitian utama adalah berkas *log* aktivitas dalam format *.json* yang diperoleh melalui fitur ekspor resmi *TikTok*.

Tabel 1. Alat dan Bahan Penelitian

Hardware	***Software***	**Bahan**
Laptop	FTK *Imager*	Berkas Ekspor Format *.zip*
Smartphone	*Autopsy*	Berkas *Log* Aktivitas Format *.json*
Kabel USB	*Python*	
	Visual Studio Code	
	Aplikasi *TikTok*	

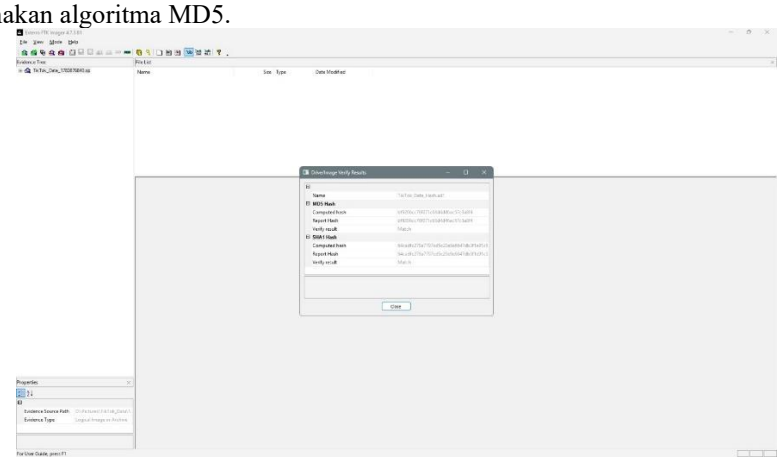
5. Hasil dan Pembahasan

3.1. Tahap *Collecting*

Tahap *Collection* merupakan proses awal dalam kerangka kerja NIST SP 800-86 yang bertujuan memperoleh barang bukti digital dengan tetap menjaga keaslian (integritas) data. Pada penelitian ini, proses pengumpulan diawali dengan pelaksanaan skenario penelitian yang telah dirancang pada Bab III. Setelah seluruh rangkaian simulasi selesai dilakukan, peneliti mengajukan permintaan data melalui fitur *Download Your Data* yang disediakan oleh aplikasi *TikTok*. Setelah permintaan tersebut diproses dan disetujui oleh pihak *TikTok*, data aktivitas akun diunduh dalam bentuk berkas terkompresi (*.zip*).

Gambar 2. Unduh Data *TikTok*

Berkas hasil unduhan kemudian dipindahkan ke stasiun kerja investigator sebagai barang bukti digital yang akan dianalisis. Untuk memastikan bahwa data yang diperoleh tetap autentik dan tidak mengalami perubahan selama proses penelitian, dilakukan verifikasi integritas menggunakan perangkat lunak FTK *Imager* melalui perhitungan nilai *hash* menggunakan algoritma MD5.



DOI: https://doi.org/10.69693/ijmst.v4i2.12395

Gambar 3. *Hashing* Data

Hasil proses *collection* menunjukkan bahwa data berhasil diperoleh dari *server TikTok* dalam format *.zip* tanpa mengalami perubahan selama proses pemindahan ke *workstation investigator*.

