OPEN ACCESS

Volume 9 (4), October-December 2025, 1489-1502

E-ISSN:2580-1643

Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

DOI: https://doi.org/10.35870/jtik.v9i4.4223

Teknik Forensika Digital untuk Investigasi Pesan Sekali Lihat (*View Once*) pada Aplikasi *Instant Messenger*

Gilang Ramadhan [1*], Yudi Prayudi [2]

[1,2] Program Studi Informatika, Program Magister, Fakultas Teknik Industri, Universitas Islam Indonesia, Kabupaten Sleman, Daerah Istimewa Yogyakarta, Indonesia.*

a r t i c l e i n f o

Article history:
Received 8 May 2025
Received in revised form 20 May 2025
Accepted 1 June 2025
Available online October 2025.

Keywords:
Instant Messenger; View Once; Anti Forensic; Digital Forensik; Mobile Forensik; NIST.

a b s t r a c t

The popularity of Instant Messaging apps encourages developers to improve features and security, especially data privacy. However, these improvements also potentially bring risks to users. One of the most popular new features is 'one-look messages' to maintain sender privacy. This feature allows messages to disappear once viewed, irrevocably and has been implemented on apps such as Snapchat, Instagram, and WhatsApp. The purpose of this research is to provide a reference on the reliability of digital forensic Tools in uncovering cybercrime. Thus, it is expected that the digital evidence obtained has strong integrity, reliability and legality to be used in the legal process. This research adopts the framework of the National Institute of Standards and Technology (NIST) and analyzes a cybercrime scenario in the form of sending files using the one-look message feature, utilizing the Magnet Axiom digital forensics tool. This research also uses a smartphone with root conditions that have Snapchat, Instagram and WhatsApp applications installed. The results of this study show that with a root smartphone, the use of Axiom magnet forensic Tools is able to acquire and analyze files sent using the one-look feature and obtain 13 digital evidence from 18 scenarios created. There is not much research that discusses the latest features of Instant Messaging applications, with this paper it can provide a little description of the Sekalin see feature and can be developed in the next paper.

Kata Kunci:
Pesan Instan; Lihat Sekali; Anti Forensik; Forensik Digital; Forensik Seluler; NIST.

a b s t r a k

Popularitas aplikasi pesan instan mendorong pengembang untuk meningkatkan fitur dan keamanan, terutama privasi data. Namun, peningkatan ini juga berpotensi membawa risiko bagi pengguna. Salah satunya pada fitur baru yang populer saat ini adalah 'pesan sekali lihat' untuk menjaga privasi pengirim. Fitur ini memungkinkan pesan hilang setelah dilihat, tidak bisa di tarik kembali dan telah diterapkan pada aplikasi seperti Snapchat, Instagram, dan WhatsApp. Tujuan penelitian ini adalah untuk memberikan referensi mengenai keandalan alat-alat forensik digital dalam mengungkap kejahatan siber. Dengan demikian, diharapkan bukti digital yang diperoleh memiliki integritas, keandalan, dan legalitas yang kuat untuk digunakan dalam proses hukum. Penelitian ini mengadopsi kerangka kerja dari National Institute of Standards and Technology (NIST) dan menganalisis skenario kejahatan siber berupa pengiriman file menggunakan fitur pesan sekali lihat, dengan memanfaatkan alat forensik digital Magnet Axiom. Penelitian ini juga menggunakan smartphone dengan kondisi root yang sudah ter-install aplikasi Snapchat, Instagram dan whatsapp .Hasil penelitian ini menunjukkan dengan smartphone keadaan root penggunaan Tools forensik magnet axiom mampu mengakuisisi dan menganalisis file yang dikirim menggunakan fitur sekali lihat dan mendapatkan 13 bukti digital dari 18 skenario yang dibuat. Belum banyaknya penelitian yang membahas tentang fitur terbaru dari aplikasi pesan instan, dengan tulisan ini bisa memberikan sedikit gambaran mengenai fitur Sekali lihat dan bisa di kembangakan dalam tulisan berikutnya.

Corresponding Author. Email: gr91089@gmail.com [1].

ACM Computing Classification System (CCS)
EBSCOhost
Communication and Mass Media Complete (CMMC)

1. Pendahuluan

Lebih dari 190 juta pengguna ponsel pintar di Indonesia menunjukkan pesatnya pertumbuhan penggunaan aplikasi pesan instan (*instant messaging*/IM), yang secara signifikan menggantikan peran SMS konvensional. Aplikasi IM memungkinkan komunikasi lintas platform dalam bentuk teks, suara, video, maupun media lainnya. Kemudahan ini menjadikan IM sangat diminati untuk berbagai kebutuhan, mulai dari percakapan harian hingga pertemuan daring (Nafila & Prayudi, 2022; Plianda & Indrayani, 2022). Tren penggunaan aplikasi pesan instan turut mendorong pengembang untuk memperbarui fitur dan sistem keamanan, terutama dalam hal perlindungan data pribadi (Yel & Nasution, 2022). Di balik manfaatnya, pengembangan tersebut juga menimbulkan potensi risiko bagi pengguna. Salah satu fitur yang kini cukup populer adalah "pesan sekali lihat", yang memungkinkan pesan secara otomatis terhapus setelah dibuka. Fitur ini telah diterapkan pada aplikasi seperti Snapchat, Instagram, dan WhatsApp. Meskipun fitur pesan sekali lihat bertujuan melindungi privasi pengirim, fitur ini juga rawan disalahgunakan untuk keperluan ilegal, seperti penipuan, intimidasi daring, distribusi konten pornografi, hingga komunikasi kelompok terlarang (Harahap, 2023).

Oleh sebab itu, diperlukan pendekatan forensik digital untuk menangani berbagai pelanggaran hukum yang melibatkan fitur ini. Peningkatan jumlah kasus kejahatan siber di Indonesia menunjukkan urgensi penanganan yang serius. Misalnya, pada akhir Desember 2023, sebanyak 11 anak di bawah umur dilaporkan menjadi korban kekerasan berbasis gender online (KBGO) oleh seorang pria berusia 21 tahun. Berdasarkan laporan Dewan Perlindungan Anak, pelaku menjanjikan "diamond" dalam permainan daring untuk memikat korban. Setelah menjalin komunikasi melalui WhatsApp, pelaku memaksa korban mengirim foto dan video pribadi dengan ancaman penghapusan akun permainan mereka (Arsyad, 2022). Salah satu taktik yang digunakan pelaku adalah anti-forensik, yakni teknik menyembunyikan atau menghapus jejak digital agar menyulitkan proses investigasi (Aziz *et al.*, 2021). Dalam konteks ini, upaya memperoleh dan mempertahankan bukti digital menjadi sangat krusial. Ketika artefak digital hilang atau rusak, proses investigasi dapat terhambat (Wirara *et al.*, 2020). Oleh karena itu, diperlukan metode dan perangkat yang tepat untuk mengekstrak serta menganalisis data digital dari fitur pesan sekali lihat pada berbagai aplikasi pesan instan. Ketepatan metode sangat menentukan keberhasilan dalam mengungkap kejahatan siber yang menggunakan fitur pesan sementara. Forensik digital sendiri merupakan disiplin yang memanfaatkan teknologi informasi untuk mengumpulkan dan menganalisis bukti elektronik dalam kasus hukum. Salah satu cabangnya, forensik seluler, berfokus pada akuisisi bukti dari perangkat mobile yang lazim digunakan sebagai media komunikasi. Kemajuan teknologi seperti Internet of Things (IoT) juga turut memperbesar peluang terjadinya kejahatan siber. Fitur seperti pesan sekali lihat yang bersifat volatil menjadi tantangan tersendiri karena bukti digitalnya mudah hilang. Oleh karena itu, teknik forensik khusus dibutuhkan agar pesan-pesan yang dihapus tersebut tetap dapat dipulihkan. Setiap kejahatan, termasuk dalam ranah digital, akan meninggalkan jejak yang dapat dianalisis sebagai barang bukti yang sah secara hukum. Penggunaan metode dan alat forensik yang tepat akan sangat membantu dalam mengidentifikasi dan memperoleh bukti digital secara valid. Teknik akuisisi yang sistematis memungkinkan proses pembuktian lebih kuat di pengadilan.

