

ANALISIS FORENSIK DIGITAL KASUS PENYEBARAN PORNOGRAFI PADA APLIKASI TELEGRAM MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Fadhil Al Fikri ¹, Novi Safriadi ², Haried Novriando ³

Informatika, Teknik, Universitas Tanjungpura, Pontianak, Indonesia

Email: fadhilvlcm01@gmail.com

Abstract (English)

The dissemination of pornographic content through Telegram requires a systematic digital forensic process to acquire and preserve relevant evidence. This study applies the National Institute of Standards and Technology (NIST) framework to a simulated communication case on a rooted Samsung J3-G20G Android device and compares the artifacts obtained with MOBILedit Forensic and Oxygen Forensic. The procedure comprises collection, examination, analysis, and reporting. Two extraction outputs were examined against ten general artifact categories and seven categories relevant to the simulated case. In the case-specific comparison, each tool recovered four of seven categories (57.1%): contacts, video, pictures, and deleted messages. Neither tool recovered message content, audio, or documents in this subset. In the broader device-level comparison, Oxygen Forensic obtained artifacts in nine of ten categories, whereas MOBILedit Forensic obtained seven; their counts and coverage therefore should not be conflated with the case-specific score. The thesis reports matching MD5 and SHA-1 hashes before and after analysis for each acquired image. These results show the value of a structured workflow and complementary tools, while limiting the conclusion to one device and one simulated scenario.

Article History

Submitted: 2 Oktober 2026

Accepted: 5 Oktober 2026

Published: 6 Oktober 2026

Key Words

Digital forensics

Telegram

NIST

MOBILedit Forensic

Oxygen Forensic

Abstrak (Indonesia)

Penyebaran konten pornografi melalui Telegram memerlukan pemeriksaan forensik digital yang sistematis agar artefak yang relevan dapat diperoleh dan dijaga integritasnya. Penelitian ini menerapkan tahapan National Institute of Standards and Technology (NIST) pada skenario komunikasi simulatif menggunakan perangkat Android Samsung J3-G20G yang telah melalui proses root, serta membandingkan hasil MOBILedit Forensic dan Oxygen Forensic. Tahap penelitian mencakup collection, examination, analysis, dan reporting. Keluaran kedua alat diperiksa menurut sepuluh kategori artefak umum dan tujuh kategori yang relevan dengan skenario kasus. Pada tujuh kategori kasus, masing-masing alat menemukan empat kategori (57,1%), yaitu kontak, video, gambar, dan pesan terhapus; konten pesan, audio, dan dokumen tidak ditemukan. Pada cakupan seluruh perangkat, Oxygen Forensic mendeteksi sembilan dari sepuluh kategori dan MOBILedit Forensic tujuh kategori, sehingga hasil ini tidak boleh disamakan dengan tingkat temuan kasus. Skripsi sumber melaporkan nilai hash MD5 dan SHA-1 yang sama sebelum dan sesudah analisis untuk tiap citra akuisisi. Temuan memperlihatkan manfaat alur kerja terstruktur dan penggunaan dua alat yang saling melengkapi, dengan batasan satu perangkat dan satu skenario simulasi.

Sejarah Artikel

Submitted: 2 Oktober 2026

Accepted: 5 Oktober 2026

Published: 6 Oktober 2026

Kata Kunci

Forensik digital

Telegram

NIST

Bukti digital

Ekstraksi data

PENDAHULUAN

Aplikasi pesan instan menyimpan komunikasi dan berkas media yang dapat menjadi artefak penting dalam penyelidikan. Pada Telegram, pemeriksaan perangkat seluler menghadapi kendala akses ke berkas aplikasi, kemungkinan penghapusan percakapan, serta kebutuhan untuk mempertahankan integritas hasil akuisisi. Pedoman forensik perangkat seluler NIST menekankan penanganan, perolehan, pemeriksaan, analisis, dan pelaporan data secara terdokumentasi [1].

Penelitian terdahulu telah menerapkan kerangka NIST 800-101 untuk pemeriksaan MiChat dan Telegram [2]. Studi lain membandingkan metode NIJ dan NIST pada media MicroSD [3],

sedangkan penelitian Telegram Web dengan DFRWS menelusuri artefak peramban dalam kasus penipuan [4]. Penelitian ini berfokus pada artefak aplikasi Telegram Android dalam skenario penyebaran konten pornografi yang disimulasikan, dengan perbandingan dua alat forensik pada perangkat yang sama. Karena objek dan jalur akuisisinya berbeda, angka hasil dari studi terdahulu tidak dijadikan pembandingan langsung.

