CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 2, November 2025, hlm. 124-134

Analisis Forensik Digital Aplikasi Signal Desktop Pada Windows 11 Menggunakan Metodologi Forensik Digital Berbasis ISO/IEC 27037:2012 Dan ISO/IEC 27042:2015

Ahmad Anwary Adzirudin[1], Ghaly Arkan Adiyatma[2], Rizky Pratama Putra[3], Trystan Adrian Hanggara Wibawa[4]

[1,2,3]Program Studi Rekayasa Keamanan Siber, Jurusan Keamanan Siber, Politeknik Siber dan Sandi Negara
Email: anwaryahmad123@gmail.com[1], ghalyarkan4@gmail.com[2], rizky.pratamap229@gmail.com[3], trystanadrian96@gmail.com[4]

Abstrak

Aplikasi Signal merupakan aplikasi pesan instan yang dikenal memiliki tingkat keamanan dan privasi tinggi melalui penerapan end-to-end encryption. Namun, keunggulan tersebut juga sering dimanfaatkan oleh pelaku kejahatan untuk menyembunyikan atau menghapus barang bukti digital, khususnya pada platform Windows. Sejumlah penelitian sebelumnya telah menunjukkan keberhasilan analisis forensik terhadap Signal Messenger pada perangkat seluler dengan berbagai metode dan alat bantu. Akan tetapi, penelitian terkait artefak digital Signal Desktop pada sistem operasi terbaru masih terbatas. Penelitian ini berfokus pada eksplorasi artefak digital aplikasi Signal Desktop di lingkungan Windows 11 untuk mengungkap potensi bukti digital yang dapat diperoleh. Metodologi penelitian menggunakan standar ISO/IEC 27037:2012 untuk tahap identifikasi, pengumpulan, akuisisi, dan preservasi bukti, serta ISO/IEC 27042:2015 untuk tahap analisis, interpretasi, dan pelaporan. Alat bantu forensik yang digunakan adalah FTK Imager untuk akuisisi data dan Autopsy untuk analisis. Penelitian dilakukan dengan tiga skenario, yaitu penggunaan normal tanpa penghapusan, penghapusan pesan dan file, serta proses *uninstall* aplikasi. Hasil penelitian menunjukkan bahwa artefak digital seperti pesan teks, gambar, video, dan file PDF masih dapat ditemukan pada skenario penggunaan normal. Pada skenario penghapusan, artefak gambar, video, dan file PDF dapat dipulihkan sebagai *deleted files*, sedangkan teks pesan sulit direkonstruksi. Sementara itu, pada skenario *uninstall*, sebagian besar artefak digital tidak lagi dapat ditemukan. Temuan ini membuktikan bahwa penerapan ISO/IEC 27037:2012 dan ISO/IEC 27042:2015 efektif dalam memperoleh, menjaga integritas, serta menganalisis bukti digital aplikasi Signal Desktop secara sistematis.

Kata kunci: *Forensik Digital, Signal Desktop, Windows 11, ISO/IEC 27037:2012, ISO/IEC 27042:2015, FTK Imager, Autopsy*

Digital Forensic Analysis Of Desktop Signal Applications On Windows 11 Using Digital Forensic Methodology Based On ISO/IEC 27037:2012 And ISO/IEC 27042:2015

Abstract

The Signal application is an instant messaging platform well-known for its high level of security and privacy through the use of end-to-end encryption. However, these advantages are often exploited by criminals to conceal or erase digital evidence, especially on the Windows platform. Previous studies have demonstrated the effectiveness of forensic methods on Signal Messenger mobile devices using various tools and frameworks, but research on Signal Desktop artifacts in the latest operating systems remains limited. This study explores digital artifacts of Signal Desktop on Windows 11 to identify potential digital evidence that can be recovered. The methodology applies ISO/IEC 27037:2012 for the identification, collection, acquisition, and preservation of evidence, and ISO/IEC 27042:2015 for the analysis, interpretation, and reporting stages. The forensic tools employed are FTK Imager for data acquisition and Autopsy for artifact analysis. The experiment was conducted using three scenarios: normal usage without deletion, deletion of messages and files, and application uninstallation. The results show that digital artifacts such as text messages, images, videos, and PDF files can be retrieved in normal usage. In the deletion scenario, images, videos, and PDF files were recoverable as deleted files, whereas text messages were unrecoverable. In the uninstallation scenario, most artifacts were no longer accessible. These findings confirm that ISO/IEC 27037:2012 and ISO/IEC 27042:2015 provide a systematic and reliable framework for acquiring, preserving, and analyzing digital evidence in the context of Signal Desktop..