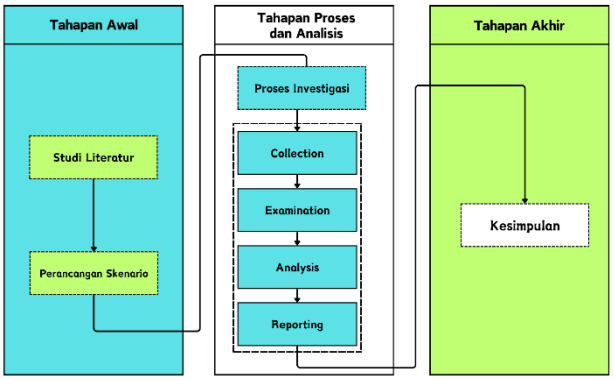
Penelitian terdahulu oleh Rofiq *et al.* (2022) telah melakukan analisis terhadap fitur pesan sekali lihat pada WhatsApp dan Telegram menggunakan perangkat Android yang telah di-root. Dengan mengacu pada kerangka kerja NIST SP 800-101 Rev-1, penelitian tersebut berhasil mengidentifikasi artefak media dari WhatsApp, namun tidak berhasil pada Telegram, kecuali dalam bentuk riwayat percakapan. Berdasarkan temuan tersebut, studi ini dirancang untuk menganalisis bukti digital dari fitur pesan sekali lihat pada aplikasi Snapchat, WhatsApp, dan Instagram menggunakan perangkat Android yang telah di-root. Penelitian ini juga menerapkan kerangka kerja NIST sebagai standar investigasi forensik digital, serta menggunakan alat Magnet Axiom untuk proses akuisisi data.

2. Metodologi Penelitian

Metodologi penelitian merupakan fondasi utama dalam pelaksanaan studi ilmiah. Komponen ini memberikan panduan sistematis bagi peneliti dalam merancang, melaksanakan, dan menganalisis rangkaian kegiatan penelitian. Setiap tahapan dirancang untuk menjawab rumusan masalah secara terstruktur dan logis melalui pendekatan ilmiah, sehingga tujuan penelitian dapat tercapai secara optimal. Penelitian ini menerapkan metode deskriptif dengan pendekatan eksperimental, yang difokuskan pada investigasi fitur "pesan sekali lihat" dalam aplikasi pesan instan. Secara garis besar, tahapan penelitian dibagi menjadi tiga bagian utama:

1) Tahap Persiapan
   Tahapan awal mencakup studi literatur untuk memperoleh pemahaman teoretis serta perencanaan teknis, termasuk pemilihan perangkat lunak dan perangkat keras yang diperlukan. Pada tahap ini pula dilakukan konfigurasi sistem, pengujian rooting perangkat, serta instalasi aplikasi yang menjadi objek pengujian.
2) Tahap Pelaksanaan dan Analisis
   Merupakan inti dari proses penelitian yang terdiri atas perancangan skenario pengiriman pesan menggunakan fitur sekali lihat, pelaksanaan pengujian, serta akuisisi dan analisis bukti digital. Kerangka kerja yang digunakan mengacu pada pedoman National Institute of Standards and Technology (NIST), yang terdiri dari empat fase utama: pengamanan (preservation), akuisisi (acquisition), pemeriksaan dan analisis (examination and analysis), serta pelaporan (reporting).
3) Tahap Penyimpulan
   Tahap akhir berisi perumusan kesimpulan dari hasil analisis, sekaligus memberikan rekomendasi teknis untuk penelitian sejenis di masa mendatang, khususnya terkait efektivitas alat forensik digital dalam mengungkap bukti dari fitur pesan sementara pada aplikasi pesan instan.

Setiap tahap dilaksanakan secara sistematis guna menjamin validitas hasil dan meningkatkan akurasi temuan dalam proses investigasi digital forensik.



Gambar 1. Metodologi penelitian

Studi Literatur

Tahapan studi literatur merupakan bagian awal yang penting dalam proses penelitian, karena berfungsi sebagai landasan teoritis yang mendasari seluruh rangkaian kegiatan analisis. Kegiatan ini dilakukan melalui pengumpulan dan penelaahan berbagai sumber referensi ilmiah, seperti jurnal terakreditasi, artikel ilmiah, dan dokumen teknis yang berkaitan dengan topik penelitian. Dalam studi ini, penelusuran literatur diarahkan pada referensi yang membahas metode pencarian data digital pada perangkat seluler, karakteristik artefak dari fitur pesan sementara, serta perangkat lunak forensik yang umum digunakan, seperti Magnet Axiom. Penelaahan juga dilakukan terhadap literatur yang menjelaskan standar operasional dalam investigasi forensik digital, khususnya kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST). Pemahaman yang diperoleh dari tahapan ini digunakan sebagai dasar dalam menyusun desain pengujian dan metode analisis yang diterapkan pada tahap selanjutnya. Dengan pendekatan ini, penelitian dapat dijalankan secara terstruktur dan berbasis teori yang dapat dipertanggungjawabkan secara ilmiah.

Perancangan Skenario

Perancangan skenario dilakukan sebagai bagian dari simulasi investigasi kejahatan siber. Tujuan dari tahapan ini adalah menciptakan kondisi terkontrol yang memungkinkan peneliti mengamati perilaku sistem dan mengidentifikasi artefak digital yang dihasilkan selama penggunaan fitur "pesan sekali lihat" pada aplikasi pesan instan. Skenario yang dikembangkan dalam penelitian ini difokuskan pada proses pengiriman file (gambar dan video) melalui fitur pesan sekali lihat pada tiga aplikasi yang menjadi

objek pengujian, yaitu Snapchat, WhatsApp, dan Instagram. Pengiriman pesan dilakukan selama tiga hari berturut-turut, untuk mengevaluasi daya tahan dan jejak digital yang ditinggalkan oleh masing-masing aplikasi setelah fitur tersebut digunakan. Skenario ini menjadi pedoman utama dalam pelaksanaan eksperimen, serta berperan penting dalam proses identifikasi dan validasi bukti digital yang diperoleh pada tahap analisis forensik.

