JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Analisis Barang Barang Bukti Digital Pada Aplikasi *Instagram* Berbasis *Android* Menggunakan Metode *National Institute Of Justice (NIJ)*

Muhamad Hasan Firdaus[1*], Fahmi Fachri[2]

[1,2,3]Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen, Jawa Tengah, Indonesia
Email: [1] firdausmuhamadhasan377@gmail.com, [2]fahmifachriumnu@gmail.com,
Email Penulis Korespondensi: [1] firdausmuhamadhasan377@gmail.com

Abstrak−Perkembangan teknologi informasi dan meningkatnya penggunaan media sosial, khususnya *Instagram*, telah memberikan dampak positif dalam komunikasi, namun juga memunculkan permasalahan baru seperti *cyberbullying*. *Cyberbullying* merupakan tindakan perundungan yang dilakukan melalui media digital dan dapat berdampak serius terhadap kondisi psikologis korban. Oleh karena itu, diperlukan pendekatan forensik digital untuk mengidentifikasi, mengumpulkan, dan menganalisis bukti digital guna mendukung proses pembuktian. Penelitian ini bertujuan untuk menerapkan metode *National Institute Of Justice (NIJ)* dalam analisis barang bukti digital pada aplikasi *Instagram* berbasis *Android*, serta mengevaluasi efektivitas penggunaan *tools ADB* (*Android Debug Bridge*) dan *FTK Imager* dalam proses *investigasi*. Metode *NIJ* terdiri dari lima tahapan, yaitu *Identification*, *Collection*, *Examination*, *Analysis*, dan *Reporting*. Hasil penelitian menunjukkan bahwa proses ekstraksi data menggunakan *ADB* berhasil dilakukan, serta pembuatan *image* forensik menggunakan *FTK Imager* dapat menjaga integritas data yang dibuktikan melalui nilai *hash MD5* dan *SHA1* yang identik. *File database* utama *Instagram*, yaitu *direct.db*, berhasil ditemukan dan dianalisis. Namun, pesan *Direct Message (DM)* yang mengandung unsur *cyberbullying* tidak ditemukan karena telah dihapus secara permanen oleh pelaku sebelum proses akuisisi dilakukan. Hal ini menunjukkan bahwa aplikasi *Instagram* memiliki mekanisme penghapusan data yang cukup kuat sehingga tidak meninggalkan artefak digital yang dapat dipulihkan melalui metode Logical acquisition. Kesimpulan dari penelitian ini adalah metode *NIJ* dapat diterapkan secara sistematis dalam *investigasi* forensik digital, serta *tools ADB* dan *FTK Imager* efektif dalam proses akuisisi dan verifikasi data. Namun, keberhasilan dalam menemukan bukti digital sangat dipengaruhi oleh waktu akuisisi dan metode yang digunakan.

Kata Kunci: Forensik Digital, *Cyberbullying, Instagram, NIJ, ADB, FTK Imager*

Abstract− The development of information technology and the increasing use of social media, particularly Instagram, have provided positive impacts on communication, but also introduced new problems such as cyberbullying. Cyberbullying is a form of harassment conducted through digital media that can have serious psychoLogical effects on victims. Therefore, a digital forensic approach is needed to identify, collect, and analyze digital evidence to support the investigation process. This study aims to implement the National Institute Of Justice (NIJ) method in analyzing digital evidence on the Instagram application based on Android, as well as to evaluate the effectiveness of ADB (Android Debug Bridge) and FTK Imager tools in the investigation process. The NIJ method consists of five stages: Identification, Collection, Examination, Analysis, and Reporting. The results show that the data extraction process using ADB was successfully carried out, and the creation of forensic images using FTK Imager was able to maintain data Integrity, as proven by identical MD5 and SHA1 hash values. The main Instagram database File, namely direct.db, was successfully identified and analyzed. However, Direct Message (DM) containing cyberbullying elements was not found because it had been permanently deleted by the perpetrator before the acquisition process. This indicates that the Instagram application has a strong data deletion mechanism that does not leave recoverable digital artifacts through Logical acquisition methods. In conclusion, the NIJ method can be systematically applied in digital forensic investigations, and ADB and FTK Imager are effective in data acquisition and verification processes. However, the success of obtaining digital evidence is highly dependent on the timing of acquisition and the methods used..

Keywords: Digital Forensics, Cyberbullying, Instagram, NIJ, ADB, FTK Imager.

1. PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi telah membawa perubahan fundamental dalam berbagai aspek kehidupan manusia. Di satu sisi, teknologi memudahkan masyarakat dalam mengakses informasi, memperluas jaringan sosial, dan mendorong inovasi di bidang pendidikan, ekonomi, serta interaksi sosial. Namun di sisi lain, kemajuan tersebut juga menghadirkan celah bagi berbagai bentuk penyalahgunaan teknologi yang dapat menimbulkan dampak negatif, salah satunya adalah fenomena *Cyberbullying*. Penggunaan media sosial yang semakin intensif menciptakan ruang virtual di mana individu dapat diserang secara verbal maupun emosional tanpa batasan ruang dan waktu, sehingga menimbulkan tekanan psikologis serta kerugian sosial dan hukum bagi korbannya [1].

Cyberbullying merupakan salah satu bentuk perilaku menyimpang di ruang digital yang semakin sering terjadi seiring dengan meningkatnya penggunaan media sosial. Fenomena *Cyberbullying* mengacu pada perilaku agresif yang dilakukan melalui media digital seperti internet atau aplikasi media sosial, dengan bentuk-bentuk seperti *flaming*, *harassment*, *denigration*, *impersonation*, *outing*, *trickery*, *exclusion*, dan *cyberstalking*. Bentuk perilaku tersebut dapat muncul melalui pesan negatif, komentar publik yang bersifat menyerang, hingga penyebaran konten yang merugikan individu atau kelompok [2]. Data nasional dan global menunjukkan bahwa *Cyberbullying* merupakan isu serius yang terus meningkat seiring tingginya penggunaan media sosial.