Keywords*: Digital Forensics, Signal Desktop, Windows 11, ISO/IEC 27037:2012, ISO/IEC 27042:2015, FTK Imager, Autopsy*

1. PENDAHULUAN

Windows merupakan sistem operasi yang paling populer digunakan pada desktop. Popularitas ini tidak terlepas dari kemudahan penggunaannya, dimana windows menawarkan antarmuka pengguna yang mudah dan menarik, sehingga cocok untuk berbagai kalangan (Statcounter GlobalStats, 2025). Kepopuleran Windows turut mendorong banyak pengembang untuk membuat aplikasi yang kompatibel dengan sistem ini, termasuk aplikasi perpesanan. Salah satu aplikasi yang banyak digunakan untuk komunikasi aman adalah Signal Desktop, aplikasi yang dapat diunduh secara gratis melalui Windows Desktop.

Signal desktop adalah aplikasi pesan instan yang dirancang dengan fokus pada keamanan dan privasi tinggi. Sebagai versi desktop dari Signal Messenger, aplikasi ini terhubung ke perangkat seluler melalui pemindaian kode QR (*quick response code*) dan memungkinkan pengguna mengirim pesan teks, foto, video, audio, *file*, serta melakukan panggilan suara dan video dengan enkripsi *end-to-end* (Irawan and Riadi, 2022). Keunggulan Signal terletak pada transparansi dan keamanannya yang kuat, menggunakan protokol Signal yang telah diadopsi oleh berbagai platform lain karena keandalannya dalam melindungi data pengguna (Cohn-Gordon *et al*., 2020).

Meskipun Signal dikenal memiliki keamanan tinggi, aplikasi ini tidak terlepas dari ancaman kejahatan seperti penipuan, manipulasi informasi, dan penyalahgunaan dalam transaksi bisnis (Bestari, 2025). Berdasarkan setiap tindak kejahatan yang dilakukan pasti meninggalkan barang bukti termasuk bukti digital (Faruq, Andri and Yudi, 2020). Barang bukti yang biasa disimpan dan ditransmisikan dalam perangkat elektronik merupakan bukti digital (Subektiningsih, 2016). Para penjahat sering mencoba untuk menyembunyikan atau menghilangkan jejak bukti digital dari perangkat elektronik hasil kejahatan (Sunardi, Riadi and Akbar, 2020). Oleh karena itu, forensik digital memegang peran penting dalam mengungkap bukti elektronik, termasuk pada aplikasi perpesanan seperti Signal yang memiliki sistem keamanan tinggi.

Forensik digital merupakan cabang ilmu yang berfokus dalam pemulihan, analisis, dan penyajian bukti digital terkait kejahatan siber dan aktivitas ilegal lainnya melalui identifikasi, preservasi, koleksi, validasi, analisis, interpretasi, dokumentasi, dan presentasi bukti digital. Bukti tersebut berasal dari perangkat elektronik seperti komputer, laptop, jam tangan pintar, dan ponsel pintar (Irawan and Riadi, 2022). Demikian pula, kerangka kerja Digital *Forensic*s Research Workshop (DFRWS) meningkatkan investigasi digital dengan memungkinkan analisis terstruktur, termasuk ekstraksi file steganografi (Prayogo and Riadi, 2022). Pentingnya model forensik yang terharmonisasi ditegaskan oleh Valjarević dan Venter (2015), yang menyoroti kompleksitas bukti digital dan ancaman siber yang terus berkembang (Valjarevic and Venter, 2013). Untuk memastikan ketelitian ilmiah dalam metodologi forensik, aturan Daubert mengatur keberterimaan kesaksian ahli, menegaskan pentingnya proses forensik yang standar (Valjarevic and Venter, 2013). Sementara Montasari, (2016), menilai model forensik yang ada berdasarkan kepatuhannya terhadap standar ilmiah dan penerapannya dalam dunia nyata (Montasari, 2016).