Kerangka NIST

Penelitian ini mengadopsi model investigasi digital yang dirancang oleh National Institute of Standards and Technology (NIST), sebagai kerangka acuan dalam pelaksanaan proses forensik digital. Model tersebut memberikan pedoman sistematis yang terbagi dalam empat tahapan utama:

1) *Preservation* (Pengamanan)
   Pada tahap ini, perangkat seluler yang diduga mengandung bukti digital diamankan untuk menjaga integritas data. Semua koneksi nirkabel dimatikan dan perangkat diisolasi dari jaringan untuk mencegah perubahan data.
2) *Acquisition* (Akuisisi)
   Proses akuisisi dilakukan dengan menyalin seluruh isi perangkat menggunakan perangkat lunak forensik seperti Magnet Axiom. Langkah ini bertujuan memperoleh salinan data yang utuh, termasuk data tersembunyi atau yang telah dihapus.
3) *Examination & Analysis* (Pemeriksaan dan Analisis)
   Tahap ini mencakup proses identifikasi dan interpretasi artefak digital dari hasil akuisisi. Pemeriksaan dilakukan untuk menemukan file, metadata, atau informasi lain yang relevan dengan skenario pengujian. Magnet Axiom digunakan untuk mengekstraksi dan menampilkan data yang diperoleh dari perangkat.
4) *Reporting* (Pelaporan)
   Seluruh hasil analisis dirangkum dalam bentuk laporan akhir yang memuat temuan utama, jejak digital yang berhasil diidentifikasi, serta verifikasi integritas bukti menggunakan nilai hash. Laporan ini dapat digunakan sebagai dokumen pendukung dalam proses pembuktian secara hukum.

Gambar 2. Alur Kerja NIST

Tahapan Kerja Berdasarkan NIST

Proses investigasi forensik digital dalam penelitian ini mengacu pada kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST), yang terdiri dari empat tahapan utama: pengamanan, pemeriksaan, analisis, dan pelaporan.

Tahap Pengamanan (*Preservation*)

Pada tahap awal ini, peneliti melakukan proses pengumpulan dan pengamanan perangkat seluler yang digunakan sebagai objek investigasi. Tujuan dari tahapan ini adalah menjaga keutuhan dan keaslian barang bukti agar tidak mengalami perubahan data selama proses investigasi berlangsung. Seluruh konektivitas nirkabel, seperti Wi-Fi dan Bluetooth, dinonaktifkan, dan perangkat dialihkan ke mode pesawat guna mencegah komunikasi data yang tidak diinginkan. Langkah ini penting untuk memastikan bahwa bukti digital tetap dalam kondisi asli dan dapat dipertanggungjawabkan secara hukum.

Tahap Pemeriksaan (*Examination*)

Pada tahap ini, dilakukan proses akuisisi data digital menggunakan perangkat lunak forensik Magnet Axiom. Alat tersebut digunakan untuk menyalin seluruh isi perangkat secara utuh, termasuk data yang disembunyikan atau telah dihapus. Proses akuisisi dilaksanakan dengan metode imaging guna memperoleh representasi digital dari perangkat yang diamankan. Tahapan ini bertujuan untuk memastikan bahwa seluruh data yang relevan dapat diakses dan dianalisis tanpa memodifikasi bukti asli.

Tahap Analisis (*Analysis*)

Data hasil akuisisi kemudian dianalisis guna mengidentifikasi artefak digital yang relevan dengan skenario pengujian. Fokus analisis diarahkan pada file media (gambar dan video) yang dikirim menggunakan fitur pesan sekali lihat, serta metadata terkait seperti waktu pengiriman, hash file, dan direktori penyimpanan. Tahapan ini dilakukan dengan tetap menjaga integritas data, sesuai pedoman standar yang ditetapkan oleh NIST. Setiap temuan dianalisis secara seksama untuk mendukung proses interpretasi hasil dan pengambilan kesimpulan.

Tahap Pelaporan (*Reporting*)

Tahap akhir berupa penyusunan laporan forensik digital yang mendokumentasikan seluruh rangkaian proses, hasil analisis, serta temuan artefak digital. Laporan ini memuat deskripsi metode akuisisi, identifikasi artefak penting, validasi melalui nilai hash, dan interpretasi data yang diperoleh dari masing-masing aplikasi yang diuji. Laporan tersebut disusun secara sistematis untuk mendukung transparansi, objektivitas, dan dapat dijadikan sebagai dokumen pendukung dalam proses hukum maupun penelitian lanjutan.

3. Hasil dan Pembahasan

Hasil

Untuk mendukung proses pengujian, implementasi, dan analisis dalam penelitian ini, digunakan berbagai perangkat keras dan perangkat lunak yang berfungsi sebagai sarana akuisisi dan analisis data digital. Seluruh alat dan bahan dipilih berdasarkan kebutuhan teknis serta kompatibilitasnya dengan proses forensik digital yang mengacu pada standar NIST. Rincian perangkat yang digunakan dalam penelitian ini disajikan pada Tabel 1.

Tabel 1. Alat dan kebutuhan Penelitian

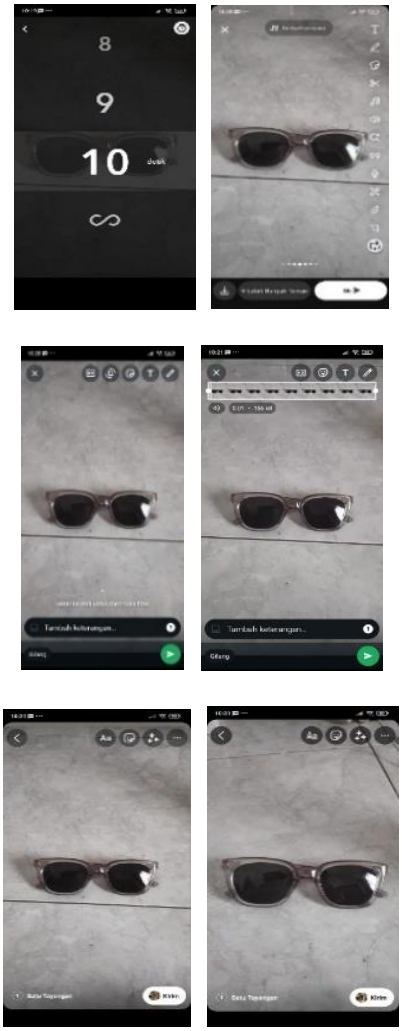
NO	Perangkat	Spesifikasi
1	Laptop Rog Strix G512LI	Processor : Intel Core i5 Ram : 8GB Storage : 512GB SSD Operating System : Windows 10 HOME
2	Smarphone Xiomi Pocophone F1	Prosessor Chipset Qualcomm SDM845 Snapdragon 845 with CPU Octa-core (4x2.8 GHz Kryo 385 Gold & 4x1.8 GHz Kryo 385 Silver) dan GPU Adreno 630 RAM 6 GB OSAndroid 10. Memori Internal 128 GB
3	Magnet Axiom Process	v5.4.0
4	Magnet Axiom Examine	v5.4.0
5	Magisk	v26.1
6	Snapchat	11.70.0.24
7	Whatshapp	2.21.150
8	Instagram	198.0.0.32.120