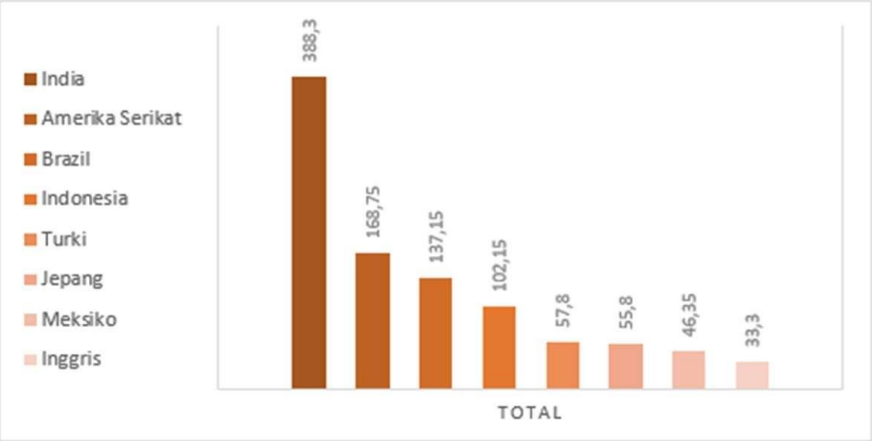
This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Berdasarkan data UNICEF, sekitar 45% dari 2.777 anak di Indonesia mengaku pernah menjadi korban *Cyberbullying*. Bentuk-bentuk *Cyberbullying* tersebut meliputi pelecehan melalui aplikasi percakapan (45%), penyebaran foto atau video pribadi tanpa izin (41%), dan bentuk pelecehan lainnya (14%). Data ini menunjukkan bahwa fenomena *Cyberbullying* telah menjadi masalah sosial yang serius dan berdampak pada kesehatan mental serta kesejahteraan psikologis korban baik secara langsung atau lewat media sosial, salah satunya adalah *Instagram* [3].

Instagram merupakan salah satu *platform* media sosial berbasis visual yang memungkinkan penggunanya untuk berbagi foto, video, serta berinteraksi melalui fitur komentar, pesan langsung *(Direct Message)*, *stories*, dan *reels*. Aplikasi ini pertama kali diluncurkan pada tahun 2010 dan berkembang pesat menjadi media sosial yang banyak digunakan oleh berbagai kalangan, khususnya remaja dan dewasa muda. Tingginya tingkat interaksi antar pengguna menjadikan *Instagram* tidak hanya sebagai sarana hiburan dan komunikasi, tetapi juga sebagai ruang ekspresi sosial yang rentan terhadap penyalahgunaan, seperti penyebaran ujaran kebencian, pelecehan verbal, dan *Cyberbullying*. Oleh karena itu, *Instagram* menjadi salah satu *platform* yang sering terlibat dalam kasus perundungan digital dan membutuhkan penanganan serius melalui pendekatan forensik digital dalam proses pembuktian hukum [4].



Gambar 1. Grafik Pengguna *Instagram* 2024
Sumber: (Rahmah et al., 2026)

Berdasarkan data diatas, Indonesia menduduki peringkat ke – 4 pada penggunaan sosial media *Instagram* di dunia dengan jumlah 102,15 juta pengguna *Instagram* per April 2024. Pengguna terbesar berasal dari kelompok usia 25–34 tahun, diikuti usia 18–24 tahun, dengan dominasi pengguna perempuan. Angka tersebut menunjukkan bahwa *Instagram* merupakan *platform* yang sangat aktif digunakan oleh masyarakat Indonesia, sekaligus menjadi ruang yang rentan terhadap perilaku *Cyberbullying* [4].

Dalam konteks penegakan hukum, tindakan *Cyberbullying* dapat dijerat melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Secara teknis, proses pembuktian peristiwa *Cyberbullying* membutuhkan dukungan digital forensics untuk menemukan, mengamankan, dan menganalisis bukti digital seperti pesan, metadata, *File* media, serta aktivitas pengguna [5]. Alat forensik seperti *ADB* (*Android Debug Bridge*) dan *FTK Imager* sangat diperlukan untuk proses ekstraksi dan pembuatan *image* forensik yang terjamin integritas datanya. Seluruh proses *investigasi* dilakukan mengacu pada metode *NIJ* (*National Institute Of Justice*) yang mencakup tahapan *Identification*, *Collection*, *Examination*, *Analysis*, dan *Reporting* [6].

National Institute Of Justice (NIJ) adalah lembaga penelitian dan dukungan teknologi yang berada di bawah Departemen Kehakiman Amerika Serikat. *NIJ* mengembangkan standar dan pedoman dalam berbagai disiplin forensik termasuk forensik digital. Metode *NIJ* dalam forensik digital dirancang untuk menghasilkan bukti yang *forensically sound* dan dapat dipertanggungjawabkan secara ilmiah dan hukum. *NIJ* merupakan sebuah metode yang bertujuan untuk menjelaskan bagaimana langkah-langkah penelitian yang akan dilakukan sehingga alur dan langkah-langkah penelitian dapat diidentifikasi secara sistematis sehingga dapat dijadikan pedoman untuk memecahkan permasalahan yang ada [7]. Tahapan metode *NIJ* mencakup *Identification* (identifikasi bukti), *Collection* (pengumpulan bukti), *Examination* (pemeriksaan bukti), *Analysis* (analisis bukti), dan *Reporting* (pelaporan hasil). Metodologi ini memastikan proses *investigasi* berjalan sistematis, akurat, dan dapat diterima di pengadilan.

Berdasarkan hasil dari penelitian yang telah dilakukan dapat dibuat kesimpulan bahwa metode *National Institute Of Justice* dalam proses identifikasi barang bukti dari aplikasi *BIP Messenger* pada *smartphone Android* berhasil didapatkan dan semua *tools* yang digunakan berjalan baik dan *tools* yang digunakan dapat memenuhi kebutuhan *tools* lainnya [7].

Berdasarkan latar belakang tersebut, penelitian ini penting dilakukan mengingat tingginya angka pengguna *Instagram*, meningkatnya kasus *Cyberbullying*, serta minimnya penelitian forensik digital yang membahas analisis teknis bukti digital *Instagram* menggunakan metode *NIJ*.

This is an open access article under the CC–BY-SA license

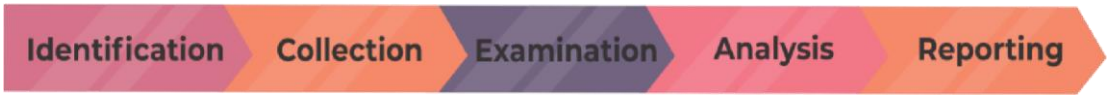
Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

2. METODOLOGI PENELITIAN

2.1 Metode NIJ

Metode penelitian yang digunakan dalam penelitian ini adalah Metode *NIJ* (*National Institute Of Justice*), yaitu kerangka kerja forensik digital yang terdiri dari lima tahap sistematis: *Identification*, *Collection*, *Examination*, *Analysis*, dan *Reporting* [8]. Dapat di lihat seperti pada gambar 3.2.