Berbagai penelitian telah dilakukan terkait forensik digital pada aplikasi perpesanan instan, termasuk Signal Messenger dengan menggunakan berbagai metode. Paulino et al. (2025) memperkenalkan skrip Python otomatis untuk menganalisis artefak forensik dari Signal Desktop pada Windows. Penelitian yang dilakukan oleh Riadi (Riadi, Herman and Imam, 2022), juga mengungkap bahwa metode forensik berbasis NIST mampu mengekstrak berbagai jenis data dari Signal Messenger, termasuk riwayat percakapan, gambar, GIF, dokumen PDF, video, serta catatan panggilan suara dan video. Hasil penelitian tersebut menunjukkan bahwa artefak digital seperti gambar, GIF, dokumen PDF, dan video dapat diperoleh secara utuh (100%) dari perangkat yang telah di-*root*. Onik (2025) menyusun tren forensik perpesanan instan terkini, menekankan perlunya metodologi konsisten dalam analisis aplikasi terenkripsi seperti Signal.

Selain itu, identifikasi juga berhasil dilakukan terhadap riwayat pesan, daftar kontak, detail panggilan, serta lokasi penyimpanan *file* video di kartu memori. Penelitian lain oleh Irawan (Irawan and Riadi, 2022), menunjukkan bahwa artefak digital dari perangkat yang telah di-*root* dapat diekstraksi menggunakan berbagai alat forensik, seperti Belkasoft Evidence Center, Magnet AXIOM, dan MOBILedit *Forensic*. Sementara itu, penelitian Riskiyadi (Riskiyadi, 2020), menunjukkan bahwa penggunaan FTK *Image*r dan Autospy memiliki kemampuan untuk mengakuisisi dan menganalisis file yang dihapus permanen maupun file yang tersimpan. Sedangkan penelitian Hafidy (El Hafidy, 2024) melakukan analisis artefak digital pada hyper-v berbasis windows subsystem for android (WSA) berdasarkan ISO/IEC 27037:2012 dan ISO/IEC 27042:2015. Hasil menunjukkan perubahan pada konfigurasi sistem, rekaman aktivitas, dan file data aplikasi setelah instalasi dan pencopotan WSA. Artefak yang ditemukan mencakup *file* konfigurasi baru, perubahan pada *registry*, rekaman penggunaan aplikasi, riwayat penggunaan, rekaman komunikasi, dan file residu aplikasi.

Berdasarkan latar belakang di atas, pada penelitian ini akan dilakukan analisis forensik digital terhadap aplikasi Signal Desktop pada Windows 11

berdasarkan ISO/IEC 27037:2012 dan ISO/IEC 27042:2015 untuk mendapatkan barang bukti digital. Pada penelitian ini akan dilakukan pengujian dengan simulai kejahatan dan skenario pengujian yang memanfaatkan fitur pada Signal Messenger. Hasil dari setiap skenario pengujian akan dianalisis dengan membandingkan data simulasi kejahatan penggunaan Signal Messenger untuk mendapatkan bukti digital. Penelitian ini juga mematuhi kaidah etika forensik digital, di mana semua skenario dilakukan pada perangkat dan akun uji coba yang dibuat khusus untuk kepentingan penelitian, bukan pada data pribadi nyata. Seluruh aktivitas pengujian dilakukan di lingkungan terkontrol tanpa melibatkan pihak ketiga, sehingga tidak menimbulkan pelanggaran privasi. Prinsip *chain of custody* diterapkan dengan mendokumentasikan setiap tahapan penanganan barang bukti digital, mulai dari akuisisi, penyimpanan, hingga analisis.

Alasan penelitian ini hanya berfokus pada aplikasi Signal dalam mode Desktop di Windows 11 adalah karena ketiga aspek tersebut memiliki urgensi dan relevansi tinggi dalam konteks keamanan siber saat ini. Pertama, Signal dipilih karena protokol enkripsinya yang dikenal paling kuat (Signal Protocol) dan telah diadopsi oleh berbagai platform lain. Kedua, penelitian difokuskan pada Desktop Mode karena sebagian besar studi terdahulu lebih banyak meneliti Signal pada perangkat seluler, sementara aspek desktop masih relatif terbatas padahal penggunaannya semakin meningkat di lingkungan kerja dan institusi. Ketiga, Windows 11 dipilih karena merupakan sistem operasi terbaru dan paling banyak digunakan pada perangkat desktop/laptop global (Statcounter GlobalStats, 2025).