Tujuan penelitian adalah mengidentifikasi kategori bukti digital yang dapat diperoleh, membandingkan cakupan MOBILedit Forensic dan Oxygen Forensic, serta memeriksa apakah nilai hash citra akuisisi tetap sama setelah analisis. Penilaian dibedakan antara artefak seluruh perangkat dan kategori yang terkait langsung dengan skenario. Perbedaan ini diperlukan karena jumlah berkas yang ditemukan secara umum tidak identik dengan bukti kejadian yang diteliti.

METODE PENELITIAN

Objek dan skenario simulasi

Penelitian menggunakan Samsung J3-G20G dengan Android 5.1.1, RAM 1,5 GB, dan penyimpanan 8 GB. Perangkat pemeriksaan terdiri atas dua laptop, yaitu Asus TUF FX516PC untuk MOBILedit Forensic dan Asus TUF FX505GM untuk Oxygen Forensic, sebagaimana dirinci dalam skripsi sumber. Perangkat Android di-root menggunakan alur pengaktifan opsi pengembang dan USB debugging, pemasangan TWRP melalui Odin, pemasangan SuperSU, serta pemeriksaan status root. Operasi root berlangsung dalam persiapan simulasi; karena dapat mengubah keadaan perangkat, status dan waktu tindakan ini perlu dicatat dalam penerapan pada perkara nyata.

Skenario melibatkan pengguna A pada Samsung dan pengguna B pada iPhone. Keduanya berkomunikasi lewat Telegram; pengguna A mengirim pesan dan media bermuatan pornografi kepada pengguna B, lalu menghapus riwayat komunikasi pada perangkatnya. Pemeriksaan pada penelitian ini diarahkan kepada perangkat Samsung. Skenario tersebut dibuat untuk penelitian, sehingga temuan merupakan hasil simulasi, bukan pengungkapan perkara pidana yang diverifikasi secara independen.

Tahapan dan ukuran hasil

Empat tahap operasional yang dipakai adalah collection, examination, analysis, dan reporting. Pada collection, perangkat diamankan dan mode pesawat diaktifkan. Examination mencakup akuisisi dengan Oxygen Forensic menggunakan pilihan full file system dan dengan MOBILedit Forensic melalui pembuatan physical image lalu ekspor full content. Analysis mengelompokkan artefak yang dilaporkan kedua alat; reporting menyajikan tabel perbandingan dan pemeriksaan hash. Penamaan metode akuisisi mengikuti catatan skripsi; penelitian sumber belum menyediakan log rinci yang memungkinkan verifikasi tingkat akses fisik di setiap tahap.

Pada Oxygen Forensic, proses yang didokumentasikan dimulai dengan pendeteksian Samsung J3-G20G, pemeriksaan koneksi, permintaan akses root dan izin USB debugging. Perangkat lunak kemudian menghitung ukuran data, mengekstraksi logical file system, memproses data Android keystore, dan menghitung hash. Hasil ekstraksi dibuka melalui menu data yang telah diperoleh. Istilah full file system dan logical file system sama-sama muncul pada dokumentasi langkah ini; artikel mempertahankan istilah tersebut sebagaimana dicatat peneliti tanpa menyimpulkan bahwa semua sektor media telah diakuisisi.

Pada MOBILedit Forensic, peneliti terlebih dahulu membuat physical image perangkat. Skripsi memperkirakan proses ini memerlukan sekitar 45 sampai 60 menit pada perangkat uji. Setelah citra selesai, peneliti memilih full content, mengisi detail laporan, menentukan format keluaran serta lokasi ekspor, lalu menjalankan akuisisi dan membaca laporan hasilnya. Waktu tersebut merupakan catatan pengamatan pada satu pengujian dan tidak dipakai sebagai

perbandingan kinerja kedua alat karena durasi Oxygen Forensic tidak diukur dengan dasar yang sama.

Sepuluh kategori untuk cakupan umum ialah informasi aplikasi, informasi akun, pesan, kontak, audio, video, informasi perangkat, gambar, dokumen, dan pesan terhapus. Tujuh kategori untuk kasus simulasi ialah pesan, kontak, audio, video, gambar, dokumen, dan pesan terhapus. Keberhasilan tingkat kategori dihitung dengan persamaan $P = (\text{jumlah kategori terdeteksi} / \text{jumlah kategori yang diuji}) \times 100\%$. Perhitungan tidak mengukur recall item, ketepatan identifikasi konten, atau ketuntasan semua artefak pada perangkat.