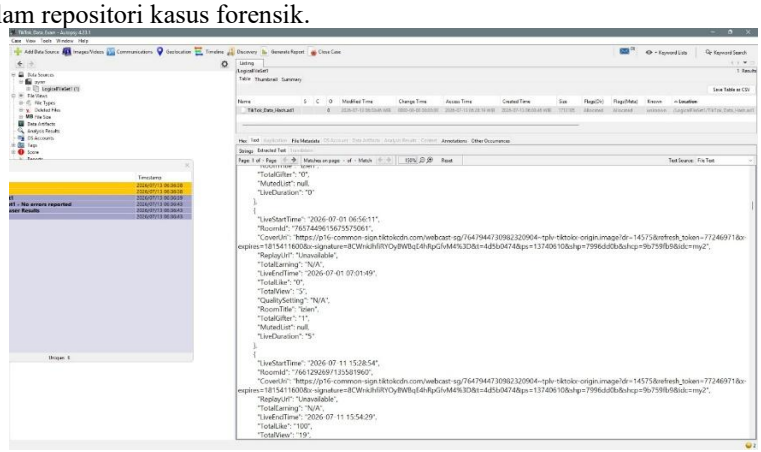
Tabel 2. Hasil Collecting

Parameter	Hasil
Nama Berkas	TikTok_Data_1783876840.zip
Ukuran Berkas	114 KB (117.367 bytes)
Format Berkas	.zip
Algoritma *Hash*	MD5 dan SHA1
Nilai *Hash* MD5	bf9206cc76f071c68d4d46ac57c3a8f4
Nilai *Hash* SHA1	64cadfc278a7797cd5c20e9e6647db3f1e91c5

Tahap *collection* berhasil dilaksanakan sesuai dengan prosedur NIST SP 800-86 karena proses pengumpulan data dilakukan melalui mekanisme resmi yang disediakan oleh *TikTok*. Penggunaan FTK *Imager* untuk menghasilkan nilai *hash* berfungsi sebagai mekanisme verifikasi integritas sehingga keaslian barang bukti tetap terjaga selama proses investigasi. Nilai *hash* yang dihasilkan menjadi acuan untuk memastikan bahwa tidak terjadi perubahan terhadap berkas sejak pertama kali diperoleh hingga tahap analisis.

3.2. Tahap *Examination*

Tahap *Examination* bertujuan melakukan pemeriksaan awal terhadap barang bukti digital tanpa mengubah isi data. Pada penelitian ini pemeriksaan dilakukan menggunakan perangkat lunak *Autopsy* dengan memuat berkas hasil ekspor *TikTok* ke dalam repositori kasus forensik.

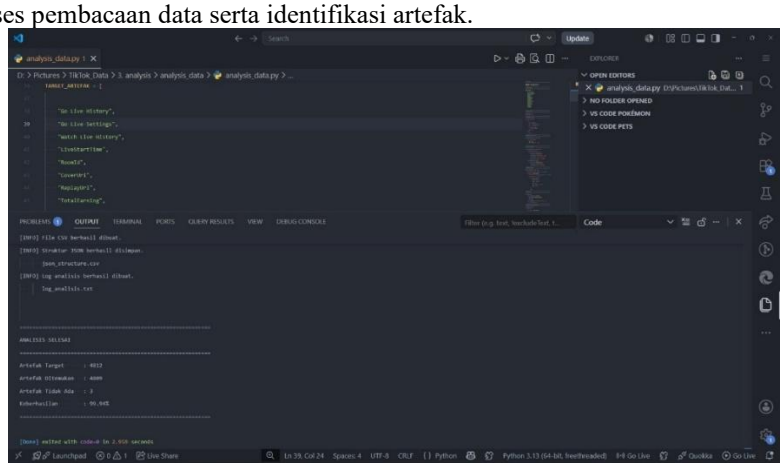


Gambar 4. Pemeriksaan Data menggunakan *Autopsy*

Autopsy digunakan untuk mengidentifikasi struktur direktori, jenis file, serta artefak digital yang tersedia pada berkas hasil ekspor. Hasil pemeriksaan menunjukkan bahwa *Autopsy* berhasil mengidentifikasi struktur data hasil ekspor *TikTok*.

3.3. Tahap *Analysis*

Tahap *Analysis* dilakukan untuk mengidentifikasi artefak digital yang berkaitan dengan tujuan penelitian. Analisis dilakukan terhadap berkas *user_data_tiktok.json* menggunakan kombinasi *Autopsy* dan skrip *Python* guna mempermudah proses pembacaan data serta identifikasi artefak.