Gambar 2. Tahapan Metode *NIJ*

a. Pada tahap *Identification*, peneliti melakukan proses identifikasi terhadap seluruh sumber bukti digital yang berkaitan dengan kasus *Cyberbullying* pada aplikasi *Instagram* [9]. Identifikasi dilakukan dengan menentukan perangkat *smartphone* yang menjadi objek pemeriksaan, mencatat spesifikasi teknis perangkat seperti jenis sistem operasi, kapasitas penyimpanan, dan versi aplikasi *Instagram*, serta mengidentifikasi akun pelaku dan korban yang terlibat dalam percakapan digital.
b. Tahap selanjutnya adalah *Collection*, yaitu proses pengumpulan atau akuisisi bukti digital secara forensik. Pada tahap ini, perangkat diamankan dari jaringan dengan mengaktifkan mode pesawat agar tidak terjadi perubahan data akibat sinkronisasi otomatis. Akuisisi data dilakukan menggunakan dua alat forensik, yaitu *ADB* (*Android Debug Bridge*) dan *FTK Imager*. *ADB* (*Android Debug Bridge*) digunakan untuk mengekstraksi data aplikasi *Instagram* secara menyeluruh, termasuk pesan, *database* aplikasi, *File* media, *cache*, serta konfigurasi akun [10]. Sementara itu, *FTK Imager* digunakan untuk membuat *image* forensik dari direktori penyimpanan data *Instagram* serta menghasilkan nilai *hash* (*MD5*, *SHA1*, atau *SHA256*) yang digunakan untuk membuktikan bahwa data hasil ekstraksi memiliki integritas yang sama dengan data asli.
c. Setelah proses akuisisi selesai, penelitian dilanjutkan ke tahap *Examination*, yaitu pemeriksaan mendalam terhadap struktur data hasil ekstraksi [11]. Pada tahap ini dilakukan eksplorasi terhadap direktori aplikasi Instagram seperti *folder database*, *cache*, media, serta *File* konfigurasi. Peneliti memeriksa *File messages.db* untuk melihat isi percakapan, identitas pengirim dan penerima, waktu pengiriman, serta mendeteksi apakah terdapat pesan yang dihapus berdasarkan *flag* tertentu dalam *database*.
d. Tahap berikutnya adalah *Analysis*, yaitu menafsirkan hasil pemeriksaan untuk menentukan relevansinya dengan kasus *Cyberbullying*. Pada tahap ini peneliti menganalisis isi pesan, komentar, dan *File* media untuk mengidentifikasi adanya unsur penghinaan, *body shaming*, ancaman, pelecehan verbal, atau bentuk lain dari Cyberbullying [12]. Analisis juga dilakukan terhadap pola percakapan, frekuensi pesan, waktu kejadian, dan hubungan antar pengguna untuk menyusun gambaran utuh tentang kronologi peristiwa. Bukti pesan yang dihapus dianalisis untuk mengetahui apakah penghapusan dilakukan secara sengaja oleh pelaku, serta dibandingkan dengan bukti *screenshot* dari korban.
e. Tahap terakhir adalah *Reporting*, yaitu penyusunan laporan forensik digital secara lengkap dan sistematis [13]. Laporan memuat dokumentasi seluruh proses mulai dari identifikasi, akuisisi, pemeriksaan, analisis, hingga kesimpulan akhir. Laporan juga dilengkapi dengan bukti visual berupa *screenshot* hasil ekstraksi, grafik timeline percakapan, nilai *hash* untuk pembuktian integritas data, serta hasil pemulihan pesan yang dihapus

3. HASIL DAN PEMBAHASAN

Implementasi metode *NIJ* dalam penelitian ini dilakukan melalui lima tahapan utama, yaitu *Identification*, *Collection*, *Examination*, *Analysis*, dan *Reporting*. Setiap tahapan dilakukan secara sistematis untuk memastikan integritas dan keabsahan bukti digital.

3.1. *Identification* (Identifikasi)

Tahap *Identification* (Identifikasi) merupakan tahapan awal dalam metode *National Institute Of Justice (NIJ)* yang bertujuan untuk mengenali dan menentukan seluruh komponen yang berpotensi menjadi sumber bukti digital dalam proses *investigasi*. Pada tahap ini dilakukan identifikasi terhadap perangkat, aplikasi, jenis data, serta *tools* yang akan digunakan dalam proses forensik digital.

Objek utama dalam penelitian ini adalah sebuah perangkat *smartphone* berbasis *Android*, yaitu *Xiaomi Redmi Note 7* dengan sistem operasi *Android* 10 (MIUI 12.5.3.0) yang telah berada dalam kondisi *rooted*. Perangkat ini digunakan sebagai media simulasi kasus *cyberbullying* pada aplikasi *Instagram*, sehingga menjadi sumber utama dalam proses pengambilan barang bukti digital.

This is an open access article under the CC–BY-SA license

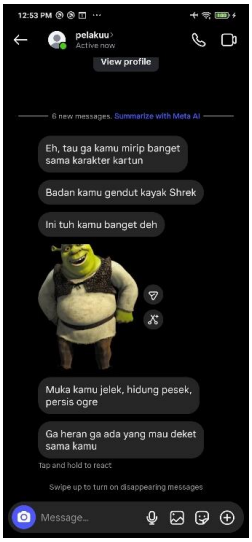
Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 3. Spesifikasi handphone

Aplikasi yang menjadi fokus *investigasi* adalah *Instagram*, khususnya pada fitur *Direct Message (DM)* yang digunakan dalam skenario *cyberbullying*. Skenario diawali dengan kondisi di mana pelaku dan korban telah saling terhubung melalui fitur pertemanan pada aplikasi *Instagram*. Pelaku kemudian mengirimkan sejumlah pesan melalui fitur *Direct Message (DM)* yang mengandung unsur penghinaan dan *body shaming* yang ditujukan secara langsung kepada korban



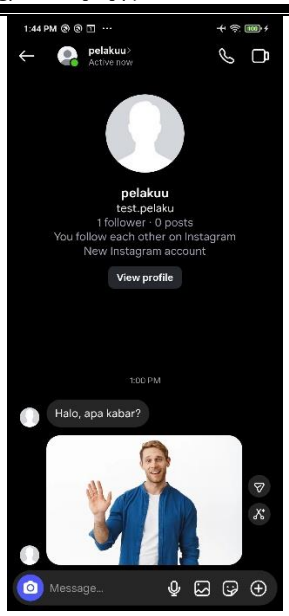
Gambar 4. DM di Sisi Korban Sebelum Dihapus

Setelah pesan terkirim dan dibaca oleh korban, pelaku kemudian melakukan penghapusan terhadap seluruh pesan yang mengandung unsur *cyberbullying* melalui fitur hapus pesan pada aplikasi *Instagram*. Tindakan penghapusan ini dilakukan dengan tujuan menghilangkan jejak digital agar aktivitas *cyberbullying* tidak dapat diketahui oleh pihak lain. Setelah menghapus pesan *body shaming*, pelaku mengirimkan satu pesan baru yang bersifat normal yaitu "Halo, apa kabar?" untuk mengaburkan jejak percakapan sebelumnya. Gambar 4.2 menampilkan tampilan DM setelah pesan *cyberbullying* dihapus, di mana hanya pesan "Halo, apa kabar?" yang tersisa dalam percakapan.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 5. Tampilan DM Setelah Dihapus

Berdasarkan hasil identifikasi awal, data yang berpotensi menjadi bukti digital meliputi *File database* aplikasi *Instagram*, terutama *File direct.db* yang menyimpan data percakapan, serta *File* pendukung lainnya yang terdapat dalam direktori penyimpanan aplikasi.