HASIL DAN PEMBAHASAN

Akuisisi dan pemeriksaan integritas

Proses examination menghasilkan citra dan laporan ekstraksi dari kedua alat. Skripsi mencatat nilai MD5 dan SHA-1 sebelum analisis, kemudian menyatakan bahwa nilainya tetap sama setelah analisis. Tabel 1 menyalin nilai sebelum analisis; kesamaan sesudah analisis didasarkan pada dokumentasi visual skripsi dan tidak dihitung ulang dari berkas citra mentah yang tidak disertakan.

Tabel 1. Nilai hash citra akuisisi yang dilaporkan dalam skripsi

Alat	MD5 sebelum analisis	SHA-1 sebelum analisis
Oxygen Forensic	2373c50a153747dfedf61923e67cc2e5	37fc848929c5f875f08a246d32e108fc25ea3dc1
MOBILedit Forensic	4bcf0dfb44e184cbe82a3536ee6fc9bb	0469231d1dbf5ff8dce0e43681937859a46ff

Kecocokan hash pada citra yang sama mendukung kesimpulan bahwa citra tersebut tidak berubah selama tahap analisis yang didokumentasikan. Hasil itu tidak dengan sendirinya membuktikan bahwa proses rooting sebelum akuisisi tidak mengubah data asli, atau bahwa seluruh rantai penguasaan barang bukti sudah terverifikasi.

Cakupan artefak pada seluruh perangkat

Tabel 2 menyajikan hasil tabel utama skripsi berdasarkan kategori artefak pada keseluruhan perangkat. Angka dalam tanda kurung adalah jumlah artefak yang dilaporkan per kategori, bukan jumlah item relevan dengan skenario pornografi. Kedua alat tidak menemukan konten pesan pada kategori messages, sementara Oxygen Forensic menemukan audio dan dokumen yang tidak tercatat pada hasil MOBILedit Forensic.

Tabel 2. Perbandingan artefak umum pada perangkat

Kategori	MOBILedit Forensic	Oxygen Forensic
Informasi aplikasi	Ada (15)	Ada (1.167)
Informasi akun	Ada (1)	Ada (9)
Pesan	Tidak ada (0)	Tidak ada (0)
Kontak	Ada (67)	Ada (489)
Audio	Tidak ada (0)	Ada (1)
Video	Ada (7)	Ada (3)
Informasi perangkat	Ada (10)	Ada (25)
Gambar	Ada (102)	Ada (88)

Dokumen	Tidak ada (0)	Ada (2)
Pesan terhapus	Ada (1)	Ada (1)

Berdasarkan keberadaan kategori, Oxygen Forensic mencakup sembilan dari sepuluh kategori, sedangkan MOBILedit Forensic mencakup tujuh. Nilai 1.167 pada informasi aplikasi Oxygen dan angka 489 kontak mengacu pada Tabel 4.1 skripsi. Narasi hasil ekstraksi di bagian lain skripsi menyebut 1.161 artefak Oxygen, termasuk 1.009 contacts; perbedaan definisi atau cakupan hitungan tersebut tidak dijelaskan. Karena itu jumlah antarkategori pada Tabel 2 tidak dijumlahkan sebagai satu total unik.

Laporan hasil ekstraksi naratif juga menyebut 278 keluaran MOBILedit Forensic yang dikelompokkan sebagai 10 photos, 206 images, 5 audio, 10 video, dan 47 documents. Kelompok ini tidak identik dengan matriks Telegram pada Tabel 2: misalnya, matriks Telegram mencatat nol audio dan nol dokumen untuk MOBILedit. Perbedaan tersebut masuk akal jika keluaran umum perangkat mencakup data di luar aplikasi dan kasus, tetapi skripsi tidak menyediakan pemetaan per item yang cukup untuk membuktikannya. Artikel ini karena itu memakai matriks kategori skripsi untuk perbandingan Telegram, bukan menggabungkan semua jumlah keluaran.

Bukti pada skenario kasus

Untuk menilai kasus simulasi, Tabel 3 menggunakan tujuh kategori pada Tabel 4.2 skripsi. Kedua alat menunjukkan hasil identik menurut ada atau tidaknya kategori, meskipun jumlah temuan kategori tertentu tidak menggambarkan seluruh isi atau konteks komunikasi. Kontak satu artefak, video satu artefak, gambar tiga artefak, dan pesan terhapus satu artefak ditemukan oleh masing-masing alat. Konten pesan tidak ditemukan oleh keduanya.