Gambar 5. Analisis Data menggunakan Skrip *Python*

Berdasarkan hasil analisis diperoleh artefak digital sebagai berikut.

DOI: https://doi.org/10.69693/ijmst.v4i2.12395

Tabel 3. Analisis Data menggunakan *Autopsy*

Artefak	Status
Go Live History	Ditemukan
Go Live Settings	Ditemukan
Watch Live History	Ditemukan
LiveStartTime	Ditemukan
RoomId	Ditemukan
CoverUri	Ditemukan
ReplayUrl	Ditemukan
TotalEarning	Ditemukan
LiveEndTime	Ditemukan
TotalLike	Ditemukan
TotalView	Ditemukan
QualitySetting	Ditemukan
RoomTitle	Ditemukan
TotalGifter	Ditemukan
MutedList	Ditemukan
LiveDuration	Ditemukan
Username	Tidak Ditemukan
Gift Name	Tidak Ditemukan
Timestamp	Tidak Ditemukan
Comments	Ditemukan

Berdasarkan hasil pemeriksaan menggunakan *Autopsy*, sistem berhasil mengidentifikasi struktur data yang tersimpan pada berkas ekspor *TikTok*. Temuan ini menunjukkan bahwa *Autopsy* mampu membaca dan mengindeks berkas JSON hasil ekspor resmi *TikTok* dengan baik. Namun demikian, terdapat artefak yang tidak ditemukan, hal tersebut perlu dianalisis lebih lanjut pada tahap berikutnya untuk mengetahui apakah penyebabnya berasal dari struktur data ekspor *TikTok* atau keterbatasan data yang disediakan oleh *platform*.

Tabel 4. Analisis Data menggunakan Skrip *Python*

Artefak	Status
Go Live History	Ditemukan
Go Live Settings	Ditemukan
Watch Live History	Ditemukan
LiveStartTime	Ditemukan
RoomId	Ditemukan
CoverUri	Ditemukan
ReplayUrl	Ditemukan
TotalEarning	Ditemukan
LiveEndTime	Ditemukan
TotalLike	Ditemukan
TotalView	Ditemukan
QualitySetting	Ditemukan
RoomTitle	Ditemukan
TotalGifter	Ditemukan
MutedList	Ditemukan
LiveDuration	Ditemukan
Username	Tidak Ditemukan
Gift Name	Tidak Ditemukan
Timestamp	Tidak Ditemukan
Comments	Ditemukan

Hasil analisis menunjukkan bahwa beberapa artefak digital berhasil diidentifikasi dari berkas hasil ekspor *TikTok*. Artefak tersebut meliputi *Go Live History, Go Live Settings, Watch Live History, LiveStartTime, RoomId, CoverUri, ReplayUrl, TotalEarning, LiveEndTime, TotalLike, TotalView, QualitySetting, RoomTitle, TotalGifter, MutedList,* dan *LiveDuration* yang dapat digunakan untuk merekonstruksi aktivitas pengguna selama sesi siaran langsung.

Apabila ditemukan artefak yang tidak sesuai dengan ekspektasi penelitian, kondisi tersebut tidak secara langsung menunjukkan kegagalan proses investigasi. Berdasarkan hasil penelitian, *Username*, *Gift Name*, dan *Timestamp* tidak tersedia pada berkas hasil ekspor resmi *TikTok*. Hal ini mengindikasikan bahwa keterbatasan berasal dari ruang lingkup data yang disediakan melalui fitur *Download Your Data*, bukan dari kemampuan *Autopsy* dan skrip *Python* dalam melakukan identifikasi artefak. Dengan kata lain, *Autopsy* dan skrip *Python* hanya dapat menampilkan data yang memang tersedia pada sumber bukti digital.