Perancangan Skenario

Perancangan skenario dalam penelitian ini bertujuan untuk menunjang keberhasilan proses investigasi terhadap fitur pesan sekali lihat pada tiga aplikasi pesan instan, yaitu Snapchat, WhatsApp Messenger, dan Instagram. Skenario dirancang sebagai simulasi kejadian pengiriman pesan yang memungkinkan peneliti mengamati jejak digital yang tertinggal, baik dalam bentuk file gambar maupun video. Simulasi dilakukan selama tiga hari berturut-turut, dimulai pada hari Senin, 9 Desember 2024 hingga Rabu, 11 Desember 2024. Pada setiap hari, dilakukan pengiriman pesan menggunakan fitur sekali lihat pada ketiga aplikasi yang menjadi objek penelitian. Rincian yang dilakukan dalam yaitu:

1) Senin, 9 Desember 2024
   Pengiriman pesan berupa gambar dan video menggunakan fitur sekali lihat pada aplikasi Snapchat, WhatsApp Messenger, dan Instagram.
2) Selasa, 10 Desember 2024
   Pengiriman pesan berupa gambar dan video menggunakan fitur sekali lihat pada ketiga aplikasi yang sama.
3) Rabu, 11 Desember 2024
   Pengiriman pesan berupa gambar dan video menggunakan fitur sekali lihat pada Snapchat, WhatsApp Messenger, dan Instagram.

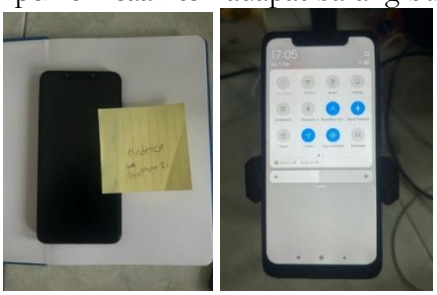
Visualisasi skenario pengiriman pesan pada masing-masing aplikasi ditampilkan pada Gambar 3. Tahapan ini selanjutnya menjadi dasar pelaksanaan proses pengujian forensik digital untuk mengidentifikasi artefak yang dapat diperoleh dari masing-masing skenario penggunaan fitur pesan sementara.



Gambar 3. Skenario dari aplikasi Snapchat, WhatsApp dan Instagram

Pengumpulan (Collection)

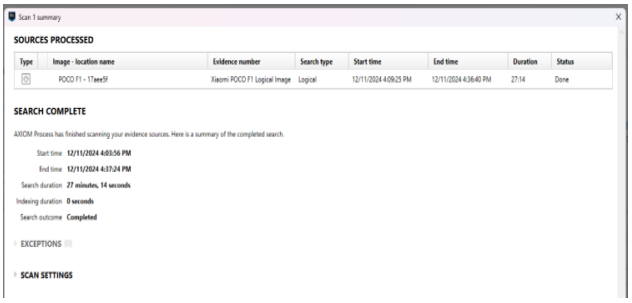
Pada gambar 4 merupakan dokumentasi barang bukti fisik *smartphone* yang digunakan untuk skenario kasus pengiriman pesan sekali lihat. Smartphone xiomi Pocophone F1 tersebut menggunakan sistem operasi android 10.0 dan sudah terinstall aplikasi *Instant Messaging* Snapchat, Instagram, dan Whatsapp. Selanjutnya akan dilakukan proses pemeriksaan terhadapa barang bukti yang di dapatkan. Langkah-langkah yang dilakukan meliputi pemberian label pada telpon pintar dan pengamanan dengan mematikan koneksi nirkabel (*Wi-Fi, Bluetooth*) serta jaringan seluler melalui mode pesawat untuk menjaga integritas barang bukti supaya tidak ada perubahan data yang ada di dalamnya. Tahap selanjutanya akan dilakukan pemeriksaan terhadapat barang bukti.



Gambar 4. Pengamanan barang bukti

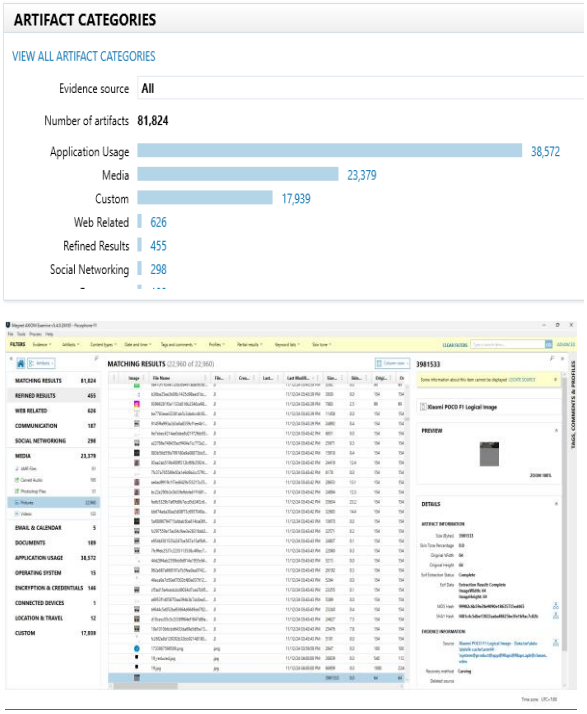
Pemeriksaan (*Examination*)

Pada tahap pemerikassan peneliti melakukan proses imaging dengan menggunakan *Tools* forensik Magnet Axiom. Proses ini dilakukan untuk mengakuisisi data dan file yang tersimpan dalam barang bukti. Proses dilakukan dengan menghubungkan barang bukti berupa Smarphone Pocophone F1 dengan kabel USB Type- C melalui port USB pada laptop, selanjutnya menjalankan aplikasi Forensik Magnet Axiom Proses *imaging* berlangsung dalam durasi yang tidak ditentukan; semakin banyak data yang ada, semakin lama waktu yang dibutuhkan. kondisi root untuk memungkinkan pengambilan data yang telah dihapus atau disembunyikan dalam upaya menghilangkan jejak atau bukti digital.



Gambar 5. Proses imaging data

Pada gambar 5 barang bukti Xiomi pocophone F1 saat proses pengambilan data menggunakan Tools Magnet Axiom pada tanggal 11 Desember 2024, dari pukul 16:03:56 hingga pukul 16:37:24, proses imaging data membutuhkan waktu 27 menit 14 detik.