Selain itu, jenis data yang diidentifikasi dalam penelitian ini meliputi:

a. Data percakapan *(Direct Message)*
b. Metadata pesan seperti timestamp dan identitas pengguna
c. *File database* aplikasi *Instagram* (*direct.db*)

Dalam tahap ini juga dilakukan identifikasi terhadap *tools* yang digunakan dalam proses *investigasi* forensik digital, yaitu:

a. *ADB* (*Android Debug Bridge*) sebagai alat untuk melakukan akuisisi data dari perangkat *Android* [14].
b. *FTK Imager* sebagai alat untuk pembuatan *image* forensik serta verifikasi integritas data menggunakan metode hashing [15].

Hasil dari tahap identifikasi ini menjadi dasar dalam menentukan proses selanjutnya, yaitu pengumpulan (*Collection*) dan analisis data, sehingga seluruh proses *investigasi* dapat dilakukan secara terarah, sistematis, dan sesuai dengan prinsip forensik digital.

3.2. *Collection* (Pengumpulan Data)

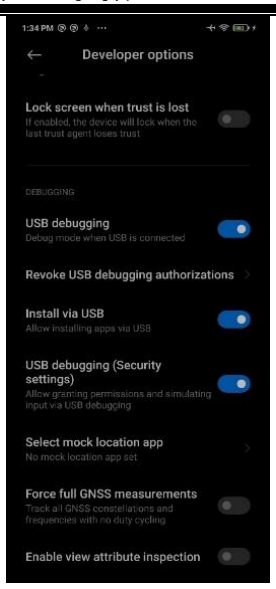
Tahap *Collection* (Pengumpulan Data) merupakan proses akuisisi barang bukti digital dari perangkat target yang telah diidentifikasi pada tahap sebelumnya. Pada tahap ini, pengumpulan data dilakukan dengan prinsip forensik digital, yaitu menjaga keaslian dan integritas data agar tidak mengalami perubahan selama proses akuisisi.

Proses pengumpulan data dilakukan terhadap perangkat *smartphone Xiaomi Redmi Note 7* yang telah berada dalam kondisi *rooted*. Sebelum proses akuisisi dilakukan, perangkat terlebih dahulu dipastikan dalam kondisi siap untuk dilakukan ekstraksi data, dengan mengaktifkan fitur *USB Debugging* serta menghubungkan perangkat ke laptop menggunakan kabel *USB*.

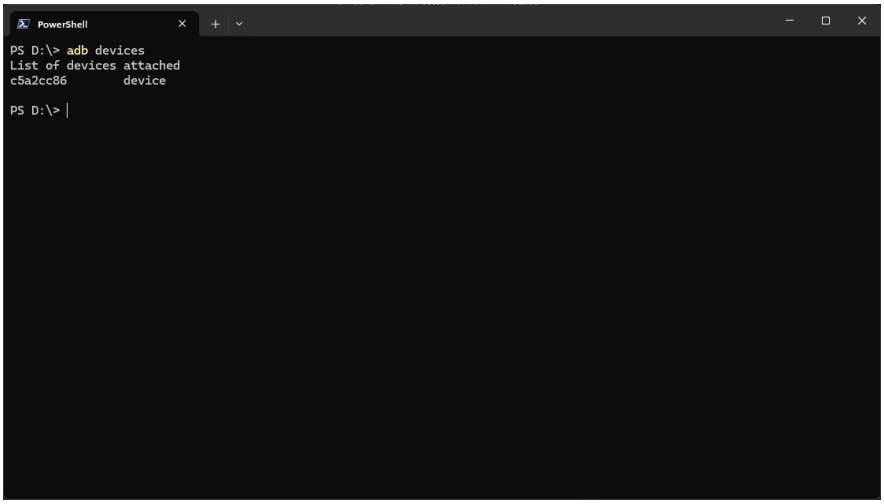
This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 6. *USB Debugging* Aktif pada Perangkat Target



Gambar 7. Koneksi *ADB* Berhasil

Selanjutnya, proses akuisisi data dilakukan menggunakan *ADB* (*Android Debug Bridge*) sebagai *tools* utama. *ADB* digunakan untuk mengakses sistem *File* perangkat *Android* dan mengekstrak data dari direktori aplikasi *Instagram* yang berada pada path /data/data/com.*Instagram*.*Android*/. Karena direktori tersebut memiliki proteksi sistem, maka digunakan akses *root* (*superuser*) untuk menyalin data tanpa mengubah isi asli dari perangkat.

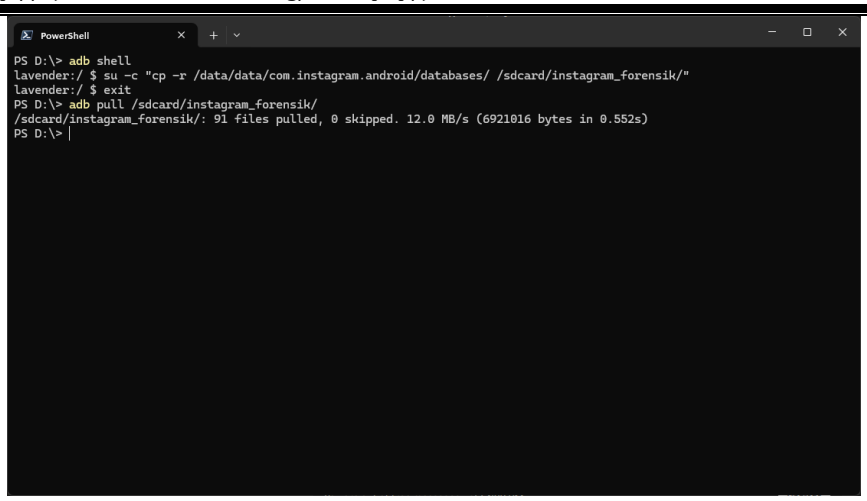
Proses akuisisi dilakukan dengan menjalankan perintah sebagai berikut:

ADB shell
Su -c "cp -r /data/data/com.*Instagram*.*Android*/*databases*/ /sdcard/*Instagram*_forensik/"
exit
ADB pull /sdcard/*Instagram_forensik*/