Tabel 3. Kategori bukti yang terkait skenario simulasi

Kategori	MOBILedit Forensic	Oxygen Forensic
Pesan	0	0
Kontak	1	1
Audio	0	0
Video	1	1
Gambar	3	3
Dokumen	0	0
Pesan terhapus	1	1

Setiap alat mendeteksi empat dari tujuh kategori, sehingga $P = 4/7 \times 100\% = 57,1\%$ setelah pembulatan satu desimal. Nilai ini adalah persentase kategori yang hadir dalam hasil ekstraksi kasus, bukan probabilitas keberhasilan pemeriksaan atau proporsi keseluruhan data yang dipulihkan. Artefak “pesan terhapus” yang dicatat sebanyak satu tidak dapat disamakan dengan pemulihan isi percakapan: kategori messages tetap bernilai nol pada tabel sumber.

Empat kategori yang ditemukan dapat memberi petunjuk awal adanya komunikasi dan media pada perangkat, tetapi pembuktian rangkaian peristiwa memerlukan hubungan yang lebih kuat antara artefak. Misalnya, berkas gambar perlu dihubungkan dengan akun Telegram, waktu pengiriman, penerima, dan konteks percakapan. Tanpa konten pesan yang terpulihkan, klaim mengenai isi obrolan harus bertumpu pada bukti lain dalam simulasi, bukan pada hasil ekstraksi kategori messages. Temuan satu pesan terhapus juga memerlukan identifikasi apakah yang diperoleh berupa isi, metadata, penanda penghapusan, atau entri aplikasi.

Implikasi dan keterbatasan

Oxygen Forensic memberi cakupan kategori umum lebih luas, sementara hasil kasus khusus dari kedua alat setara. Perbedaan ini menunjukkan bahwa pemilihan ukuran hasil memengaruhi interpretasi keunggulan alat. Jumlah gambar atau video dari keseluruhan perangkat juga tidak membuktikan semua item berkaitan dengan peristiwa simulasi; hubungan item dengan akun, waktu, pengirim, dan penerima memerlukan pemeriksaan metadata yang lebih rinci.

Penelitian hanya menggunakan satu model Android yang telah di-root, satu skenario simulasi, serta dua alat forensik. Berkas citra dan log akuisisi mentah tidak tercakup dalam dokumen skripsi yang digunakan untuk penulisan artikel ini, sehingga angka dan hash disajikan sebagai hasil yang dilaporkan oleh peneliti. Pengujian ulang pada versi Telegram dan sistem operasi yang lebih baru, beserta pencatatan versi alat, kontrol sebelum rooting, dan validasi silang isi artefak, diperlukan untuk menilai keterulangan hasil.

KESIMPULAN

Alur collection, examination, analysis, dan reporting membantu menyusun pemeriksaan Telegram Android pada skenario simulasi secara runtut. Pada tujuh kategori bukti kasus, MOBILedit Forensic dan Oxygen Forensic masing-masing mendeteksi empat kategori atau 57,1%. Oxygen Forensic menunjukkan cakupan kategori umum lebih luas, yaitu sembilan dari sepuluh dibanding tujuh dari sepuluh pada MOBILedit Forensic. Skripsi melaporkan nilai hash citra akuisisi yang tetap sama sebelum dan sesudah analisis. Kesimpulan ini berlaku untuk perangkat dan skenario yang diuji; pemeriksaan pada perangkat lain perlu mengulang akuisisi, validasi hash, dan penilaian relevansi tiap artefak.

REFERENCES

- [1] R. Ayers, S. Brothers, dan W. Jansen, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1. National Institute of Standards and Technology, 2014. doi: 10.6028/NIST.SP.800-101r1.
- [2] N. A. I. Maniar dan T. Yuniati, "Implementasi Mobile Forensic pada Aplikasi MiChat dan Telegram dengan Framework NIST 800-101," Cyber Security dan Forensik Digital, vol. 5, no. 2, hlm. 60–65, 2022. doi: 10.14421/csecurity.2022.5.2.3764.
- [3] N. Anwar, A. M. Widodo, B. A. Sekti, M. B. Ulum, M. Rahaman, dan H. D. Ariessanti, "Comparative Analysis of NIJ and NIST Methods for MicroSD Investigations: A Technopreneur Approach," Aptisi Transactions on Technopreneurship, vol. 6, no. 2, 2024. doi: 10.34306/att.v6i2.407.
- [4] K. A. Arifin dan I. Riadi, "Forensic Analysis of Online Fraud on Telegram Web using Digital Forensics Workshop Method," International Journal of Computer Applications, vol. 187, no. 30, hlm. 4–11, 2025. doi: 10.5120/ijca2025925515.