2. METODOLOGI PENELITIAN

2.1. Objek Penelitian

Penelitian ini menggunakan ISO/IEC 27037:2012 sebagai kerangka kerja dalam penanganan barang bukti dan ISO/IEC 27042:2015 sebagai kerangka kerja dalam analisis bukti digital. Objek penelitian ini adalah aplikasi pengiriman pesan Signal Messenger berbasis *Desktop*. Adapun spesifikasi objek dan perangkat pendukung yang digunakan pada penelitian ini dapat dilihat pada Tabel 1.

Tabel 1. Spesifikasi Objek dan Perangkat

No	Objek dan Perangkat	Keterangan
1	Aplikasi Signal Desktop	Versi 7.44.0
2	Laprop ASUS VivoBook A416JP	Windows 11 Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz, 1190 Mhz, 4 Core(s), 8 Logical Processor(s)
3	FTP *Image*r	Versi 4.3.1.1
4	Autopsy	Versi 4.21.0

Berdasarkan Tabel 1 objek utama penelitian yaitu aplikasi Signal Desktop. Perangkat laptop Asus VivoBook A416JP digunakan untuk menjalankan alat forensik yang sudah ditentukan. Alat forensik yang digunakan pada penelitian ini adalah FTK *Image*r, Autopsy.

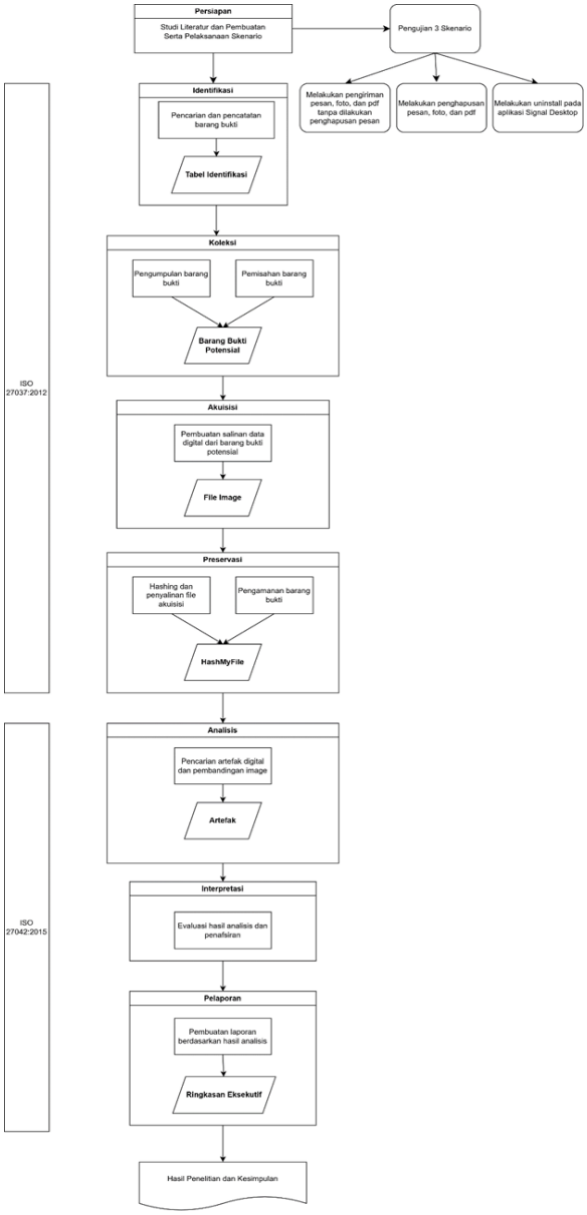
Pemilihan Signal Desktop sebagai objek penelitian didasarkan pada pertimbangan bahwa sebagian besar penelitian sebelumnya menitikberatkan pada perangkat mobile, sedangkan penggunaan aplikasi perpesanan di lingkungan desktop semakin umum dalam konteks organisasi maupun individu. Sementara itu, pemilihan Windows 11 didasarkan pada dominasi penggunaannya sebagai sistem operasi desktop terbaru dan adanya perbedaan arsitektur dibandingkan dengan versi sebelumnya, sehingga potensi artefak digital yang dihasilkan juga berbeda. Perubahan artefak *registry* dan event log di Windows 11 dibandingkan Windows 10 menunjukkan bahwa analisis platform terbaru dapat menghadirkan artefak berbeda (Medium, 2024). Dengan demikian, ruang lingkup penelitian ini secara sadar dibatasi pada Signal Desktop di Windows 11 untuk memperoleh hasil yang fokus, mendalam, serta dapat memberikan kontribusi ilmiah terhadap area yang masih kurang dieksplorasi.

