TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

Rekonstruksi Aktivitas Pengguna Situs Judi Online pada Smartphone Android melalui Analisis Digital Forensik

Aji Pangestu[*], Teri Mengkasrinal, Balthasar Sebastian Lumbantobing

Program Studi Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Jayakarta, Jakarta, Indonesia
Email: [1,*]ajikamispahing@gmail.com, [2]mengkasrinal110@gmail.com, [3]balthasar_lumbantobing@stmik.jayakarta.ac.id
Email Penulis Korespondensi: ajikamispahing@gmail.com

Abstrak–*Smartphone* Android menyimpan artefak digital yang dapat digunakan untuk menjelaskan aktivitas pengguna, tetapi mekanisme keamanan Android modern membatasi akses terhadap data internal aplikasi. Penelitian ini bertujuan mengidentifikasi artefak yang dapat diperoleh dari *smartphone* Android 11 *non-root* dan menilai kemampuannya dalam mendukung rekonstruksi aktivitas akses situs judi *online*. Penelitian menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus digital forensik berbasis simulasi di Setiadarma, Tambun Selatan, Bekasi, pada Mei–Juli 2026. Objek uji berupa Redmi 10A Android 11 *non-root*. Akuisisi dilakukan menggunakan MOBILedit Forensic, hasil ekstraksi dipreservasi dengan FTK Imager dan diperiksa menggunakan Autopsy, sedangkan Android Debug Bridge digunakan untuk validasi koneksi serta pengumpulan *netstats* dan *batterystats*. Dokumentasi Google Activity menampilkan entri kunjungan situs simulasi pada perangkat Redmi 10A, sementara *netstats* dan *batterystats* mendukung adanya penggunaan Google Chrome. Namun, riwayat penelusuran, *cookies*, *cache*, database *browser*, file unduhan, tangkapan layar, dan metadata terkait tidak ditemukan pada hasil akuisisi. Google Activity diperlakukan sebagai bukti pendukung tingkat akun, bukan sebagai artefak internal Chrome yang dipulihkan melalui akuisisi *non-root*. Oleh karena itu, rekonstruksi hanya dapat dilakukan secara parsial: penggunaan Chrome dan indikasi kunjungan situs dapat didukung, tetapi pemulihan kronologi *browser* secara lengkap belum dapat dilakukan.

Kata Kunci: Digital Forensik; Android 11; Akuisisi *Non-Root*; Google Activity; *Netstats*; *Batterystats*; Rekonstruksi Aktivitas

Abstract–Android *smartphone*s retain digital artifacts that can help explain user activity, but modern Android security mechanisms restrict access to internal application data. This study identifies artifacts obtainable from a *non-roote*d Android 11 *smartphone* and evaluates their ability to support the reconstruction of *online* gambling *website* access. A descriptive qualitative method with a simulation-based *digital forensic case study* was conducted in Setiadarma, Tambun Selatan, Bekasi, from May to July 2026. The test device was a *non-roote*d Redmi 10A running Android 11. Acquisition was performed using MOBILedit Forensic, the extracted data were preserved with FTK Imager and examined with Autopsy, while Android Debug Bridge was used to validate connectivity and collect *netstats* and *batterystats*. Google Activity documentation displayed a visit entry to the simulated site on the Redmi 10A, while *netstats* and *batterystats* supported the use of Google Chrome. However, browsing *history*, *cookies*, *cache*, *browser* databases, downloaded files, screenshots, and related metadata were not found in the acquisition output. Google Activity was treated as account-level supporting evidence rather than an internal Chrome artifact recovered through *non-root acquisition*. Consequently, the reconstruction remained partial: Chrome use and an indication of the site visit could be supported, but a complete *browser* timeline could not be recovered.

Keywords: Digital Forensics; Android 11; Non-Root Acquisition; Google Activity; Netstats; Batterystats; User Activity Reconstruction

1. PENDAHULUAN

Penggunaan *smartphone* Android telah menjadikan perangkat bergerak sebagai sumber penting bukti digital. Aktivitas komunikasi, akses internet, penggunaan aplikasi, penyimpanan file, dan interaksi akun dapat meninggalkan informasi perangkat, metadata, catatan aplikasi, file media, serta jejak penggunaan layanan. Dalam proses investigasi, bukti tersebut harus dikumpulkan dan dianalisis secara sistematis agar hubungan antara perangkat, pengguna, waktu, dan aktivitas dapat dijelaskan tanpa melampaui kekuatan data yang tersedia. Peran forensik *smartphone* dalam mengungkap jejak digital telah dibahas oleh Aprilia dan Kurniawan (2024), sedangkan Qurrota et al. (2025) dan Ali dan Yustiana (2025) menekankan pentingnya prosedur, integritas, serta interpretasi bukti dalam penegakan hukum berbasis data digital.

Salah satu aktivitas yang relevan untuk diperiksa adalah akses situs judi *online* melalui *browser* pada *smartphone*. Akses berbasis web tidak selalu memerlukan aplikasi khusus dan dapat menghasilkan riwayat penelusuran, *cookies*, *cache*, file unduhan, serta catatan aktivitas akun. Kanda dan Aziz (2024) menggambarkan dampak sosial penggunaan judi *online*, sedangkan Ramdani et al. (2025) menempatkan forensik digital dan open-source intelligence sebagai bagian dari upaya mendeteksi serta menangani cybercrime judi *online*. Riffai Achmad dan Muntasiroh (2024) juga menunjukkan bahwa investigasi pascakejadian pada platform dan web membutuhkan korelasi beberapa sumber karena satu artefak belum tentu cukup untuk menjelaskan keseluruhan aktivitas.

Android modern menerapkan isolasi aplikasi, pembatasan izin, enkripsi, dan direktori privat yang memengaruhi kedalaman akuisisi. Pada kondisi *non-root*, pemeriksa hanya memperoleh data yang dapat diakses melalui antarmuka sistem atau metode yang didukung perangkat. Pendekatan tersebut lebih rendah risiko terhadap perubahan sistem, tetapi tidak selalu dapat mengambil basis data internal aplikasi. Juniansyah et al. (2024) menunjukkan bahwa keamanan dan akses pada Android bergantung pada konfigurasi perangkat, sedangkan Hidayah dan Fachri (2024), Prambudi et al. (2025), serta Mualfah et al. (2025) memperlihatkan bahwa hasil temuan dapat berbeda menurut aplikasi, framework, dan tools forensik yang digunakan. Dengan demikian, keberhasilan koneksi perangkat tidak dapat langsung disamakan dengan keberhasilan memperoleh seluruh artefak.

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

Kerangka *National Institute of Standards and Technology* digunakan untuk menjaga alur pemeriksaan melalui tahap *collection*, *examination*, *analysis*, dan *reporting*. Agustiono et al. (2024) menerapkan metode NIST untuk pemulihan bukti yang dihapus, sedangkan Isnaeni dan Fachri (2025) menerapkannya pada TikTok. Penelitian lain menggunakan DFRWS atau ACPO pada Threads, Discord, dan aplikasi mobile lain (Ajuj et al., 2024; Nirmala et al., 2024). Rifkiansyah et al. (2026) menunjukkan bahwa artefak dari perangkat wearable dapat dikorelasikan untuk pembuktian alibi dan rekonstruksi aktivitas. Kesamaan penelitian tersebut terletak pada kebutuhan untuk memisahkan tahap pengumpulan, pemeriksaan, interpretasi, dan pelaporan agar keluaran tools tidak langsung dianggap sebagai kesimpulan.