This is an open access article under the CC–BY-SA license

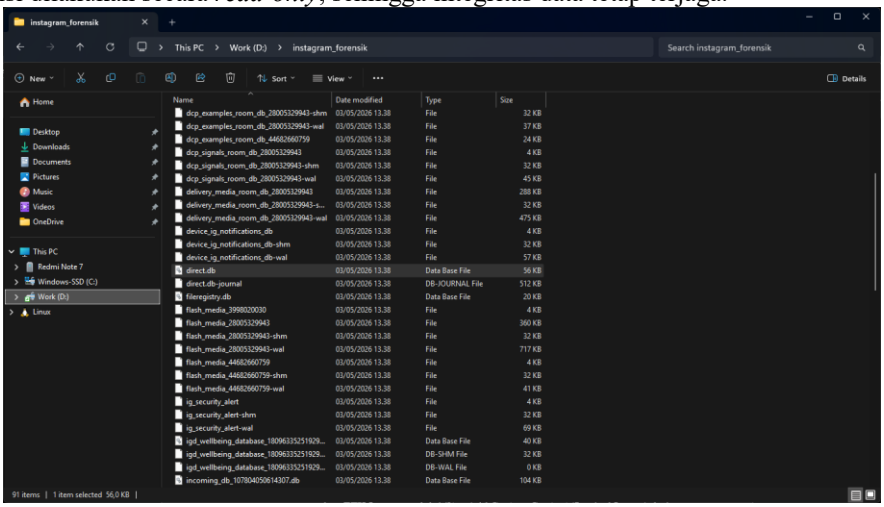
Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 8. Proses Akuisisi Data via *ADB*

Perintah tersebut bertujuan untuk menyalin *folder database Instagram* ke penyimpanan eksternal (/sdcard/), kemudian mengekstraknya ke perangkat laptop tanpa melakukan perubahan terhadap data asli. Proses ini memastikan bahwa metode akuisisi dilakukan secara *read-only*, sehingga integritas data tetap terjaga.



Gambar 9. Proses Akuisisi Data via *ADB*

Setelah proses ekstraksi menggunakan *ADB* selesai, tahap selanjutnya adalah pembuatan *image* forensik menggunakan *FTK Imager*. Proses ini dilakukan dengan mengimpor folder hasil ekstraksi ke dalam *FTK Imager* melalui fitur *Add Custom Content* (*Logical Image*), sehingga dihasilkan *File image* dengan format .ad1.

Selain itu, *FTK Imager* secara otomatis menghasilkan nilai *hash* berupa *MD5* dan *SHA1* yang digunakan untuk memverifikasi integritas data. Berdasarkan hasil verifikasi, nilai *hash* antara data asli dan *File image* menunjukkan hasil yang identik (*match*), yang menandakan bahwa tidak terjadi perubahan data selama proses akuisisi.

Tabel 1. Hasil Verifikasi *Hash FTK Imager*

No	Jenis *Hash*	Nilai *Hash* Data Asli	Nilai *Hash File Image*	Status
1	*MD5*	c0d09f238a30c12e9ea7d043958529aa	c0d09f238a30c12e9ea7d043958529aa	*Match*
2	*SHA1*	cc832536fb7a22279caa7e1d15c68f78675d5d20	cc832536fb7a22279caa7e1d15c68f78675d5d20	*Match*

Dengan demikian, tahap *Collection* berhasil dilakukan dengan baik, ditandai dengan:

a. Berhasilnya ekstraksi *File database Instagram* dari perangkat
b. Terbentuknya *File image* forensik
c. Terverifikasinya integritas data melalui nilai hash

Hasil dari tahap ini selanjutnya digunakan pada proses pemeriksaan (*Examination*) dan analisis (*Analysis*) dalam tahapan metode *NIJ* berikutnya.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

3.3. *Examination* (Pemeriksaan)

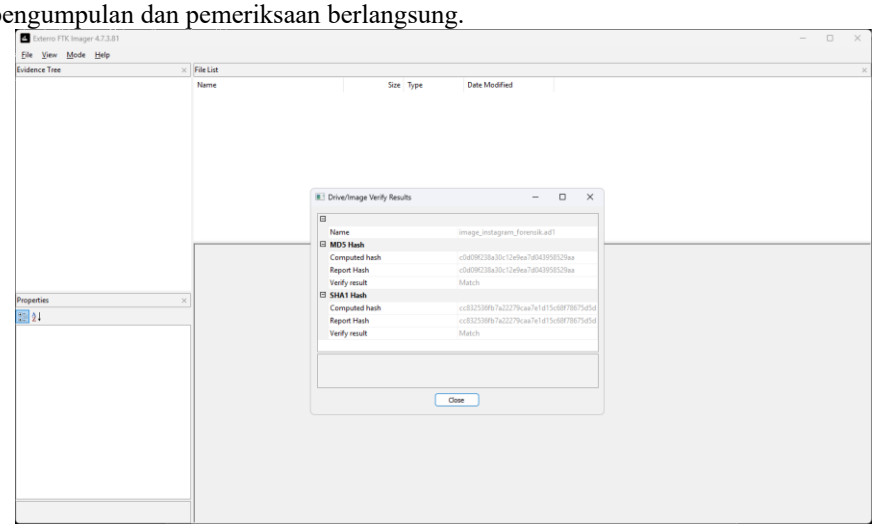
Tahap *Examination* (Pemeriksaan) merupakan proses untuk menelaah dan memverifikasi data hasil akuisisi yang telah diperoleh pada tahap *Collection*. Tujuan dari tahap ini adalah untuk memastikan bahwa data yang dikumpulkan relevan, utuh, serta siap untuk dianalisis lebih lanjut tanpa mengubah struktur asli dari data tersebut.

Pada penelitian ini, proses pemeriksaan dilakukan terhadap *File* hasil ekstraksi menggunakan *FTK Imager*. Data yang telah diperoleh dari proses akuisisi menggunakan *ADB* berupa folder *Instagram_forensik* kemudian diimpor ke dalam *FTK Imager* untuk dilakukan penelusuran struktur *File* dan identifikasi artefak digital yang tersedia.

Hasil pemeriksaan menunjukkan bahwa *File database* utama aplikasi *Instagram*, yaitu *direct.db*, berhasil ditemukan dalam direktori hasil ekstraksi. *File* ini merupakan *database* berbasis *SQLite* yang berfungsi untuk menyimpan data percakapan *Direct Message (DM)* pada aplikasi *Instagram*.

Selain *File direct.db*, ditemukan pula beberapa *File* pendukung lainnya dalam direktori *database* yang berpotensi mengandung informasi tambahan terkait aktivitas aplikasi. Struktur *File* yang ditampilkan oleh *FTK Imager* menunjukkan bahwa data tersimpan dalam kondisi utuh dan tidak mengalami kerusakan selama proses akuisisi.