Temuan ini menunjukkan bahwa penggunaan data ekspor resmi *TikTok* masih memiliki keterbatasan untuk memperoleh seluruh metadata aktivitas pengguna. Oleh karena itu, apabila investigasi memerlukan artefak yang lebih lengkap, seperti metadata transaksi *Live Gift*, maka diperlukan metode akuisisi lain yang mampu memperoleh data langsung dari perangkat atau penyimpanan aplikasi.

DOI: https://doi.org/10.69693/ijmst.v4i2.12395

3.4. Tahap *Reporting*

Tahap *Reporting* merupakan tahap akhir dalam metode NIST SP 800-86 yang bertujuan mendokumentasikan seluruh proses investigasi digital secara sistematis agar hasil penelitian dapat dipertanggungjawabkan. Seluruh artefak yang berhasil diperoleh pada tahap *Collection*, *Examination*, dan *Analysis* disusun ke dalam bentuk laporan yang memuat informasi mengenai integritas barang bukti, hasil identifikasi artefak, serta interpretasi terhadap data yang ditemukan.

Pada penelitian ini, laporan akhir disusun berdasarkan hasil pemeriksaan menggunakan FTK *Imager*, *Autopsy*, dan skrip *Python*. FTK *Imager* digunakan untuk memastikan integritas barang bukti melalui proses *hashing*, *Autopsy* digunakan untuk mengidentifikasi artefak digital pada berkas hasil ekspor *TikTok*, sedangkan *Python* digunakan untuk mengotomatisasi proses analisis dan menghasilkan laporan dalam bentuk file CSV dan TXT.

Ringkasan Hasil Investigasi

Berdasarkan seluruh tahapan investigasi, diperoleh hasil identifikasi artefak digital sebagaimana ditunjukkan pada Tabel berikut.

Tabel 5. Ringkasan Hasil Investigasi

Tahapan	Tools	Hasil
Collecting	FTK *Imager*	Berkas hasil ekspor *TikTok* berhasil diverifikasi menggunakan algoritma MD5 sehingga integritas barang bukti tetap terjaga.
Examination	*Autopsy*	Struktur data JSON berhasil dibaca dan artefak digital *TikTok Live* berhasil diidentifikasi.
Analysis	*Autopsy* dan Skrip *Python*	Data JSON berhasil diparsing, artefak divalidasi, serta hasil analisis diekspor ke dalam format CSV dan TXT.
Reporting	Dokumentasi Penelitian	Seluruh hasil investigasi disusun menjadi laporan penelitian sesuai metode NIST SP 800-86.

Ringkasan Artefak Digital

Hasil analisis menunjukkan bahwa tidak seluruh artefak yang menjadi target penelitian tersedia pada data hasil ekspor *TikTok*. Ringkasan hasil identifikasi artefak dapat dilihat pada Tabel berikut.

Tabel 6. Ringkasan Artefak Digital

Artefak	Status
Go Live History	Ditemukan
Go Live Settings	Ditemukan
Watch Live History	Ditemukan
LiveStartTime	Ditemukan
RoomId	Ditemukan
CoverUri	Ditemukan
ReplayUrl	Ditemukan
TotalEarning	Ditemukan
LiveEndTime	Ditemukan
TotalLike	Ditemukan
TotalView	Ditemukan
QualitySetting	Ditemukan
RoomTitle	Ditemukan
TotalGifter	Ditemukan
MutedList	Ditemukan
LiveDuration	Ditemukan
Comments	Ditemukan
Username	Tidak Ditemukan
Gift Name	Tidak Ditemukan
Timestamp	Tidak Ditemukan

Dokumentasi Hasil Analisis

Sebagai bentuk dokumentasi investigasi, hasil analisis yang diperoleh dari skrip *Python* diekspor ke dalam beberapa format untuk memudahkan proses verifikasi dan penyusunan laporan penelitian.