Ketelitian identifikasi file dan metadata juga menentukan kualitas rekonstruksi. Fawzan dan Luthfi (2025) membahas identifikasi jenis file pada artefak digital, sedangkan Qonita et al. (2025) menggunakan Autopsy untuk memeriksa metadata lokasi Android. Fahrudin dan Muflih (2024) menunjukkan bahwa struktur aplikasi dan perlindungan data memengaruhi artefak yang dapat diperoleh, sementara Firmansyah (2024) menekankan kesiapan forensik dan dokumentasi proses sebagai bagian dari pengelolaan bukti. Karakteristik perangkat Android sendiri terus berkembang seiring perubahan perangkat keras dan sistem operasi (Syahputra et al., 2024). Oleh sebab itu, temuan negatif, seperti tidak ditemukannya riwayat, *cookies*, atau *cache*, tetap perlu dilaporkan karena menunjukkan batas empiris metode yang digunakan.

Penelitian ini memfokuskan pemeriksaan pada Redmi 10A dengan Android 11 dalam kondisi *non-root* yang digunakan untuk menjalankan skenario akses situs judi *online* melalui Google Chrome. MOBILedit Forensic digunakan sebagai alat akuisisi utama, Android Debug Bridge digunakan untuk validasi koneksi serta memperoleh *netstats* dan *batterystats*, FTK Imager digunakan untuk preservasi dan peninjauan hasil ekstraksi, sedangkan Autopsy digunakan untuk memeriksa struktur file serta artefak yang tersedia. Google Activity dikumpulkan sebagai bukti pendukung tingkat akun, bukan sebagai artefak internal Chrome hasil ekstraksi. Celah penelitian terletak pada masih terbatasnya pembahasan yang membedakan secara tegas antara aktivitas yang terlihat pada layanan akun, aktivitas yang dapat didukung oleh statistik sistem, dan artefak *browser* yang benar-benar berhasil dipulihkan melalui akuisisi *non-root*. Banyak penelitian terdahulu menitikberatkan artefak yang berhasil ditemukan, sedangkan kondisi ketika sumber data internal tidak dapat diperoleh masih jarang dijelaskan sebagai temuan utama. Penelitian ini karena itu tidak hanya mencatat keluaran *tools*, tetapi juga menilai asal bukti, kedalaman informasi, kemampuan verifikasi ulang, dan batas kesimpulan yang dapat dibuat. Tujuan penelitian adalah mengidentifikasi data yang dapat dan tidak dapat diperoleh, menilai keterkaitan temuan dengan skenario aktivitas, serta menentukan tingkat rekonstruksi. Kontribusi penelitian terletak pada pemisahan yang tegas antara artefak hasil akuisisi *non-root*, artefak sistem pendukung, dan dokumentasi akun agar kesimpulan tidak melampaui bukti.

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus digital forensik berbasis simulasi. Simulasi diposisikan sebagai prosedur untuk menghasilkan artefak, bukan sebagai jenis penelitian utama. Pengujian dilakukan di lingkungan pengujian pribadi peneliti di Setiadarma, Tambun Selatan, Bekasi, Jawa Barat, pada Mei–Juli 2026. Perangkat uji yang digunakan adalah Redmi 10A dengan Android 11, RAM 3 GB, penyimpanan internal 32 GB, dan status *non-root*. Objek penelitian adalah artefak digital yang muncul atau berpotensi tertinggal setelah aktivitas akses situs melalui Google Chrome. Penelitian tidak menganalisis server, basis data, keamanan jaringan, transaksi perjudian, maupun akun pihak lain. Unit analisis berupa satu perangkat uji dan keluaran digitalnya, bukan responden manusia. Rangkuman tahapan penelitian dan fungsi setiap perangkat lunak ditunjukkan pada Tabel 1.

Tabel 1. Tahapan Penelitian dan Fungsi Perangkat Lunak

Tahap	Aktivitas Utama	Tools/Sumber	Keluaran
Persiapan	Mencatat kondisi perangkat, waktu, dan status non-root	Dokumentasi manual	Kondisi awal perangkat
Dokumentasi akun	Merekam entri aktivitas yang tampil pada akun Google	Google Activity	Bukti pendukung tingkat akun
Validasi dan artefak sistem	Memastikan perangkat terdeteksi serta mengambil netstats dan batterystats	Android Debug Bridge	Status koneksi dan statistik penggunaan aplikasi
Akuisisi	Mengambil data yang masih dapat diakses secara logis	MOBILedit Forensic	Folder ekstraksi dan laporan akuisisi
Preservasi/peninjauan	Meninjau struktur dan mendokumentasikan hasil ekstraksi	FTK Imager	Struktur file dan nilai hash apabila tersedia
Pemeriksaan	Mencari file, metadata, dan artefak browser pada data ekstraksi	Autopsy	Temuan dan artefak yang tidak ditemukan
Analisis/pelaporan	Mengorelasikan seluruh sumber dan menyusun batas rekonstruksi	Analisis kualitatif	Status rekonstruksi dan keterbatasan

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

2.2 Tahapan dan Skenario Penelitian

Tahapan penelitian disusun dengan mengadaptasi proses *collection*, *examination*, *analysis*, dan *reporting*. Sebelum akuisisi, kondisi perangkat, status *non-root*, waktu, koneksi USB, dan USB debugging dicatat. Dokumentasi Google Activity dikumpulkan melalui antarmuka akun sebagai bukti pendukung yang terpisah dari hasil ekstraksi. Setelah skenario dijalankan, MOBILedit Forensic digunakan untuk melakukan akuisisi terhadap data yang masih dapat diakses tanpa modifikasi sistem. Android Debug Bridge digunakan untuk memastikan perangkat terdeteksi serta mengumpulkan data sistem melalui perintah *dumpsys netstats* dan *dumpsys batterystats*. Folder hasil ekstraksi dipreservasi dan ditinjau menggunakan FTK Imager, termasuk dokumentasi struktur file dan nilai hash apabila tersedia. Selanjutnya, folder hasil ekstraksi dimasukkan ke Autopsy sebagai sumber data untuk memeriksa file, direktori, metadata, dan kemungkinan artefak *browser*.

Skenario aktivitas dirancang agar setiap langkah memiliki waktu acuan yang dapat dibandingkan dengan hasil pemeriksaan. Perangkat disiapkan pada pukul 21.30 WIB, Google Chrome dibuka pada pukul 21.32 WIB, situs simulasi diakses pada pukul 21.33 WIB, gambar diunduh pada pukul 21.35 WIB, halaman permainan dibuka pada pukul 21.38 WIB, dan sebagian aktivitas dihapus pada pukul 21.39 WIB. Aktivitas ini dipilih untuk menghasilkan beberapa kategori artefak yang relevan, yaitu informasi perangkat, daftar aplikasi, file gambar, tangkapan layar, file unduhan, metadata file, riwayat penelusuran, *cookies*, dan *cache*. Waktu skenario tidak diperlakukan sebagai bukti dengan sendirinya, melainkan sebagai data pembanding saat mengevaluasi artefak yang diperoleh.
Urutan waktu skenario yang digunakan sebagai data pembanding ditampilkan pada Tabel 2.