Selanjutnya, dilakukan proses verifikasi integritas data menggunakan fitur hashing pada *FTK Imager*. Nilai *hash* yang dihasilkan menggunakan algoritma *MD5* dan *SHA1* menunjukkan hasil yang identik antara data hasil ekstraksi dan *File image* forensik yang telah dibuat sebelumnya. Hal ini membuktikan bahwa tidak terjadi perubahan atau manipulasi data selama proses pengumpulan dan pemeriksaan berlangsung.



Gambar 10. Hasil Verifikasi *Hash MD5* dan *SHA1*

Pada tahap ini, peneliti tidak melakukan perubahan ataupun modifikasi terhadap isi *File*, melainkan hanya melakukan proses identifikasi dan validasi terhadap data yang tersedia. Dengan demikian, prinsip forensik digital dalam menjaga keaslian bukti (*forensically sound*) tetap terpenuhi.

Berdasarkan hasil pemeriksaan, dapat disimpulkan bahwa:

a. *File database* utama (*direct.db*) berhasil diidentifikasi
b. Struktur *File* dapat diakses dan dibaca dengan baik
c. Data dalam kondisi utuh dan tidak rusak
d. Integritas data terjamin melalui verifikasi hash

Hasil dari tahap *Examination* ini menjadi dasar dalam melakukan proses analisis lebih lanjut pada tahap berikutnya, yaitu *Analysis*, untuk menginterpretasikan isi data dan menentukan keterkaitannya dengan kasus *cyberbullying* yang diteliti.

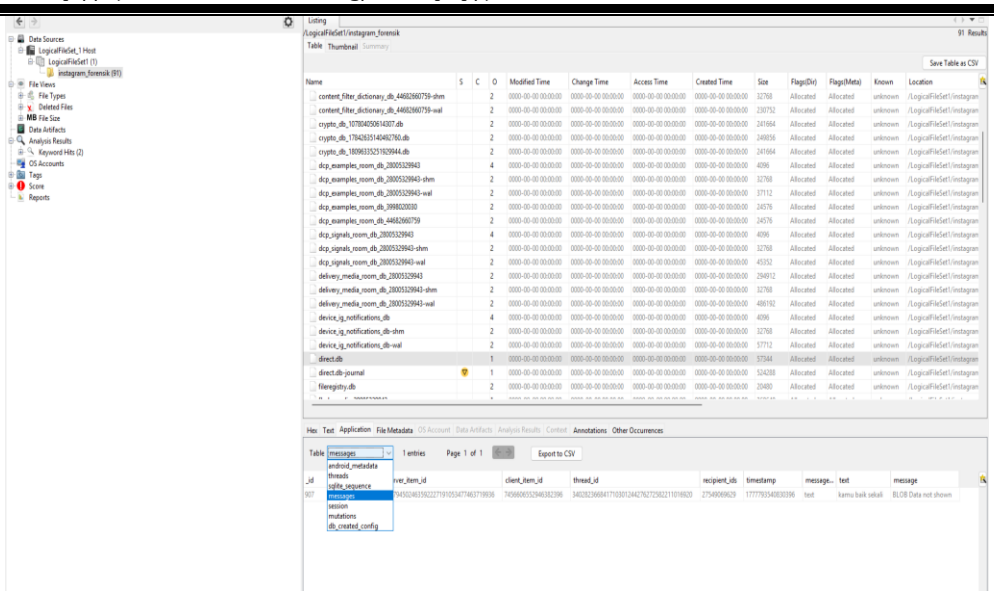
3.4. *Analysis* (Analisis)

Tahap *Analysis* (Analisis) merupakan proses penafsiran terhadap data yang telah diperiksa pada tahap sebelumnya untuk menemukan keterkaitan antara artefak digital dengan kasus *cyberbullying* yang disimulasikan. Pada tahap ini, analisis dilakukan terhadap *File* hasil ekstraksi, khususnya *File database direct.db* yang diperoleh dari aplikasi *Instagram*.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 11. Messages pada *direct.db*

Berdasarkan hasil pemeriksaan menggunakan *FTK Imager*, *File direct.db* berhasil diidentifikasi sebagai *database* utama yang menyimpan data percakapan Direct Message (DM). Struktur *File* menunjukkan bahwa data tersimpan dalam format *database SQLite* yang umumnya digunakan oleh aplikasi mobile untuk menyimpan informasi secara terstruktur.

Hasil analisis menunjukkan bahwa:

a. *File database Instagram* berhasil diperoleh dan dapat diakses
b. Struktur data dalam *File* tetap utuh dan tidak mengalami kerusakan
c. Data metadata seperti keberadaan *File* dan struktur penyimpanan berhasil diidentifikasi

Namun demikian, pesan *Direct Message (DM)* yang mengandung unsur *cyberbullying* sesuai dengan skenario penelitian tidak ditemukan dalam *File database* yang dianalisis. Kondisi ini terjadi karena pelaku dalam skenario telah menghapus seluruh pesan sebelum proses akuisisi data dilakukan.

Tidak ditemukannya pesan tersebut menunjukkan bahwa aplikasi *Instagram* menerapkan mekanisme penghapusan data secara permanen (*permanent deletion*), khususnya pada *File database direct.db*, sehingga data yang telah dihapus tidak lagi tersimpan dan tidak dapat dipulihkan melalui metode *Logical extraction* yang digunakan dalam penelitian ini.

Selain itu, tidak ditemukan pula artefak sisa (*residual data*) atau jejak data terhapus yang dapat digunakan untuk proses *recovery*. Hal ini mengindikasikan bahwa sistem penyimpanan aplikasi *Instagram* pada versi yang digunakan telah dirancang untuk menghapus data secara menyeluruh tanpa meninggalkan fragmen data yang dapat dianalisis kembali.

Temuan ini menjadi salah satu hasil penting dalam penelitian, yang menunjukkan bahwa keberhasilan *investigasi* forensik digital sangat dipengaruhi oleh waktu akuisisi data. Jika proses pengambilan data dilakukan setelah bukti dihapus oleh pelaku, maka kemungkinan untuk menemukan kembali bukti digital menjadi sangat kecil.

Meskipun pesan *cyberbullying* tidak berhasil ditemukan, proses analisis tetap memberikan hasil yang signifikan, yaitu:

a. Membuktikan bahwa *File database Instagram* dapat diekstraksi dan dianalisis
b. Menunjukkan keterbatasan metode forensik terhadap data yang telah dihapus secara permanen
c. Memberikan gambaran nyata tentang tantangan *investigasi* forensik digital pada aplikasi media sosial modern

Dengan demikian, tahap *Analysis* tidak hanya berfokus pada keberhasilan menemukan bukti, tetapi juga pada pemahaman terhadap perilaku sistem aplikasi dalam mengelola dan menghapus data, yang menjadi aspek penting dalam *investigasi* forensik digital.