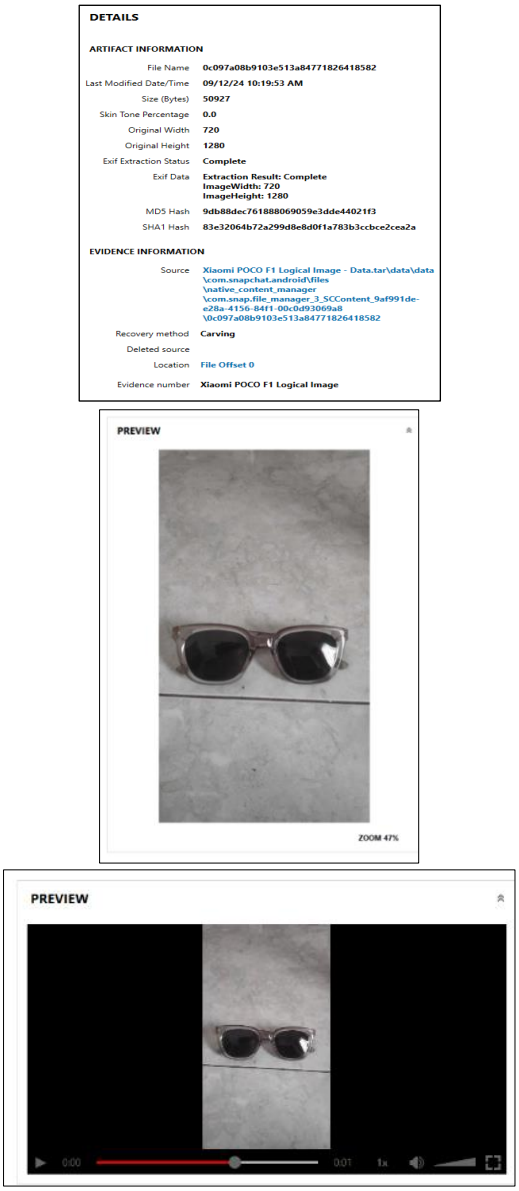


Gambar 6. Informasi Artefak Dari Smarphone Hasil Akusisi Magnet Axiom

Hasi dari pemeriksaan menggunkaan *Tools* Magnet Axiom menemukan 81.824 artefak dari smartphone Pocophone F1. Penelitian ini secara khusus berfokus pada pencarian bukti digital berupa foto dan video yang menggunakan fitur sekali lihat. Dalam artefak media, berhasil diakuisisi 22.960 foto dan 132 video dari total 23.379 artefak media yang ditemukan daapt dilihat pada gambar 6. Hasil akuisisi menggunakan *Tools* Magnet Axiom kemudian akan dianalisis lebih lanjut menggunakan tool Axiom Examine untuk mencari bukti digital yang dihasilkan berdasarkan skenario yang telah dibuat.

Analisis (Analysis)

pada proses ini bertujuan untuk mengungkap dengan melakukan analisis atas hasil dari tahap examination untuk memperoleh data yang diharapkan sebagai bukti digital. Proses dilakukan dengan mencari data yang dihapus atau file yang tersembunyi saat penggunaan fitur sekali lihat. Selanjutnya dilakukan dokumentasi terhadap data atau file yang telah ditemukan.



Gambar 7. Beberapa artefak temuan bukti digital yang berhasil

Pada gambar 7 memperlihatkan beberapa bukti artefak yang berhasil ditemukan setelah di lakuan akusisi menggunakan *Tools* forensik Magnet Axiom pada aplikasi Snapchat, WhatsApp dan Instagram, temuan juga memperlihatkan meta data dari bebrapa bukti digital yang ditemukan antaranya detail waktu pengiriman pesan tersebut, adanya nilai hash dan lokasi ditemukannya artefak bukti digital.

Tabel 2. Hasil Temuan Tanggal 09/12/2024

No	Skenario Tanggal 09/12/24	Nama File	Nilai Hash	Lokasi
1	Snapchat Pesan Gambar Pukul 10:19:53 AM	0c097a08b9103e513a847718264185 82	83e32064b72a299d8e8d0f1a783b3ccbce2cea2a	Data.tar\data\data\com.snapchat.android\files\native_content_manager\com.snap.file_manager_3_SCContent_9af991de-e28a-4156-84f1-00c0d93069a8\0c097a08b9103e513a8477182641858
2	Snapchat Pesan video Pukul 10:20:10 AM	2c7ff86795ef25a68f043889950d5230	0053356594e803c5f5b52ba5ad77724ff29f9093	Data.tar\data\data\com.snapchat.android\files\native_content_manager\com.snap.file_manager_3_SCContent_9af991de-e28a-4156-84f1-00c0d93069a8\2c7ff86795ef25a68f043889950d5230
3	WhatsApp Pesan Gambar Pukul 10:20:36 AM	ae2d4f51-dea9-46c2-a12d-0a7066a70dad.jpg	78a8fc78cdb61e6d4634576cf37eb372ec36dc69	Data.tar\data\data\com.whatsapp\files\.Shared\ae2d4f51-dea9-46c2-a12d-0a7066a70dad.jpg
4	WhatsApp Pesan video pukul	Tidak ditemukan	Tidak ditemukan	Tidak ditemukan
5	Instagram Pesan Gambar pukul	Tidak ditemukan	Tidak ditemukan	Tidak ditemukan
6	Instagram Pesan video pukul	Tidak ditemukan	Tidak ditemukan	Tidak ditemukan

Tabel 3. Hasil Temuan Tanggal 10/12/24

No	Skenario Tanggal 10/12/24	Nama File	Nilai Hash	Lokasi
1	Snapchat Pesan Gambar Pukul 10/12/24 PM	36cb3b87a0893a38cd894da497218593	8c23352ec6e63f3d74089b95fbe6452083c74613	Data.tar\data\data\com.snapchat.android\files\native_content_manager\com.snap.file_manager_3_SCContent_9af991de-e28a-4156-84f1-00c0d93069a8\36cb3b87a0893a38cd894da497218593
2	Snapchat Pesan video Pukul 08:15:07 PM	e7967 45cf084294702c382a16bd0c5f9	2721a2acac689786b5ec59590e36d8bca7f5a445	Data.tar\data\data\com.snapchat.android\files\native_content_manager\com.snap.file_manager_3_SCContent_9af991de-e28a-4156-84f1-

				00c0d93069a8\e796745cf 084294702c382a16bd0c5f9
3	WhatsApp Pesan Gambar Pukul PM	9abb556d-bd83-4888-868f-bd65db0e18fd.jpg	7390022ef02b6d44c7249746a2f9d8db8a57f8ef	Data.tar\data\data\com.whatsapp\files\.Shared\9abb556d-bd83-4888-868f-bd65db0e18fd.jpg

Tabel 4. Hasil Temuan Tanggal 10/12/24 (Lanjutan)