Tabel 2. Skenario Aktivitas Pengguna

Waktu	Aktivitas	Tujuan Pembentukan Artefak
17.00 WIB	*Smartphone* disiapkan dalam kondisi aktif dan *non-root*	Informasi perangkat dan kondisi awal
17.01 WIB	Google Chrome dibuka	Informasi penggunaan aplikasi
17.03 WIB	Situs simulasi diakses	Riwayat penelusuran dan data sesi
17.04 WIB	Gambar diunduh	File unduhan dan metadata
17.05 WIB	Halaman permainan dibuka	*Cache*, *cookies*, dan histori
17.40 WIB	Sebagian aktivitas dihapus	Pengujian persistensi artefak

2.3 Teknik Pemeriksaan dan Analisis

Pada tahap *examination*, setiap keluaran diperiksa berdasarkan nama file, lokasi penyimpanan, ukuran, ekstensi, metadata waktu, dan keterkaitannya dengan aktivitas yang disimulasikan. Artefak dibedakan menjadi artefak primer, artefak sistem pendukung, dan dokumentasi akun/observasi. Artefak primer meliputi riwayat penelusuran, *cookies*, *cache*, basis data *browser*, file unduhan, tangkapan layar, dan metadata. Artefak sistem pendukung meliputi informasi perangkat, daftar aplikasi, *netstats*, *batterystats*, dan laporan akuisisi. Google Activity ditempatkan sebagai dokumentasi akun karena diperoleh dari antarmuka layanan Google dan bukan dari direktori internal Chrome pada paket ekstraksi. Temuan dikelompokkan menjadi ditemukan dan relevan, ditemukan tetapi mendukung secara tidak langsung, serta tidak ditemukan pada hasil akuisisi.

Keabsahan analisis dijaga melalui dokumentasi kondisi perangkat, pencatatan waktu skenario, pembagian fungsi tools, dan pemeriksaan silang antara laporan MOBILedit Forensic, struktur hasil pada FTK Imager, hasil ingest pada Autopsy, keluaran Android Debug Bridge, serta dokumentasi Google Activity. Penelitian tidak menyamakan riwayat yang terlihat langsung pada antarmuka Google Chrome atau Google Activity dengan artefak internal *browser* yang berhasil diakuisisi. *Netstats* dan *batterystats* juga tidak diperlakukan sebagai bukti URL karena keduanya hanya menunjukkan aktivitas jaringan dan penggunaan aplikasi. Pelaporan mencakup temuan positif maupun artefak yang tidak berhasil diperoleh agar ketiadaan data pada keluaran tools tidak disalahartikan sebagai ketiadaan aktivitas pada perangkat.

Analisis dilakukan secara kualitatif terhadap keberadaan, konteks, hubungan waktu, dan kecukupan setiap artefak. Suatu aktivitas dinyatakan dapat didukung apabila tersedia artefak yang berkaitan langsung atau beberapa artefak pendukung yang konsisten. Aktivitas dinyatakan terbatas apabila hanya dapat disimpulkan pada tingkat penggunaan aplikasi tanpa informasi URL atau isi halaman. Aktivitas dinyatakan tidak dapat direkonstruksi apabila artefak utama yang dibutuhkan tidak ditemukan. Karena hanya menggunakan satu perangkat, hasil penelitian tidak digeneralisasi untuk seluruh perangkat Android.

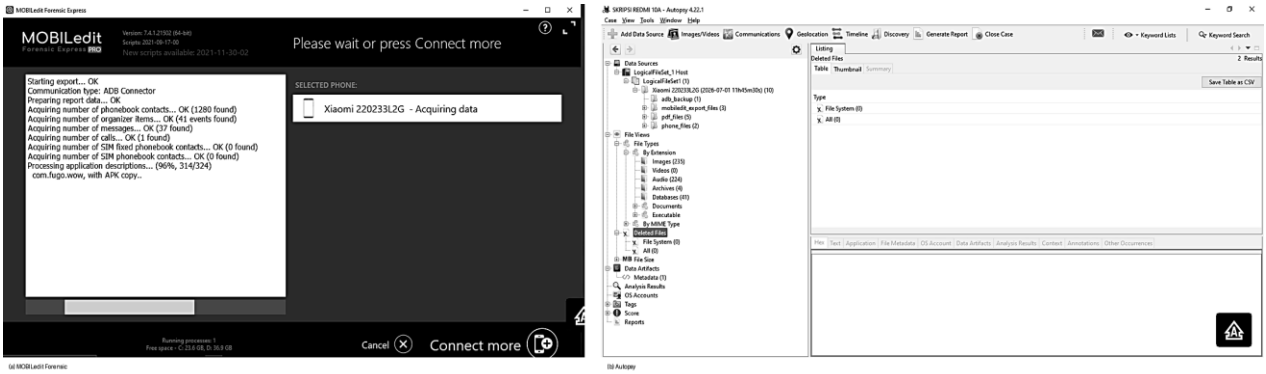
3. HASIL DAN PEMBAHASAN

3.1 Hasil Akuisisi dan Pemeriksaan

Proses akuisisi dimulai setelah skenario aktivitas selesai. *Smartphone* dapat dikenali oleh komputer dan terhubung ke MOBILedit Forensic, sehingga informasi dasar perangkat dan daftar aplikasi yang terpasang dapat dikumpulkan. Keberadaan Google Chrome pada daftar aplikasi mendukung bahwa *browser* tersebut tersedia pada perangkat uji, tetapi belum membuktikan halaman yang dibuka atau tindakan yang dilakukan di dalamnya. Laporan MOBILedit Forensic mendokumentasikan bahwa proses ekstraksi telah dijalankan pada perangkat yang sama. Hasil ekstraksi kemudian

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

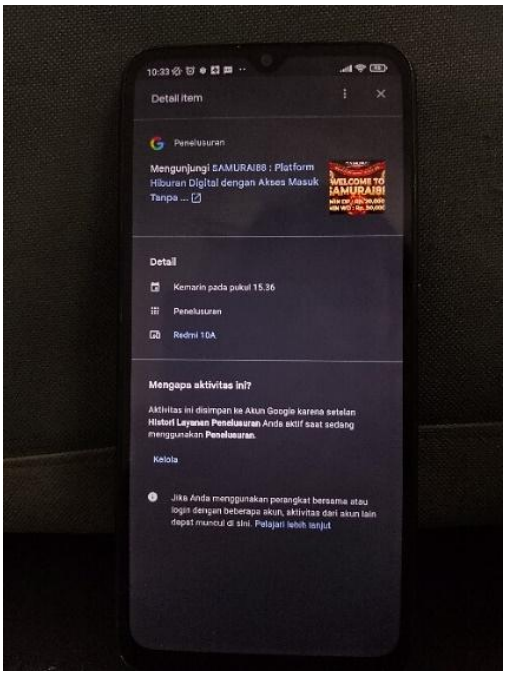
ditinjau menggunakan FTK Imager dan dimasukkan ke Autopsy untuk pemeriksaan lanjutan. Proses koneksi, akuisisi, dan pemeriksaan hasil ekstraksi ditunjukkan pada Gambar 1.