3.5. *Reporting* (Pelaporan)

Tahap *Reporting* (Pelaporan) merupakan tahap akhir dalam metode *National Institute Of Justice (NIJ)* yang bertujuan untuk menyusun seluruh hasil proses *investigasi* forensik digital ke dalam bentuk laporan yang sistematis, jelas, dan dapat dipertanggungjawabkan secara ilmiah maupun hukum. Tahap ini menjadi sangat penting karena hasil analisis yang telah dilakukan harus dapat disajikan secara terstruktur agar mudah dipahami oleh pihak yang berkepentingan.

Dalam penelitian ini, laporan forensik digital disusun berdasarkan seluruh tahapan yang telah dilakukan sebelumnya, mulai dari *Identification*, *Collection*, *Examination*, hingga *Analysis*. Setiap proses didokumentasikan secara rinci untuk memastikan transparansi serta menjaga validitas hasil penelitian.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Tabel 2. Rekapitulasi Hasil Temuan Bukti Digital

No	Jenis Bukti	Deskripsi	*Tools*	Status
1	*File direct.db*	*Database* DM *Instagram*	*ADB*	Berhasil diekstrak
2	*Image* Forensik .ad1	Salinan terverifikasi *direct.db*	*FTK Imager*	Berhasil dibuat
3	*Hash MD5*/*SHA1*	Bukti integritas data	*FTK Imager*	*Match*/Terverifikasi

Laporan yang dihasilkan mencakup beberapa komponen utama, yaitu:

a. Identifikasi kasus, meliputi deskripsi singkat skenario *cyberbullying*, perangkat yang digunakan, serta aplikasi yang dianalisis.
b. Proses akuisisi data, yang menjelaskan penggunaan *ADB* dalam mengekstrak data dari perangkat *Android*, termasuk perintah yang digunakan dan lokasi direktori sumber data.
c. Verifikasi integritas data, yang dilakukan menggunakan *FTK Imager* dengan menghasilkan nilai *hash MD5* dan *SHA1* untuk memastikan bahwa data tidak mengalami perubahan selama proses akuisisi.
d. Hasil pemeriksaan dan analisis data, yang berisi temuan terhadap *File database direct.db*, struktur data yang tersedia, serta hasil analisis terkait keberadaan atau ketiadaan bukti *cyberbullying*.
e. Dokumentasi proses *investigasi*, berupa tangkapan layar (*screenshot*) dari setiap tahapan, mulai dari koneksi *ADB*, proses ekstraksi data, hingga hasil verifikasi hash.

Selain itu, laporan juga secara eksplisit menyampaikan bahwa pesan *Direct Message (DM)* yang mengandung unsur *cyberbullying* tidak berhasil ditemukan dalam proses analisis. Hal ini dijelaskan secara objektif sebagai akibat dari penghapusan pesan oleh pelaku sebelum proses akuisisi dilakukan, serta adanya mekanisme penghapusan permanen yang diterapkan oleh aplikasi *Instagram*.

Penyajian hasil secara jujur dan transparan ini bertujuan untuk menjaga integritas ilmiah penelitian, serta memberikan gambaran yang realistis mengenai kemampuan dan keterbatasan metode forensik digital yang digunakan. Dengan demikian, laporan yang dihasilkan tidak hanya menyampaikan keberhasilan proses *investigasi*, tetapi juga mengungkap keterbatasan yang ditemui selama penelitian.

Berdasarkan seluruh tahapan yang telah dilakukan, laporan forensik digital dalam penelitian ini telah memenuhi prinsip-prinsip dasar forensik, yaitu:

a. Keaslian (*Authenticity*): data tidak mengalami perubahan sejak proses akuisisi
b. Integritas (*Integrity*): dibuktikan melalui verifikasi *hash MD5* dan *SHA1*
c. Keterulangan (*Repeatability*): proses dapat direplikasi dengan langkah yang sama
d. Akuntabilitas (*Accountability*): setiap tahapan terdokumentasi dengan jelas

Dengan terpenuhinya prinsip-prinsip tersebut, hasil laporan forensik digital yang dihasilkan dalam penelitian ini dapat dijadikan sebagai referensi ilmiah maupun sebagai dasar pendukung dalam proses pembuktian pada kasus *cyberbullying* berbasis digital.

Pembahasan Implementasi Metode *NIJ* dalam *Investigasi* Digital

Berdasarkan hasil penelitian yang telah dilakukan menggunakan metode *National Institute Of Justice (NIJ)*, proses analisis forensik digital pada aplikasi *Instagram* berbasis *Android* menunjukkan bahwa setiap tahapan dalam metode *NIJ* memiliki peran penting dalam memastikan keabsahan dan integritas bukti digital.

Penerapan metode *NIJ* dalam penelitian ini terbukti mampu memberikan alur kerja yang sistematis dan terstruktur dalam proses *investigasi* forensik digital. Tahapan *Identification*, *Collection*, *Examination*, *Analysis*, dan *Reporting* saling berkaitan dan membentuk proses *investigasi* yang komprehensif.

Pada tahap *Identification*, peneliti berhasil mengidentifikasi perangkat, aplikasi, serta jenis data yang berpotensi menjadi barang bukti digital. Keberhasilan tahap ini sangat menentukan keberlanjutan proses *investigasi*, karena kesalahan dalam identifikasi dapat menyebabkan hilangnya bukti penting.

Tahap *Collection* menunjukkan bahwa penggunaan *ADB* mampu melakukan ekstraksi data dari direktori sistem *Android* secara efektif, khususnya pada aplikasi *Instagram*. Selain itu, *FTK Imager* berhasil digunakan untuk membuat *image* forensik dan menghasilkan nilai *hash* yang identik, sehingga membuktikan bahwa data tidak mengalami perubahan selama proses akuisisi. Hal ini sejalan dengan prinsip forensik digital yaitu menjaga integritas (*Integrity*) dan keaslian (*Authenticity*) data.

Pada tahap *Examination*, *File database* utama yaitu *direct.db* berhasil ditemukan dan diverifikasi dalam kondisi utuh. Struktur *database* yang berbasis *SQLite* memudahkan proses penelusuran data, meskipun tidak semua data yang diharapkan dapat ditemukan.

Tahap *Analysis* menjadi bagian paling krusial dalam penelitian ini. Hasil analisis menunjukkan bahwa meskipun *File database* berhasil diakses, pesan *Direct Message (DM)* yang mengandung unsur *cyberbullying* tidak ditemukan.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7 Nomor 4 Agustus 2026, Page 412-423
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Hal ini disebabkan oleh penghapusan data oleh pelaku sebelum proses akuisisi dilakukan. Temuan ini menunjukkan bahwa sistem *Instagram* memiliki mekanisme penghapusan data yang bersifat permanen.