No	Skenario Tanggal 10/12/24	Nama File	Nilai Hash	Lokasi
4	WhatsApp Pesan video pukul	Tidak ditemukan	Tidak ditemukan	Tidak ditemukan
5	Instagram Pesan Gambar Pukul 08:13:23 PM	pending_media_2308884126145962449.jpg	fc49197592fff28de058dd2dacfab6a1106311f8	Data.tar\data\data\com.instagram.android\files\pending_media_images\pending_media_2308884126145962449.jpg
6	Instagram Pesan video Pukul 08:13:42 PM	VID_20241210_051340_238.mp4	ec6255a0cd391d155dde5e8fb34cdb707cb2a061	Data.tar\data\data\com.instagram.android\files\rendered_videos\VID_20241210_051340_238.mp4

Tabel 5. Hasil Temuan Tanggal 11/12/2024

No	Skenario Tanggal 11/12/24	Nama File	Nilai Hash	Lokasi
1	Snapchat Pesan Gambar Pukul 03:41:03 PM	c0f0b14e30db5b4f5f9bd3b475a8949b	7222c23bc6b6de58a77e2bbb7c8640fc4b699cb7	Data.tar\data\data\com.snapchat.android\files\native_content_manager\com.snap.file_manager_3_SCContent_9af991de-e28a-4156-84f1-00c0d93069a8\c0f0b14e30db5b4f5f9bd3b475a8949b
2	Snapchat Pesan video Pukul 03:41:18 PM	29d16227a719649eb52b1afe8711ff91	c1ed45bedd044d9421cd4c448f7b4ffe27e0b5ee	Data.tar\data\data\com.snapchat.android\files\native_content_manager\com.snap.file_manager_3_SCContent_9af991de-e28a-4156-84f1-00c0d93069a8\29d16227a719649eb52b1afe8711ff91
3	WhatsApp Pesan Gambar Pukul 03:39:17 PM	03ddd106-2171-4feb-9dbf-840ce7d6cd96.jpg	58e2bb65059434c7272373f41cb95282491a05d5	Data.tar\data\data\com.whatsapp\files\.Shared\03ddd106-2171-4feb-9dbf-840ce7d6cd96.jpg

4	WhatsApp Pesan video Pukul 03:39:17 PM	Tidak ditemukan	Tidak ditemukan	Tidak ditemukan
5	Instagram Pesan Gambar Pukul 03:40:21 PM	pending_media_610369083281451556 6.jpg	bcac415249d4af94cc22dd8bbf24bd120fed40af	Data.tar\data\data\com.instagram.android\files\pending_media_images\pending_media_6103690832814515566.jpg
6	Instagram Pesan video Pukul 03:40:38 PM	VID_20241211_004036_752.mp4	effea64e92e09ea5ae1ec1e4474aca20482857b1	Data.tar\data\data\com.instagram.android\files\rendered_videos\VID_20241211_004036_752.mp4

Hasil temuan dari proses investigasi digital dirangkum dalam Tabel 3, 4, dan 5. Ketiga tabel tersebut menyajikan data artefak yang berhasil diperoleh dari perangkat seluler yang telah di-*root*, melalui skenario pengujian fitur pesan sekali lihat pada aplikasi Snapchat, WhatsApp Messenger, dan Instagram. Proses akuisisi dilakukan selama tiga hari, sesuai dengan desain skenario yang telah ditentukan sebelumnya. Secara keseluruhan, total skenario dan jumlah artefak digital yang berhasil diidentifikasi ditampilkan dalam Tabel 5. Berdasarkan hasil pengujian, terdapat beberapa kondisi di mana artefak tidak berhasil ditemukan. Salah satunya adalah pada aplikasi Instagram, di mana baik foto maupun video dari fitur pesan sekali lihat yang dikirim pada tanggal 9 Desember 2024 tidak terdeteksi. Selain itu, seluruh skenario pengujian pada WhatsApp tidak menghasilkan artefak berupa video dari fitur serupa, meskipun artefak gambar masih dapat ditemukan.

Tabel 6. Total keberhasilan menemukan artefak bukti digital pesan sekali lihat

Skenario	Snapchat	Instagram	WhatsApp
Pesan Gambar Sekali Lihat	3	2	3
Pesan Video Sekali Lihat	3	2	-

Reporting

Reporting adalah tahap terakhir setelah proses pemeriksaan dan pengumpulan bukti digital menggunakan *Tools* Magnet Axiom, langkah berikutnya adalah menyusun laporan lengkap yang berisi temuan analisis. Hasil akuisisi barang bukti digital dari aplikasi Snapchat, WhatsApp dan Instagram diringkas dalam Tabel 7.

Tabel 7. Hasil Akusisi barang bukti digital dari aplikasi Snapchat, WhatsApp, dan Instagram menggunakan Tools Magnet Axiom

Barang Bukti	Skenario 09/12/24			Skenario 10/12/24			Skenario 11/12/24		
	Snapchat	WhatsApp	Instagram	Snapchat	WhatsApp	Instagram	Snapchat	WhatsApp	Instagram
Gambar	✓	✓	x	✓	✓	✓	✓	✓	✓
Video	✓	✓	x	✓	x	✓	✓	x	✓

Penelitian ini menguji tiga aplikasi pesan instan—Snapchat, Instagram, dan WhatsApp—untuk memperoleh bukti digital dari fitur pesan sekali lihat. Validasi terhadap bukti digital dilakukan melalui pemeriksaan nilai *hash* dari hasil akuisisi dan analisis menggunakan perangkat lunak forensik Magnet Axiom. Nilai *hash* merupakan kode unik dalam bentuk karakter alfanumerik yang dihasilkan oleh algoritma tertentu berdasarkan isi file digital. Kode ini digunakan untuk memastikan keutuhan dan keaslian data digital, sehingga artefak yang diperoleh dapat dipertanggungjawabkan secara hukum (Kustian, 2023). Hasil pengujian menunjukkan capaian sebagai berikut:

1) Snapchat

   Seluruh bukti digital yang dikirim dalam skenario pengujian 3 gambar dan 3 video berhasil diidentifikasi. Dengan kata lain, 6 dari 6 artefak

dapat diperoleh dari perangkat yang telah di-*root*.

2) Instagram
   Sebanyak 4 dari 6 artefak berhasil ditemukan, terdiri dari 2 gambar dan 2 video. Tidak ditemukan bukti pada tanggal 9 Desember 2024, namun pada tanggal 10 dan 11 Desember bukti digital dapat diperoleh.
3) WhatsApp
   Hanya 3 dari 6 artefak yang berhasil diidentifikasi, seluruhnya berupa gambar. Tidak ditemukan artefak video dari fitur pesan sekali lihat pada semua skenario pengujian.