Gambar 1. Proses akuisisi menggunakan MOBILedit Forensic dan pemeriksaan menggunakan Autopsy

Pemeriksaan terhadap artefak primer memberikan hasil terbatas. File gambar yang direncanakan sebagai artefak unduhan tidak ditemukan pada keluaran yang diperiksa. Tangkapan layar, file unduhan, dan metadata terkait juga tidak tersedia untuk dikorelasikan dengan waktu skenario. Pada sisi *browser*, riwayat penelusuran, *cookies*, *cache*, serta basis data internal Google Chrome tidak berhasil ditemukan dalam folder hasil ekstraksi maupun hasil pemeriksaan Autopsy. Dengan demikian, informasi perangkat dan daftar aplikasi merupakan temuan dari hasil akuisisi utama, sedangkan artefak primer yang dapat menunjukkan URL, sesi, isi halaman, atau aktivitas pengunduhan tidak tersedia.

Selain keluaran akuisisi utama, tahap *collection* juga mencakup dokumentasi Google Activity yang terhubung dengan perangkat. Pada Gambar 2 terlihat entri kunjungan ke situs simulasi dan identitas perangkat Redmi 10A. Bukti ini mendukung bahwa akun Google pada perangkat merekam aktivitas penelusuran yang berkaitan dengan objek simulasi.

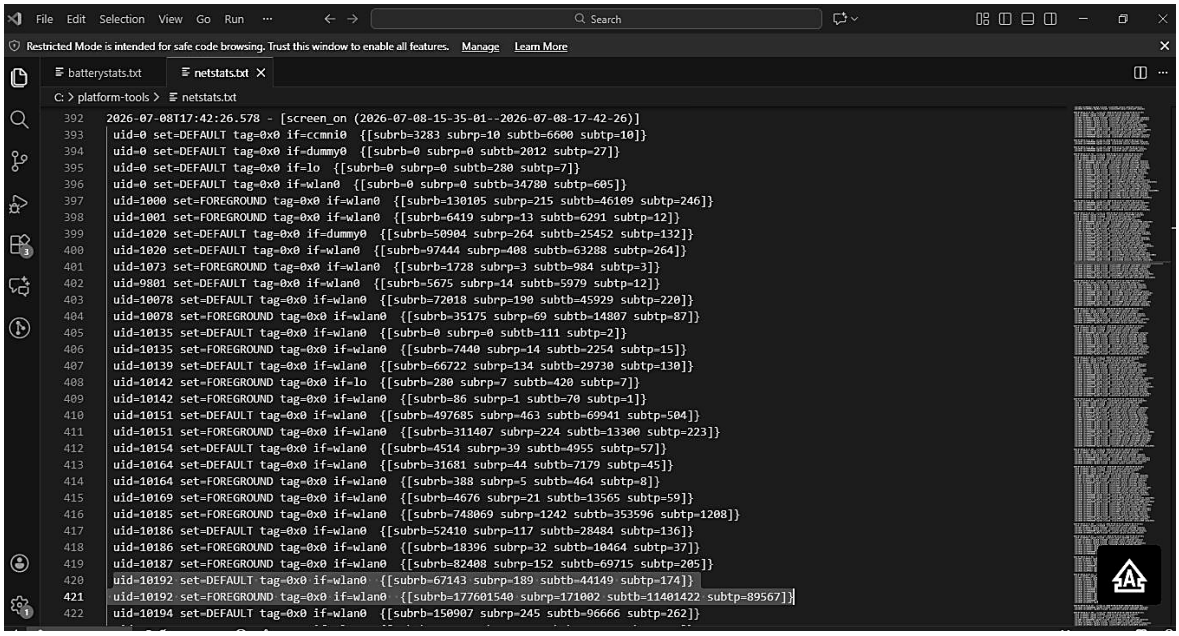


Gambar 2. Bukti pendukung kunjungan situs pada Google Activity

Google Activity tidak diperlakukan sebagai riwayat Chrome yang berhasil dipulihkan dari folder hasil akuisisi. Data tersebut diperoleh melalui antarmuka akun Google dan dikategorikan sebagai bukti pendukung tingkat akun/observasi. Tampilan waktunya bersifat relatif terhadap saat bukti dibuka, sehingga tidak digunakan sebagai satu-satunya dasar untuk mengesahkan urutan waktu skenario. Nilai forensiknya adalah menguatkan indikasi kunjungan situs, sedangkan keberhasilan akuisisi *non-root* terhadap basis data internal Chrome tetap tidak dapat dinyatakan.

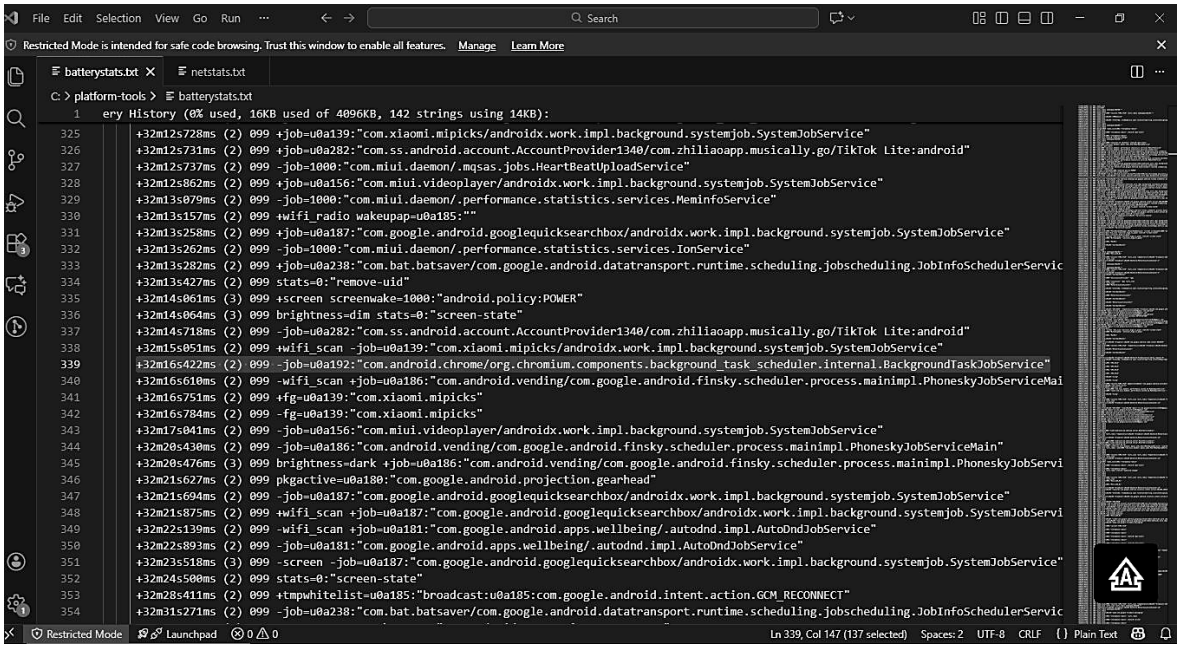
Di luar hasil ekstraksi utama, Android Debug Bridge menghasilkan artefak sistem pendukung berupa *netstats*. Data ini mencatat statistik jumlah data yang dikirim dan diterima oleh aplikasi. Hasil pemeriksaan menunjukkan adanya aktivitas transfer data pada UID yang dikaitkan dengan Google Chrome dalam keluaran pendukung penelitian. Temuan tersebut dapat mendukung adanya penggunaan jaringan oleh Chrome, tetapi tidak menunjukkan alamat URL, isi halaman, atau situs tertentu. Contoh keluaran *netstats* ditunjukkan pada Gambar 3.