Tabel 7. Dokumentasi Hasil Analisis

Dokumen	Fungsi
hasil_analisis.csv	Menyimpan seluruh artefak beserta status identifikasi.
log_analisis.txt	Mencatat proses analisis, waktu eksekusi, dan statistik hasil identifikasi.
json_structure.csv	enyimpan struktur data JSON yang berhasil diparsing

Berdasarkan seluruh tahapan investigasi yang telah dilakukan, metode NIST SP 800-86 mampu memberikan alur kerja yang sistematis dalam proses identifikasi artefak digital pada data hasil ekspor *TikTok*. Tahap *Collection*

DOI: https://doi.org/10.69693/ijmst.v4i2.12395

memastikan integritas barang bukti melalui verifikasi nilai hash menggunakan FTK *Imager*. Selanjutnya, tahap *Examination* menggunakan *Autopsy* berhasil mengidentifikasi struktur data JSON beserta artefak digital yang berkaitan dengan aktivitas *TikTok Live*. Pada tahap *Analysis*, penggunaan *Python* membantu mengotomatisasi proses *parsing* data, memvalidasi artefak yang ditemukan, serta menghasilkan dokumentasi hasil analisis dalam format CSV dan TXT.

Meskipun demikian, hasil penelitian menunjukkan bahwa tidak seluruh artefak yang direncanakan pada skenario penelitian dapat ditemukan. Artefak seperti *Username*, *Gift Name*, dan *Timestamp* tidak tersedia pada data hasil ekspor resmi *TikTok*. Kondisi tersebut mengindikasikan bahwa keterbatasan penelitian lebih dipengaruhi oleh ruang lingkup data yang disediakan melalui fitur *Download Your Data* dibandingkan oleh kemampuan perangkat lunak forensik yang digunakan. Dengan demikian, hasil investigasi tetap dapat dipertanggungjawabkan karena proses identifikasi dilakukan terhadap seluruh data yang tersedia tanpa melakukan modifikasi terhadap barang bukti.

Secara keseluruhan, kombinasi penggunaan FTK *Imager*, *Autopsy*, dan *Python* mendukung proses investigasi digital secara komplementer. FTK *Imager* berperan dalam menjaga integritas barang bukti, *Autopsy* berfungsi mengidentifikasi artefak digital, sedangkan *Python* meningkatkan efisiensi analisis melalui otomasi ekstraksi dan penyusunan laporan. Pendekatan ini menunjukkan bahwa penerapan metode NIST SP 800-86 dapat digunakan sebagai kerangka kerja yang sistematis dalam analisis data hasil ekspor *TikTok*.

6. Kesimpulan

Penelitian ini berhasil membuktikan bahwa penerapan metode NIST SP 800-86 menyediakan kerangka kerja yang sistematis dan terstandar untuk melakukan investigasi forensik digital pada data ekspor resmi *TikTok*. Penggunaan FTK *Imager*, *Autopsy*, dan skrip *Python* secara terintegrasi terbukti efektif dalam menjaga integritas barang bukti melalui verifikasi *hash* serta memfasilitasi identifikasi artefak aktivitas *Live Gift*. Meskipun terdapat keterbatasan data yang disediakan oleh *platform* melalui fitur *Download Your Data* seperti ketiadaan *username*, *gift name*, dan *timestamp* secara eksplisit, penelitian ini menunjukkan bahwa data yang tersedia tetap memiliki nilai pembuktian yang tinggi dan dapat dipertanggungjawabkan secara hukum. Hasil penelitian ini berimplikasi pada pentingnya standarisasi prosedur akuisisi data media sosial bagi penegak hukum, dan disarankan bagi penelitian selanjutnya untuk mengeksplorasi teknik akuisisi data tingkat lanjut guna mendapatkan artefak yang lebih komprehensif dalam pengungkapan kasus kejahatan siber.