Analisis lebih lanjut menunjukkan bahwa setiap aplikasi memiliki karakteristik tersendiri dalam mengelola pesan sementara, yang berdampak pada kemungkinan ditemukannya artefak digital:

1) Snapchat memiliki sistem otomatis yang menghapus pesan segera setelah dibuka, dengan durasi tampilan yang dapat diatur antara 1 hingga 10 detik. Selain itu, riwayat obrolan akan dihapus dalam waktu 24 jam, dan aplikasi ini mampu mendeteksi aktivitas tangkapan layar oleh pengguna, yang terekam dalam log percakapan.
2) WhatsApp menerapkan perlindungan tambahan dengan memblokir fitur tangkapan layar untuk pesan sekali lihat, menjadikannya lebih sulit diakses melalui teknik forensik standar. Pada versi 2.21.150 yang diuji menggunakan Magnet Axiom v5.4.0, tidak ditemukan artefak video, yang mengindikasikan adanya mekanisme penghapusan yang lebih agresif atau enkripsi tambahan.
3) Instagram menampilkan fitur pesan sekali lihat yang secara otomatis menghapus pesan dalam waktu dua hari. Artefak dari pesan yang dikirim pada tanggal pertama pengujian tidak ditemukan, yang menunjukkan kemungkinan penghapusan otomatis sebelum proses akuisisi dilakukan.

Berdasarkan temuan tersebut, dapat disimpulkan bahwa penggunaan fitur pesan sekali lihat pada Snapchat, dengan kondisi perangkat telah di-*root*, memungkinkan akuisisi penuh terhadap artefak digital baik gambar maupun video. Pada Instagram, sebagian artefak dapat ditemukan, sedangkan pada WhatsApp hanya artefak gambar yang berhasil diidentifikasi. Validasi terhadap keabsahan bukti digital dilakukan melalui pemeriksaan nilai *hash*, yang menjadi indikator integritas setiap file hasil akuisisi. Nilai *hash* yang konsisten dan tidak berubah menjamin bahwa data belum mengalami modifikasi selama proses analisis.

DETAILS

ARTIFACT INFORMATION

File Name	0c097a08b9103e513a84771826418582
Last Modified Date/Time	09/12/24 10:19:53 AM
Size (Bytes)	50927
Skin Tone Percentage	0.0
Original Width	720
Original Height	1280
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 720 ImageHeight: 1280
MD5 Hash	9db88dec761888069059e3dde44021f3
SHA1 Hash	83e32064b72a299d8e8d0f1a783b3ccbce2cea2a

EVIDENCE INFORMATION

Source	Xiaomi POCO F1 Logical Image - Data.tar\data\data\com.snapchat.android\files\native_content_manager\com.snap.file_manager_3_SCContent_9af991de-e28a-4156-84f1-00c0d93069a8\0c097a08b9103e513a84771826418582
Recovery method	Carving
Deleted source	
Location	File Offset 0
Evidence number	Xiaomi POCO F1 Logical Image

Gambar 8. Validasi temuan artefak digital

Bukti validasi dari fitur pesan sekali lihat ditemukan menggunakan *Tools* Magnet Axiom pada gambar 8 memperlihatkan informasi kapan waktu pesan yang dikirim sama dengan Screenshot skenario sebelum dikirim, pada tanggal 09/12/2024 pada pukul 10:19:52. bukti artefak yang ditemukan juga menunjukkan adanya nilai hash.

Pembahasan

Penelitian ini bertujuan untuk mengkaji efektivitas teknik forensik digital dalam menginvestigasi fitur

pesan sekali lihat (*view once*) pada aplikasi pesan instan, yaitu Snapchat, WhatsApp, dan Instagram. Skenario pengiriman pesan berupa gambar dan video dilakukan selama tiga hari berturut-turut, mulai tanggal 9 hingga 11 Desember 2024, menggunakan perangkat Android yang telah di-*root*. Hasil investigasi menggunakan perangkat lunak Magnet Axiom berhasil mengidentifikasi 13 dari 18 artefak digital yang dikirim melalui fitur tersebut. Secara rinci, aplikasi Snapchat menunjukkan hasil paling optimal dengan tingkat keberhasilan 100%, di mana semua pesan gambar dan video yang dikirimkan berhasil diperoleh kembali. Hal ini menunjukkan bahwa meskipun fitur pesan sekali lihat bertujuan menghapus jejak pesan secara otomatis, penggunaan teknik forensik dengan dukungan sistem terbuka (perangkat *rooted*) masih memungkinkan untuk mengekstraksi artefak dari aplikasi tersebut. Pada Instagram, sebanyak empat artefak digital berhasil ditemukan, yaitu dua gambar dan dua video. Meskipun pada hari pertama pengujian tidak ditemukan artefak apapun, temuan dari dua hari berikutnya menunjukkan bahwa fitur pesan sekali lihat di Instagram masih menyisakan jejak digital yang dapat diakses menggunakan metode forensik tertentu.

Berbeda halnya dengan WhatsApp, hanya tiga artefak digital berupa gambar yang berhasil diidentifikasi, sementara tidak ditemukan artefak video dari seluruh skenario pengujian. Hal ini mengindikasikan bahwa sistem proteksi WhatsApp terhadap pesan sekali lihat, khususnya untuk konten video, memiliki mekanisme penghapusan atau enkripsi yang lebih kuat, sehingga menyulitkan proses akuisisi. Temuan penelitian ini sejalan dengan studi sebelumnya. Penelitian yang dilakukan oleh Rofiq *et al.* (2022) menggunakan kerangka kerja NIST SP 800-101 Rev-1 pada WhatsApp dan Telegram, menunjukkan bahwa proses akuisisi data dari fitur *view once* pada WhatsApp berhasil dilakukan pada perangkat yang telah di-*root*, namun fitur *self-destruct* pada Telegram tidak menghasilkan artefak selain riwayat percakapan. Hal serupa juga ditemukan dalam penelitian Sidik Asyaky *et al.* (2018), yang menyatakan bahwa proses akuisisi terhadap pesan yang ditarik atau dihapus dari aplikasi seperti WhatsApp, Telegram, Line, dan IMO masih menjadi tantangan, karena data tersebut belum tersimpan secara permanen dalam basis data utama aplikasi. Qibriya *et al.* (2021) berhasil mengakses berbagai data dari perangkat Android menggunakan metode *physical imaging*, termasuk percakapan, berkas media, dan daftar kontak. Sementara itu, Rafiq *et al.* (2022) membandingkan kinerja perangkat lunak Belkasoft Evidence Center dengan Magnet Axiom dalam akuisisi artefak dari aplikasi Instagram, dan menemukan bahwa Magnet Axiom lebih unggul dalam memulihkan data yang telah dihapus. Studi oleh Liffner (2019) juga memperkuat temuan ini, dengan menunjukkan bahwa aplikasi Snapchat masih memungkinkan untuk dilakukan ekstraksi data, termasuk gambar dan percakapan, bahkan untuk video yang belum sepenuhnya dilihat oleh pengguna, asalkan perangkat telah di-*root*. Secara keseluruhan, berbagai penelitian sebelumnya menunjukkan adanya hambatan umum dalam memperoleh artefak digital dari fitur yang dirancang untuk menjaga privasi dan menghapus pesan secara otomatis. Hal tersebut menjadi tantangan utama dalam ranah forensik digital, terutama untuk mengembangkan teknik investigasi yang lebih efektif dan relevan. Masih terbatasnya jumlah penelitian yang secara khusus membahas fitur-fitur terbaru seperti pesan sekali lihat memperkuat urgensi pengembangan studi lanjutan di bidang ini.