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709



Gambar 3. Hasil pengumpulan netstats menggunakan Android Debug Bridge

Android Debug Bridge juga menghasilkan *batterystats* yang memuat catatan aktivitas aplikasi, termasuk proses latar belakang dan identitas paket com.android.chrome. Data ini mendukung bahwa Google Chrome aktif pada perangkat dalam periode pencatatan sistem. *Batterystats* tetap dapat berfungsi sebagai artefak pendukung meskipun riwayat penelusuran dihapus karena catatan tersebut dikelola oleh sistem Android, bukan oleh basis data internal Chrome. Namun, seperti *netstats*, *batterystats* tidak dapat membuktikan URL atau halaman spesifik yang diakses. Contoh keluarannya ditunjukkan pada Gambar 4.



Gambar 4. Hasil pengumpulan batterystats menggunakan Android Debug Bridge

Ringkasan status setiap kategori artefak dan interpretasinya disajikan pada Tabel 3.

Tabel 3. Hasil Pemeriksaan Artefak Digital

No.	Kategori Artefak	Status	Interpretasi
1	Informasi perangkat	Ditemukan	Mendukung identifikasi perangkat dan kondisi pemeriksaan
2	Daftar aplikasi	Ditemukan	Menunjukkan Google Chrome terpasang, tetapi tidak membuktikan URL yang diakses

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

No.	Kategori Artefak	Status	Interpretasi
3	Google Activity	Ditemukan sebagai dokumentasi akun	Menampilkan entri kunjungan situs pada Redmi 10A, tetapi bukan hasil ekstraksi internal Chrome
4	File gambar	Tidak ditemukan	Tidak dapat digunakan sebagai bukti hasil unduhan
5	Tangkapan layar	Tidak ditemukan pada hasil akuisisi	Tidak tersedia sebagai artefak hasil ekstraksi
6	File unduhan	Tidak ditemukan	Aktivitas pengunduhan tidak dapat dibuktikan dari hasil akuisisi
7	Metadata file	Tidak ditemukan	Korelasi waktu dan lokasi file tidak dapat dilakukan
8	Riwayat browser	Tidak ditemukan	Akses situs tidak dapat diverifikasi dari basis data histori hasil akuisisi
9	Cookies	Tidak ditemukan	Data sesi tidak tersedia pada ekstraksi non-root
10	Cache	Tidak ditemukan	Konten halaman tidak dapat direkonstruksi dari cache
11	Netstats	Ditemukan	Mendukung aktivitas jaringan Chrome, tetapi tidak memuat URL
12	Batterystats	Ditemukan	Mendukung aktivitas paket Chrome, tetapi tidak memuat halaman yang diakses

3.2 Upaya Rekonstruksi Aktivitas Pengguna

Ketiadaan artefak *browser* harus ditafsirkan secara hati-hati. Setelah skenario, riwayat akses masih dapat dilihat secara langsung pada antarmuka Google Chrome dan Google Activity menampilkan entri kunjungan ke situs simulasi. Akan tetapi, riwayat tersebut tidak muncul sebagai file atau basis data pada keluaran MOBILedit Forensic dan Autopsy. Pada saat yang sama, *netstats* dan *batterystats* mendukung bahwa Google Chrome digunakan. Korelasi ini memberikan dukungan pada tingkat akun dan penggunaan aplikasi, tetapi tidak mengubah fakta bahwa akuisisi *non-root* tidak berhasil memperoleh *history*, *cookies*, *cache*, atau basis data internal Chrome. Oleh karena itu, dokumentasi Google Activity diperlakukan sebagai bukti pendukung yang dapat diperiksa secara visual, bukan sebagai bukti bahwa artefak internal *browser* telah dipulihkan.

Hasil tersebut konsisten dengan karakteristik akuisisi *non-root* pada Android modern. Google Chrome menyimpan data penting pada ruang privat aplikasi yang dilindungi mekanisme isolasi Android. Ketika alat tidak memperoleh izin untuk membaca direktori tersebut, basis data histori, *cookies*, *cache*, dan data sesi tidak ikut masuk ke paket ekstraksi. Autopsy dan FTK Imager hanya dapat memeriksa sumber data yang telah berhasil diperoleh dan tidak menggantikan metode akuisisi yang memiliki akses lebih dalam. Sebaliknya, *netstats* dan *batterystats* dapat diambil melalui layanan sistem sehingga tetap tersedia sebagai artefak pendukung, walaupun kedalamannya tidak setara dengan artefak internal *browser*.

Upaya rekonstruksi dilakukan dengan membandingkan delapan tahap pemeriksaan dengan seluruh sumber yang tersedia. Kondisi *smartphone* dan pelaksanaan akuisisi dapat didukung oleh informasi perangkat serta laporan MOBILedit Forensic. Pembukaan atau penggunaan Google Chrome didukung secara tidak langsung oleh daftar aplikasi, *netstats*, dan *batterystats*. Kunjungan ke situs simulasi memperoleh dukungan tambahan dari Google Activity, tetapi dukungan tersebut berada pada tingkat akun/observasi dan bukan dari basis data *history* hasil akuisisi. Pengunduhan gambar tidak dapat dibuktikan karena file dan metadata tidak ditemukan; pembukaan halaman permainan tidak dapat direkonstruksi melalui *cache*, *cookies*, atau *history*; dan penghapusan sebagian aktivitas tidak menghasilkan artefak terpulihkan yang dapat dibandingkan. Hasil ini menunjukkan bahwa rekonstruksi bersifat parsial dan sumber bukti harus disebutkan secara terpisah.

Dengan hasil tersebut, rekonstruksi tidak dapat disusun sebagai kronologi forensik lengkap yang seluruh tahapnya berasal dari hasil akuisisi *non-root*. Kronologi skenario tetap digunakan sebagai acuan pengujian, sedangkan Google Activity memberi dukungan kontekstual terhadap kunjungan situs dan *netstats* serta *batterystats* mendukung penggunaan Chrome. Penelitian dapat menyatakan bahwa perangkat uji teridentifikasi, Google Chrome terpasang dan digunakan, entri kunjungan situs terlihat pada akun Google, proses akuisisi telah dilakukan, serta hasil pemeriksaan tidak memuat artefak internal *browser*. Pembedaan tersebut mencegah dokumentasi skenario atau bukti akun dianggap sebagai hasil pemulihan basis data Chrome. Status dukungan terhadap setiap langkah rekonstruksi dirangkum pada Tabel 4.