Ucapan Terimakasih

Penulis memanjatkan puji syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penelitian ini dapat terselesaikan dengan baik. Penulis menyadari bahwa keberhasilan dalam penyusunan penelitian ini tidak terlepas dari dukungan, bimbingan, serta doa dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih yang tulus kepada:

1. Orang tua tercinta, yang senantiasa memberikan kasih sayang, dukungan moril maupun materiil, serta doa yang tiada putus yang menjadi kekuatan utama penulis dalam menempuh pendidikan dan menyelesaikan penelitian ini.
2. Dosen pembimbing, yang telah meluangkan waktu, memberikan arahan, ilmu, serta bimbingan yang sangat berharga selama proses penyusunan penelitian ini hingga mencapai hasil akhir.
3. Teman-teman seperjuangan, yang selalu memberikan semangat, bantuan teknis, serta berbagi pengalaman dan keceriaan di masa-masa sulit selama proses pengerjaan penelitian.
4. Diri sendiri, terima kasih telah berjuang dengan gigih, tetap bertahan di tengah tantangan, tidak menyerah saat menghadapi keterbatasan data, serta konsisten meluangkan waktu dan pikiran untuk menyelesaikan amanah ini dengan penuh tanggung jawab.

Semoga segala bantuan yang telah diberikan mendapat balasan yang setimpal dari Tuhan Yang Maha Esa. Penulis berharap penelitian ini dapat memberikan kontribusi nyata bagi pengembangan ilmu pengetahuan, khususnya di bidang forensik digital.

Reference

Agustiono, W., Suci, D. W., & Prastiti, N. (2024). Analisis Forensik Digital Menggunakan Metode NIST Untuk Memulihkan Barang Bukti Yang Dihapus. *Jurnal Teknologi Dan Informasi*, *14*(2), 174–185. Https://Doi.Org/10.34010/JATI.V14I2.12952

Gani, T. A. (2023). *Kedaulatan Data Digital Untuk Integritas Bangsa*. Syiah Kuala University Press. Https://Books.Google.Co.Id/Books?Hl=Id&Lr=&Id=US_TEAAAQBAJ&Oi=Fnd&Pg=PP1&Dq=Integritas+Data+Buku&Ots=Ulo-Mrdwep&Sig=Hwafftxa4e1cgfpikbyxiy9ys5o&Redir_Esc=Y#V=Onepage&Q=Integritas Data Buku&F=False

Hutagalung, J., Ramadhan, P. S., & Sihombing, S. J. (2023). Keamanan Data Menggunakan Secure Hashing Algorithm (SHA)-256 Dan Rivest Shamir Adleman (RSA) Pada Digital Signature. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(6), 1213–1222. Https://Doi.Org/10.25126/JTIIK.2023107319

Kemal, A. (2026). *Menjerat Raksasa Digital Dalam Lingkaran Setan Judi Online*. Kompas.Com. Https://Nasional.Kompas.Com/Read/2026/04/23/09200021/Menjerat-Raksasa-Digital-Dalam-Lingkaran-Setan-Judi-Online

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide To Integrating Forensic Techniques Into Incident Response. In *The National Institute Of Standards And Technology*. Https://Nvlpubs.Nist.Gov/Nistpubs/Legacy/SP/Nistspecialpublication800-86.Pdf

DOI: https://doi.org/10.69693/ijmst.v4i2.12395

Margono, R. (2026). *Manajemen Barang Bukti Dalam Perkara Pidana Materiil*. Profesor Rudi Margono. Https://Books.Google.Co.Id/Books?Hl=Id&Lr=&Id=Tmpfeqaaqbaj&Oi=Fnd&Pg=PA2&Dq=Chain+Of+Custody+Buku&Ots=K1anvwm10o&Sig=Cq9toy_4Qi58HGMj1WZyKT6pM6Y&Redir_Esc=Y#V=Onepage&Q=Chain Of Custody Buku&F=False

Matondang, J., Maulana, I., & Carudin, C. (2023). Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan NIST. *Innovative: Journal Of Social Science Research*, *3*(4), 2154–2165. Http://J-Innovative.Org/Index.Php/Innovative/Article/View/3708