4. Kesimpulan dan Saran

Penelitian ini telah mengevaluasi efektivitas teknik forensik digital dalam menginvestigasi fitur pesan sekali lihat (*view once*) pada tiga aplikasi pesan instan, yaitu Snapchat, WhatsApp, dan Instagram. Proses pengujian dilakukan selama tiga hari, mulai 9 hingga 11 Desember 2024, dengan skenario pengiriman gambar dan video melalui fitur pesan sementara pada perangkat Android yang telah di-*root*. Dari total 18 artefak digital yang ditargetkan, sebanyak 13 berhasil diperoleh menggunakan perangkat lunak Magnet Axiom. Aplikasi Snapchat menunjukkan tingkat keberhasilan tertinggi dengan temuan lengkap terhadap seluruh bukti digital yang dikirim, terdiri dari tiga gambar dan tiga video. WhatsApp hanya menghasilkan tiga artefak digital berupa gambar, tanpa ditemukan satupun artefak video. Sementara itu, Instagram menghasilkan empat artefak, masing-masing dua gambar dan dua video. Perbedaan karakteristik dari fitur pesan sekali lihat pada ketiga aplikasi mempengaruhi tingkat keberhasilan akuisisi

bukti digital. Snapchat secara otomatis menghapus pesan dari riwayat obrolan setelah 24 jam dan menampilkan notifikasi jika terjadi tangkapan layar oleh penerima. WhatsApp menerapkan sistem perlindungan dengan memblokir fungsi tangkapan layar, yang berpotensi menjadi tantangan dalam proses akuisisi forensik. Instagram memiliki durasi penyimpanan pesan sementara hingga dua hari, namun artefak digitalnya cenderung sulit ditemukan. Berdasarkan temuan tersebut, penelitian ini merekomendasikan beberapa hal untuk pengembangan studi selanjutnya:

1) Penggunaan Versi Aplikasi Terbaru
   Disarankan untuk menggunakan versi aplikasi terkini agar hasil investigasi mencerminkan kondisi keamanan dan fitur aktual yang diterapkan oleh masing-masing pengembang.
2) Kombinasi Perangkat Forensik
   Penelitian lanjutan perlu mempertimbangkan penggunaan berbagai perangkat lunak forensik sebagai upaya untuk meningkatkan keberhasilan akuisisi data digital, mengingat setiap alat memiliki kemampuan dan pendekatan teknis yang berbeda.
3) Pendekatan Multiplatform dan Multi-skenario
   Evaluasi lebih lanjut dapat dilakukan dengan memperluas skenario pengujian, termasuk pengujian pada perangkat dengan sistem operasi berbeda atau kondisi jaringan tertentu, guna memperoleh gambaran yang lebih utuh mengenai efektivitas teknik forensik digital terhadap fitur pesan sekali lihat.

5. Daftar Pustaka

Arsyad, J. H. (2022). Perlindungan hukum korban kekerasan berbasis gender online (KBGO) dalam hukum positif Indonesia. *Jurnal Cakrawala Informasi*, 2(2), 26–41. https://doi.org/10.54066/jci.v2i2.241.

Asyaky, M. S., Widiyasono, N., & Gunawan, R. (2018). Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android. *Sinkron: jurnal dan penelitian teknik informatika*, *3*(1), 220-231.

Aziz, M. A., Sulistyo, W. Y., & Astari, S. R. (2021). Komparatif anti forensik aplikasi instant messaging berbasis web menggunakan metode Association of Chief Police Officers (ACPO). *JURISTIK (Jurnal Riset Teknologi Informasi dan Komputer)*, 1(01), 8–15. https://doi.org/10.53863/juristik.v1i01.341.

Harahap, D. P. (2023). Implementasi digital forensik aplikasi dompet digital dan pesan instan pada Android dengan menggunakan metode NIST. *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, 6(1), 533–541. https://doi.org/10.30865/komik.v6i1.5715.

Kustian, M. A. (2023). Analisis forensik penggunaan fungsi hash dalam menentukan keaslian video, metadata image dan magic number file. *Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi*, 2(2), 10–16. https://doi.org/10.20885/snati.v2i2.21.

Majalista, R., & Sutabri, T. (2023). Analisis Pencarian Data Smartphone Menggunakan Nist untuk Penyelidikan Digital Forensik. *Jurnal Informatika Teknologi dan Sains (Jinteks)*, *5*(1), 81-85. https://doi.org/10.51401/jinteks.v5i1.2200.

Nafila, F. L. (2021). Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android Menggunakan metode NIST.

Nordin, A., & Liffner, F. (2019). Forensiska Artefakter hos Mobila Applikationer: Utvinning och Analys av Applikationen Snapchat.

Plianda, I. A., & Indrayani, R. (2022). Analisa dan perbandingan performa tools forensik digital pada smartphone Android menggunakan Instant Messaging WhatsApp. *Jurnal Media Informatika Budidarma*, 6(1), 500. https://doi.org/10.30865/mib.v6i1.3487.

Putra, G. A. A. P., Sukerti, N. K., & Putri, N. M. D. K. (2024, October). Simulasi Investigasi pada FlashDisk dalam Mengungkap Pesan pada Kasus Perdagangan Narkoba Menggunakan Metode Steganografi. In *Seminar Hasil Penelitian Informatika dan Komputer (SPINTER)| Institut*

Teknologi dan Bisnis STIKOM Bali (Vol. 1, No. 3, pp. 340-345).

Qibriya, M. R. D., Ambarwati, A., & Susilo, K. E. (2021). Analisis forensik digital pada aplikasi instant messaging di smartphone berbasis Android untuk bukti digital. *Jurnal Teknologi Informasi*, 5(2), 114–121. https://doi.org/10.36294/jurti.v5i2.2200.

Rafiq, I. A., Riadi, I., & Herman. (2022). Perbandingan forensic tools pada Instagram menggunakan metode NIST. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 7(2), 134–142. https://doi.org/10.14421/jiska.2022.7.2.134-142.

Rofiq, T. Y. R. A., Setiadji, M. Y. B., & Priambodo, D. F. (2022). Analisis bukti digital pada fitur view once WhatsApp dan self-destruct Telegram menggunakan metode NIST SP 800-101 Rev-1. *Politeknik Siber dan Sandi Negara*, xiv, 58.

Wirara, A., Hardiawan, B., & Salman, M. (2020). Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan "WhatsApp". *Teknoin*, *26*(1), 66-74. https://doi.org/10.20885/teknoin.vol26.iss1.art7.

Yel, M. B., & Nasution, M. K. M. (2022). Keamanan informasi data pribadi pada media sosial. *Jurnal Informatika Kaputama*, 6(1), 92–101. https://doi.org/10.59697/jik.v6i1.144.