Tabel 4. Status Rekonstruksi Aktivitas Pengguna

No.	Aktivitas	Bukti yang Tersedia	Status Rekonstruksi
1	Smartphone digunakan	Informasi perangkat dan koneksi	Dapat didukung
2	Google Chrome dibuka	Daftar aplikasi, netstats, dan batterystats	Dapat didukung secara tidak langsung

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

No.	Aktivitas	Bukti yang Tersedia	Status Rekonstruksi
3	Situs simulasi diakses	Google Activity menampilkan entri kunjungan; history internal tidak ditemukan	Didukung terbatas oleh bukti akun, bukan artefak internal Chrome
4	Gambar diunduh	File unduhan dan metadata tidak ditemukan	Tidak dapat dibuktikan dari hasil akuisisi
5	Halaman permainan dibuka	Cache, cookies, history, dan URL internal tidak ditemukan	Tidak dapat direkonstruksi secara spesifik
6	Sebagian aktivitas dihapus	Artefak terpulihkan tidak ditemukan	Menunjukkan batas akuisisi non-root
7	Akuisisi dilakukan	Laporan MOBILedit Forensic	Dapat didukung
8	Pemeriksaan dilakukan	Autopsy tidak menemukan artefak Chrome; ADB memperoleh statistik pendukung	Mendukung rekonstruksi parsial

3.3 Analisis Keterbatasan Akuisisi Non-Root

Evaluasi terhadap kekuatan bukti dilakukan dengan membedakan artefak primer, artefak sistem pendukung, dokumentasi akun, dan dokumentasi skenario. Artefak primer adalah data yang secara langsung merekam tindakan tertentu, seperti basis data *History*, entri URL, *cookies* sesi, *cache* halaman, atau file unduhan beserta metadata. Artefak sistem pendukung meliputi *netstats* dan *batterystats* yang dapat menunjukkan aktivitas jaringan serta penggunaan Google Chrome, tetapi tidak menjelaskan halaman yang dibuka. Google Activity termasuk dokumentasi akun karena menampilkan entri aktivitas yang tersimpan pada layanan Google, sedangkan foto dan catatan waktu skenario digunakan sebagai konteks pengujian. Dalam penelitian ini, artefak primer tidak berhasil diperoleh, tetapi dokumentasi akun dan artefak sistem pendukung tersedia. Oleh sebab itu, kunjungan situs dapat didukung secara terbatas, sedangkan keberhasilan pemulihan riwayat internal Chrome tidak dapat dinyatakan.

Pembedaan tersebut membantu mencegah dua kesalahan interpretasi. Kesalahan pertama adalah *false negative*, yaitu menyimpulkan bahwa aktivitas tidak terjadi hanya karena artefak internal tidak ditemukan. Kegagalan ekstraksi, pembatasan izin, enkripsi, atau perubahan struktur aplikasi dapat menyebabkan data tidak tersedia pada hasil akuisisi. Kesalahan kedua adalah *false attribution*, yaitu menghubungkan artefak umum dengan aktivitas spesifik tanpa bukti langsung. *Netstats* dapat menunjukkan transfer data oleh Chrome dan *batterystats* dapat menunjukkan aplikasi aktif, tetapi keduanya tidak dapat mengidentifikasi URL. Karena itu, setiap kesimpulan pada tabel rekonstruksi dibatasi sesuai kekuatan dan kedalaman data yang mendukungnya. Hasil penelitian juga menegaskan pentingnya pelaporan artefak yang ditemukan maupun tidak ditemukan. Tabel hasil memisahkan informasi perangkat dan daftar aplikasi yang diperoleh melalui akuisisi, Google Activity yang diperoleh sebagai dokumentasi akun, *netstats* dan *batterystats* yang diperoleh melalui Android Debug Bridge, serta riwayat *browser*, *cookies*, *cache*, file unduhan, tangkapan layar, dan metadata yang tidak tersedia pada hasil ekstraksi. Transparansi ini membentuk audit trail yang lebih jelas dan menunjukkan bahwa dukungan terhadap kunjungan situs berasal dari sumber akun, bukan dari keberhasilan mengambil basis data *history* melalui MOBILedit Forensic.

3.4 Perbandingan dengan Penelitian Terdahulu

Temuan penelitian ini dapat dibandingkan dengan penelitian Isnaeni dan Fachri (2025), Ajuj et al. (2024), dan Nirmala et al. (2024), yang memperoleh artefak dari TikTok, Threads, dan Discord menggunakan framework digital forensik yang terstruktur. Rifkiansyah et al. (2026) juga berhasil mengorelasikan artefak smartwatch untuk rekonstruksi aktivitas. Perbedaannya, penelitian ini menghadapi keterbatasan pada tahap ketersediaan sumber data: basis data internal Google Chrome tidak masuk ke hasil akuisisi *non-root*. Oleh karena itu, teknik analisis lanjutan hanya dapat diterapkan pada file dan keluaran yang benar-benar tersedia, sedangkan Google Activity harus diposisikan sebagai sumber pendukung tingkat akun. Perbandingan antar-tools pada penelitian Mualfah et al. (2025) menunjukkan bahwa jumlah dan jenis bukti dapat berbeda menurut perangkat lunak forensik yang digunakan. Hidayah dan Fachri (2024) serta Prambudi et al. (2025) juga memperlihatkan bahwa objek aplikasi, kondisi perangkat, dan framework memengaruhi hasil. Qonita et al. (2025) menunjukkan kemampuan Autopsy dalam pemeriksaan metadata ketika sumber data tersedia. Temuan tersebut mendukung penjelasan bahwa Autopsy dan FTK Imager tidak dapat mengompensasi data internal yang tidak berhasil diperoleh pada tahap akuisisi. Kualitas rekonstruksi ditentukan oleh rantai *collection*, *examination*, *analysis*, dan *reporting* secara keseluruhan.

Agustiono et al. (2024) menunjukkan bahwa pemulihan bukti yang dihapus membutuhkan metode dan sumber data yang sesuai, sedangkan Fahrudin dan Muflih (2024) memperlihatkan bahwa perlindungan aplikasi dapat membatasi artefak yang tersedia. Firmansyah (2024) menekankan kesiapan forensik dan dokumentasi agar proses pemeriksaan dapat ditelusuri, dan Ali dan Yustiana (2025) menempatkan integritas bukti sebagai unsur penting dalam penyelidikan. Penelitian ini sejalan dengan prinsip tersebut dengan melaporkan asal setiap bukti secara eksplisit: Google Activity sebagai dokumentasi akun, *netstats* dan *batterystats* sebagai artefak sistem, serta hasil MOBILedit Forensic sebagai keluaran akuisisi utama.