Tahap *Reporting* menghasilkan dokumentasi lengkap yang mencakup seluruh proses *investigasi*. Laporan disusun secara sistematis dan memenuhi prinsip forensik seperti *Repeatability* dan *Accountability*.

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan mengenai analisis barang bukti digital pada aplikasi *Instagram* berbasis *Android* menggunakan metode *National Institute Of Justice (NIJ)*, maka dapat diperoleh beberapa kesimpulan sebagai berikut, Metode *National Institute Of Justice (NIJ)* yang terdiri dari tahapan *Identification*, *Collection*, *Examination*, *Analysis*, dan *Reporting* dapat diterapkan dengan baik dalam proses *investigasi* forensik digital. Setiap tahapan mampu memberikan alur kerja yang terstruktur dalam mengidentifikasi, mengumpulkan, memeriksa, menganalisis, hingga melaporkan bukti digital. Penggunaan *ADB* (*Android Debug Bridge*) dalam proses ekstraksi data dari perangkat *Android* berhasil dilakukan, khususnya dalam mengambil *File database* aplikasi *Instagram*. Selanjutnya, *FTK Imager* berhasil digunakan untuk membuat *image* forensik serta melakukan verifikasi integritas data melalui nilai *hash MD5* dan *SHA1* yang menunjukkan hasil identik (*match*). Hal ini membuktikan bahwa data yang diperoleh bersifat valid dan tidak mengalami perubahan. *File database* utama *Instagram* yaitu *direct.db* berhasil ditemukan dan dianalisis. Namun, pesan *Direct Message (DM)* yang mengandung unsur *cyberbullying* tidak berhasil ditemukan karena telah dihapus oleh pelaku sebelum proses akuisisi dilakukan. Penelitian ini menunjukkan bahwa metode *Logical acquisition* yang digunakan memiliki keterbatasan dalam memulihkan data yang telah dihapus secara permanen. Aplikasi *Instagram* terbukti memiliki mekanisme penghapusan data yang cukup kuat sehingga tidak meninggalkan artefak sisa yang dapat dianalisis kembali. Waktu dalam melakukan pengambilan data menjadi faktor krusial dalam *investigasi* forensik digital. Semakin cepat proses akuisisi dilakukan setelah kejadian, maka semakin besar peluang untuk memperoleh bukti digital yang relevan.

UCAPAN TERIMAKASIH

Penulis mengucapkan puji syukur kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga penelitian ini dapat diselesaikan dengan baik. Penulis juga menyampaikan terima kasih kepada Program Studi Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen, yang telah memberikan dukungan dan fasilitas selama proses penelitian. Ucapan terima kasih juga disampaikan kepada dosen pembimbing, rekan-rekan, serta semua pihak yang telah memberikan arahan, masukan, dan bantuan sehingga penelitian yang berjudul "Analisis Barang Bukti Digital pada Aplikasi *Instagram* Berbasis *Android* Menggunakan Metode *National Institute of Justice (NIJ)*" dapat terselesaikan dengan baik.

REFERENCES

[1] A. M. Rohmy, T. Suratman, and A. I. Nihayaty, "UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi," *Dakwatuna J. Dakwah dan Komun. Islam*, vol. 7, no. 2, p. 309, 2021, doi: 10.54471/dakwatuna.v7i2.1202.

[2] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[3] D. Babel, "*Cyberbullying*, Ancaman Nyata Bagi Anak-anak di Dunia Maya," *JournalArta Ber. Inf. Terkini dan Terbaru*, 2024.

[4] M. Rahmah, D. Valdiani, and P. Handayani, "Pengaruh Pemasaran Media Sosial *Instagram* Terhadap Keputusan Pembelian Produk Bedak Padat Maybelline Di Kota Bogor," vol. 3, no. 1, pp. 192–204, 2026.

[5] M. Fridha, T. Palupi, and F. Norhabiba, "Edukasi Literasi Digital pada Remaja dalam Menangkal *Cyberbullying*," *J. Abdidas*, vol. 2, no. 4, pp. 1014–1020, 2024, doi: https://doi.org/10.31004/abdidas.v2i4.408.

[6] Y. Safitri, F. Firmansyah, and M. A. Mu'min, "Mobile Forensic *Analysis* on IMO Messenger Application Using ACPO and *NIJ* Frameworks," *Insect (Informatics Secur. J. Tek. Inform.*, vol. 11, no. 1, pp. 1–12, 2025, doi: 10.33506/insect.v10i2.4052.

[7] R. A. Soni, Yulia Fatma, "Akuisisi bukti digital aplikasi pesan instan 'bip'menggunakan metode *National Institute Of Justice (NIJ)*," *Vol. 3, No. 1, Juni 2022, hal. 34-42 J. Comput. Sci. Inf. Technol.*, vol. 3, no. 1, pp. 34–42, 2022.

[8] I. Anshori, K. Eka, S. Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada *Smartphone Android* Menggunakan Metode *NIJ*," vol. 5, no. 2, pp. 118–134, 2021.

[9] A. Sukma Setiahawa, N. Syafrin, and S. Arif, "*Cyberbullying* Di Media Sosial *Instagram* Ditinjau Dari Perspektif Islam," *KOLONI J. Multidisiplin Ilmu*, vol. 1, no. 3, pp. 2828–6863, 2022.

[10] Soni, E. Ramadhan, and D. Mualfah, "*Investigasi* Bukti Digital Aplikasi WeChat Menggunakan Framework

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**

Integrated Digital Forensics Proses Model (IDFPM) Berbasis SNI 27037 : 2014," *J. INTEK*, vol. 4, no. 1, pp. 25–31, 2021, doi: 10.37729/intek.v4i1.1114.

[11] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. MEDIA Inform. BUDIDARMA*, vol. 6, no. April, pp. 1263–1271, 2022, doi: 10.30865/mib.v6i2.3946.

[12] E. Pudjiarti, S. Faizah, and S. Hardani, "Analisa Kesadaran Masyarakat Terhadap Bahaya Cybercrime Pada Penggunaan Teknologi dan Media Sosial," vol. 10, no. 1, pp. 24–37, 2023.

[13] A. Primukti, P. K. Sari, D. Suhartono, and K. N. Isnaini, "TIKTOK BERBASIS WEB MENGGUNAKAN METODE *NATIONAL INSTITUTE OF JUSTICE* (*NIJ*)," vol. 13, no. 2, 2025.

[14] S. K. Saad, U. A. Dahlan, U. A. Dahlan, A. Fadlil, and U. A. Dahlan, "Analisis Forensik Aplikasi Dropbox Pada *Android* Menggunakan Metode NIST," pp. 119–123.

[15] 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.

This is an open access article under the CC–BY-SA license

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **25/05/2026**; Accepted: **26/06/2026**; Published:**15/08/2026**