Maulidal, D. (2026). Analisis Forensik Windows Timeline Untuk Rekonstruksi Aktivitas Pengguna Berbasis NIST SP 800-86. *Info Kripto*, *20*(1), 1–11. Https://Doi.Org/10.56706/IK.V20I1.157

Nouvan. (2026). *Indonesia Jadi Negara Pengguna Tiktok Terbanyak Di Dunia 2025*. Dataloka. Https://Dataloka.Id/Humaniora/4424/Indonesia-Jadi-Negara-Pengguna-Tiktok-Terbanyak-Di-Dunia-2025/

Purnama, K. E., Rozikin, C., & Ridha, A. A. (2023). Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode NIST. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*(2), 1100–1107. Https://Doi.Org/10.36040/JATI.V7I2.6660

Reportal, D. (2025). *Tiktok Users, Stats, Data, Trends, And More — Datareportal – Global Digital Insights*. Https://Datareportal-Com.Translate.Goog/Essential-Tiktok-Stats?_X_Tr_Sl=En&_X_Tr_Tl=Id&_X_Tr_Hl=Id&_X_Tr_Pto=Tc

Runtuwene, E. R., Kumajas, S. C., & Kainde, Q. C. (2024). Face Identification Using Image Procesing With The National Institute Of Standards And Technology (NIST) Method. *Jurnal Teknik Informatika (Jutif)*, *5*(4), 375–384. Https://Doi.Org/10.52436/1.JUTIF.2024.5.4.2350

Salim, M., Ahmad, S., Husain, H., Syaifuddin, Ardiansyah, M., Andaria, A. C., Dalai, H., Kamase, H. W., Safaruddin, & Saleh, M. (2025). *Pengantar Forensik Digital*. Yayasan Tri Edukasi Ilmiah. Https://Books.Google.Com/Books?Hl=Id&Lr=&Id=ASQ-EQAAQBAJ&Oi=Fnd&Pg=PA1&Dq=Forensic+Digital+Buku&Ots=Daxxsxm6t7&Sig=3brbzwv_Fsfybesjfbxxb05ladm

Tamam, M. B., Hoiriyah, Anwari, & Efenie, Y. (2023). Analisis Forensik Originalitas Gambar Menggunakan Autopsy Dan Opencv. *Jurnal Satya Informatika*, *8*(01), 43–49. Https://Doi.Org/10.59134/JSK.V8I01.236

Tulisan, K. (2026). *Penggunaan Data Pengguna Oleh Tiktok: Inovasi Digital Atau Ancaman Bagi Privasi Konsumen?* Kompasiana. Https://Www.Kompasiana.Com/Ghefiraprisilia0794/6a335f63ed64150235351d62/Penggunaan-Data-Pengguna-Oleh-Tiktok-Inovasi-Digital-Atau-Ancaman-Bagi-Privasi-Konsumen

Widiyasono, N. (2024). *Pengantar Ilmu Forensika Digital* (Pp. 0–266). CV Angkasa Media Literasi. Https://Books.Google.Co.Id/Books?Hl=Id&Lr=&Id=Swnreqaaqbaj&Oi=Fnd&Pg=PA1&Dq=Pengantar+Ilmu+Forensika+Digital+&Ots=V6wfdt5l5j&Sig=1b0tnfwz2kna2vrbrvc75_IY0vI&Redir_Esc=Y#V=Onepage&Q=Pengantar Ilmu Forensika Digital&F=False

Yuadi, I. (2023). *Forensik Digital Dan Analisis Citra* (Pp. 1–444). CV. AE Media Grafika. Https://Www.Google.Co.Id/Books/Edition/Forensik_Digital_Dan_Analisis_Citra/Lxfreaaaqbaj

DOI: https://doi.org/10.69693/ijmst.v4i2.12395