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

3.5 Implikasi dan Keterbatasan Penelitian

Penggunaan kerangka NIST membantu menempatkan setiap hasil pada tahap yang benar. Pada *collection*, perangkat, dokumentasi skenario, Google Activity, hasil MOBILedit Forensic, *netstats*, dan *batterystats* dikumpulkan. Pada *examination*, file dan folder yang tersedia ditinjau menggunakan FTK Imager dan Autopsy, sedangkan keluaran Android Debug Bridge dan tampilan Google Activity diperiksa sesuai sumbernya. Pada *analysis*, seluruh temuan dibandingkan dengan skenario untuk menentukan batas inferensi. Pada *reporting*, artefak positif dan negatif disampaikan secara eksplisit. Pendekatan ini sejalan dengan Agustiono et al. (2024), tetapi hasil pada media atau aplikasi lain tidak dapat langsung digeneralisasi ke Android 11 yang memiliki mekanisme izin dan isolasi aplikasi berbeda.

Temuan negatif dalam penelitian ini tetap memiliki nilai ilmiah. Hasil tersebut memberikan batas empiris bagi akuisisi *non-root* pada konfigurasi perangkat yang diuji dan mencegah anggapan bahwa tidak ditemukannya *history*, *cookies*, atau *cache* berarti aktivitas tidak pernah terjadi. Google Activity menunjukkan bahwa aktivitas akun dapat tetap tercatat di luar paket ekstraksi, sedangkan *netstats* dan *batterystats* menunjukkan bahwa artefak sistem dapat melengkapi pemeriksaan ketika artefak aplikasi tidak tersedia. Namun, korelasi multi-sumber tetap diperlukan dan setiap sumber harus dinilai menurut asal, waktu, serta kedalaman informasinya.

Dari sisi penggunaan alat, MOBILedit Forensic bermanfaat untuk mengidentifikasi perangkat, menjalankan ekstraksi yang didukung, dan menghasilkan laporan terstruktur. Android Debug Bridge tidak menjadi alat akuisisi utama, tetapi berfungsi untuk validasi koneksi serta memperoleh *netstats* dan *batterystats*. FTK Imager digunakan untuk preservasi, peninjauan struktur hasil ekstraksi, dan dokumentasi nilai hash, sedangkan Autopsy membantu pencarian, klasifikasi file, dan pemeriksaan metadata pada sumber data yang tersedia. Pembagian ini menunjukkan bahwa tidak ditemukannya artefak Chrome bukan berarti alat pemeriksaan tidak mampu menganalisisnya, melainkan karena sumber data internal yang diperlukan tidak berhasil masuk ke hasil akuisisi. Implikasi praktisnya adalah bahwa akuisisi *non-root* lebih sesuai diposisikan sebagai metode pemeriksaan awal atau triase. Metode ini dapat menghasilkan profil perangkat, daftar aplikasi, laporan ekstraksi, serta statistik sistem tertentu, tetapi belum tentu cukup untuk rekonstruksi aktivitas *browser* yang spesifik. Untuk memperoleh bukti URL dan data sesi, pemeriksa dapat mempertimbangkan *file system acquisition*, *physical acquisition*, ekstraksi berbasis agen yang didukung perangkat, atau sumber *cloud* yang diperoleh secara legal. Metode yang lebih dalam tetap harus mempertimbangkan legalitas, risiko perubahan sistem, dokumentasi, kemampuan pengulangan, model perangkat, patch keamanan, versi Android, dan status enkripsi.

Penelitian ini memiliki beberapa keterbatasan. Pengujian hanya menggunakan satu Redmi 10A Android 11, satu *browser*, satu skenario, dan satu rangkaian tools, sehingga hasil tidak dapat digeneralisasi ke seluruh perangkat Android. Penelitian tidak membandingkan kondisi *root* dan *non-root*, tidak menggunakan *file system acquisition* atau *physical acquisition*, serta tidak memeriksa server penyedia layanan. *Netstats* dan *batterystats* hanya memberikan bukti penggunaan aplikasi secara tidak langsung dan tidak memuat URL. Google Activity menggunakan tampilan waktu relatif dan dikumpulkan sebagai dokumentasi akun, sehingga tidak dipakai sebagai satu-satunya *timestamp* untuk menyusun urutan kejadian. Perubahan versi aplikasi dan pembaruan keamanan juga dapat menghasilkan temuan berbeda.

Meskipun demikian, keterbatasan tersebut memperjelas ruang kontribusi penelitian. Fokus pada satu konfigurasi memungkinkan hubungan antara jenis akses, sumber bukti, keluaran tools, dan tingkat rekonstruksi dijelaskan secara rinci. Keberhasilan koneksi perangkat dan tersedianya laporan akuisisi belum cukup untuk menyatakan rekonstruksi berhasil. Rekonstruksi memiliki dasar yang lebih kuat ketika artefak spesifik dapat ditemukan, diverifikasi, dan dikorelasikan, sedangkan bukti akun harus tetap dibedakan dari hasil ekstraksi. Prinsip ini juga terlihat pada penelitian aplikasi dan perangkat lain yang menggunakan tahapan terstruktur (Ajuj et al., 2024; Rifkiansyah et al., 2026). Kontribusi utama penelitian adalah penetapan batas inferensi dari akuisisi *non-root* secara transparan.

3.6 Ringkasan Jawaban Rumusan Masalah

Ringkasan jawaban terhadap tiga rumusan masalah disusun berdasarkan hasil akuisisi, pemeriksaan, dan korelasi artefak. Ringkasan ini membedakan data yang berhasil diperoleh, fungsi temuan dalam rekonstruksi, serta batas metode non-root sebagaimana ditunjukkan pada Tabel 5.

Tabel 5. Ringkasan Jawaban Rumusan Masalah

No.	Rumusan Masalah	Hasil Penelitian
1	Artefak apa yang dapat diperoleh melalui akuisisi non-root?	MOBILedit Forensic memperoleh informasi perangkat dan daftar aplikasi. Pengumpulan pendukung juga menghasilkan netstats dan batterystats melalui Android Debug Bridge. Riwayat browser, cookies, cache, basis data Chrome, file unduhan, tangkapan layar, dan metadata terkait tidak ditemukan pada hasil akuisisi.
2	Bagaimana artefak digunakan untuk rekonstruksi aktivitas?	Informasi perangkat dan aplikasi mendukung identifikasi objek. Netstats dan batterystats mendukung penggunaan Chrome. Google Activity menampilkan entri kunjungan situs sebagai bukti tingkat akun, tetapi bukan hasil pemulihan history internal Chrome. Rekonstruksi karena itu bersifat parsial.

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

No.	Rumusan Masalah	Hasil Penelitian
3	Apa kendala dan keterbatasan metode non-root?	Direktori privat Google Chrome tidak dapat diakses melalui metode yang digunakan pada Android 11. Akibatnya, artefak primer browser tidak tersedia dan bukti pendukung tidak dapat menggantikan basis data internal untuk menyusun kronologi lengkap.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa akuisisi *non-root* pada Redmi 10A Android 11 dapat memperoleh informasi dasar perangkat dan daftar aplikasi, sementara pengumpulan pendukung melalui Android Debug Bridge menghasilkan *netstats* dan *batterystats*. Dokumentasi Google Activity juga menampilkan entri kunjungan ke situs simulasi pada perangkat Redmi 10A. Temuan tersebut mendukung bahwa Google Chrome digunakan dan aktivitas kunjungan situs tercatat pada tingkat akun. Namun, Google Activity bukan artefak internal Chrome yang dipulihkan dari hasil akuisisi, dan tampilan waktunya bersifat relatif sehingga tidak digunakan sebagai satu-satunya dasar penentuan urutan kejadian. Riwayat penelusuran, *cookies*, *cache*, basis data *browser*, file unduhan, tangkapan layar, dan metadata terkait tidak berhasil ditemukan pada keluaran MOBILedit Forensic yang diperiksa menggunakan FTK Imager dan Autopsy. Oleh karena itu, rekonstruksi hanya dapat dilakukan secara parsial: kondisi perangkat, keberadaan aplikasi, penggunaan Chrome, dokumentasi kunjungan situs pada akun Google, serta pelaksanaan akuisisi dapat didukung, tetapi kronologi internal *browser*, proses pengunduhan gambar, pembukaan halaman permainan, dan artefak penghapusan tidak dapat dipulihkan secara lengkap. Ketiadaan artefak pada hasil akuisisi tidak membuktikan bahwa aktivitas tidak terjadi, melainkan menunjukkan keterbatasan akses terhadap direktori privat aplikasi pada metode *non-root*. Penelitian selanjutnya perlu membandingkan beberapa perangkat, versi Android, dan *browser* serta menguji *file system acquisition*, *physical acquisition*, atau sumber akun/*cloud* yang diperoleh secara legal dengan dokumentasi waktu dan nilai hash yang lebih lengkap.

REFERENCES

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

Ajuj, A., Bintang, R. M. G. S., & Bahytsani, D. A. (2024). Analisis bukti digital forensik pada aplikasi Threads menggunakan metode Digital Forensic Research Workshop. Jurnal Informatika Komputer, Bisnis dan Manajemen, 22(2), 1–10. https://doi.org/10.61805/fahma.v22i2.118

Ali, I., & Yustiana. (2025). Implementasi penggunaan forensik digital dalam penyelidikan dan penyidikan tindak pidana di Polres Wajo. LEGAL: Journal of Law, 4(2), 53–66.

Aprilia, R., & Kurniawan, Y. P. (2024). Peran forensik smartphone dalam mengungkap jejak digital transaksi pencucian uang elektronik. JISPENDIORA: Jurnal Ilmu Sosial, Pendidikan dan Humaniora, 3(3), 110–118. https://doi.org/10.56910/jispendiora.v3i3.2917

Fahrudin, A., & Muflih, G. Z. (2024). Analisis forensik digital pada pesan WhatsApp yang terenkripsi dengan Pretty Good Privacy menggunakan framework DFRWS. JATI (Jurnal Mahasiswa Teknik Informatika), 9(1), 780–787. https://doi.org/10.36040/jati.v9i1.12506

Fawzan, I., & Luthfi, A. (2025). Identifikasi jenis file pada artefak digital menggunakan algoritma K-Nearest Neighbor. JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), 10(2), 1474–1481. https://doi.org/10.29100/jipi.v10i2.6263

Firmansyah, R. A. (2024). Framework integrasi digital forensic readiness dan information security management system di lingkungan pemerintahan [Disertasi doktoral, Universitas Islam Indonesia].

Hidayah, A., & Fachri, F. (2024). Analisis bukti digital terhadap kasus prostitusi online pada aplikasi MiChat menggunakan metode ACPO. JATI (Jurnal Mahasiswa Teknik Informatika), 9(1), 906–912. https://doi.org/10.36040/jati.v9i1.12441

Isnaeni, F., & Fachri, F. (2025). Analisis forensik smartphone Android pada aplikasi TikTok menggunakan metode NIST. JATI (Jurnal Mahasiswa Teknik Informatika), 9(1), 1404–1410.

Juniansyah, N., Singasatia, D., & Muhyidin, Y. (2024). Analisis dan simulasi pengujian serangan keamanan smartphone Android menggunakan metode penetration testing dengan tools PhoneSploit. Jurnal Teknologika, 14(2), 584–596. https://doi.org/10.51132/teknologika.v14i2.418

Kanda, A. S., & Aziz, F. (2024). Analisis dampak kasus judi online terhadap masyarakat. Jurnal Ilmiah Research Student, 1(3), 829–836.

Mualfah, D., Israndi, F., & Ramadhan, R. A. (2025). Analisis perbandingan tools forensic pada aplikasi Facebook Messenger menggunakan metode National Institute of Standards Technology (NIST). Jurnal Fasilkom, 15(3), 533–541.

Nirmala, A., Giovani, M., & Sidabutar, J. (2024). Analisis forensik aplikasi Discord pada Android berdasarkan ACPO framework. Journal of Information Systems Management and Digital Business, 1(3), 307–313.

TIN: Terapan Informatika Nusantara
Vol 7, No 2, July 2026, page 1335-1344
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i2.10709

Prambudi, R. P., Riadi, I., & Murinto. (2025). Analisis forensik mobile pada aplikasi e-commerce menggunakan metode Association of Chief Police Officers. Cyber Security dan Forensik Digital, 8(1), 44–52. https://doi.org/10.14421/csecurity.2025.8.1.5234

Qonita, N. N., Salmalina, D. T., Sajmira, D. D., & Mustofa, H. (2025). Analisis forensik metadata lokasi Android dengan Autopsy dan evaluasi akurasi Haversine. Cyber Security dan Forensik Digital, 8(2), 89–96.

Qurrota, S., Rizqi, A., & Kurniawan, Y. P. (2025). Digital forensik sebagai penegakan hukum pada kasus fraud COD dalam industri logistik. Jurnal Hukum Lex Generalis, 6(7), 1–15.

Ramdani, M. A. R. F., Hadiana, A. I., & Ilyas, R. (2025). Pemanfaatan open-source intelligence untuk deteksi dan penanganan cybercrime judi online berbasis forensik digital. Jurnal Algoritma, 22(2), 22–34. https://doi.org/10.33364/algoritma/v.22-2.2314

Riffai Achmad, M., & Muntasiroh, L. (2024). Digital forensik untuk investigasi pasca kejadian platform dan web security. Prosiding Seminar Nasional UNIMUS, 7, 812–819.

Rifkiansyah, M. K., Azinar, A. W., Fitrani, A. S., & Aji, S. (2026). Analisis artefak forensik pada smartwatch generasi terbaru menggunakan metode NIST untuk pembuktian alibi dan rekonstruksi aktivitas pengguna. JATI (Jurnal Mahasiswa Teknik Informatika), 10(1), 699–705.

Syahputra, F., Sabrina, E., Sembiring, D. A. P., Siahaan, E. T., Lubis, M. F., & Ulwi, M. Z. (2024). Rancang bangun media pembelajaran pengenalan hardware komputer berbasis Android. JATI (Jurnal Mahasiswa Teknik Informatika), 8(5), 11024–11029. https://doi.org/10.36040/jati.v8i5.11767