2.2. Desain dan Metode Penelitian

Penelitian ini dilakukan berdasarkan beberapa tahapan yang mengacu pada standar ISO/IEC 27037:2012 (ISO/IEC, 2012) dan ISO/IEC 27042:2015 (ISO/IEC, 2015), yaitu tahapan identifikasi, pengumpulan, akuisisi, preservasi, analisis, interpretasi, dan pelaporan. Untuk memastikan integritas bukti digital, studi ini mengikuti kerangka umum forensik digital: akuisisi, analisis, dan pelaporan (Digital forensics, 2025). Standar ISO/IEC 27037:2012 memuat pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital. Tahapannya mencakup:

1. Identifikasi: mengenali dan mendokumentasikan perangkat atau data yang berpotensi sebagai bukti digital.
2. Pengumpulan: memindahkan barang bukti digital dari lokasi temuan ke laboratorium tanpa mengubah isinya.
3. Akuisisi: membuat salinan forensik (imaging) dari media asli untuk menjaga integritas bukti.
4. Preservasi: melindungi integritas dan keaslian data hasil akuisisi agar tetap sah secara hukum.

Sementara itu, standar ISO/IEC 27042:2015 memberikan pedoman analisis, interpretasi, dan pelaporan bukti digital.



Gambar 1. Desain Penelitian

Persiapan penelitian ini diawali dengan tahap persiapan yang mencakup studi literatur, penyiapan kebutuhan, dan penyusunan skenario pengujian.

Studi literatur dilakukan untuk memahami konsep, teori, serta temuan-temuan sebelumnya guna membangun landasan teori yang kokoh dalam menganalisis informasi terkait perangkat, serta metodologi penelitian yang digunakan. Referensi diperoleh dari berbagai sumber seperti jurnal, buku, paper, dan artikel. Landasan teori yang diperlukan dalam penelitian ini meliputi forensik digital, bukti digital, ISO/IEC 27037:2012, ISO/IEC 27042:2015, Signal Desktop, dan alat-alat forensik.

Tahap persiapan kebutuhan bertujuan untuk merancang dan menyiapkan segala kebutuhan yang diperlukan dalam pelaksanaan pengujian, sehingga penelitian dapat membentuk hubungan sebab-akibat terhadap objek yang diteliti. Selanjutnya penyusunan skenario dilakukan untuk mengidentifikasi perubahan artefak yang terjadi pada sistem Windows 11, yang akan digunakan untuk menganalisis jejak digital yang dihasilkan oleh aplikasi Signal Desktop.

Tahap selanjutnya pada penelitian ini adalah pengujian yang mengacu pada standar ISO/IEC 27037:2012 dan ISO/IEC 27042:2015. Secara garis besar, metode ini terdiri dari tujuh tahap yaitu identifikasi, pengumpulan, akuisisi, reservasi, analisis, interpretasi, dan pelaporan.

1. Identifikasi

Tahap identifikasi akan melibatkan proses pencarian, pengenalan, dan dokumentasi semua artefak digital yang berpotensi. Proses identifikasi ini meliputi pencatatan kondisi barang, identitasnya, serta informasi penting yang dapat diperoleh darinya. Hasil identifikasi tersebut kemudian dicatat dalam formulir identifikasi barang bukti.

2. Pengumpulan

Tahap ini mencakup proses pengumpulan barang bukti yang telah diidentifikasi dengan tujuan memindahkannya dari lokasi asli ke laboratorium untuk proses akuisisi. Seluruh proses koleksi harus dilakukan tanpa mengubah data yang tersimpan di perangkat.

3. Akuisisi

Tahapan akuisisi bertujuan untuk membuat salinan data dari Windows 11 yang sudah ter *install* aplikasi Signal. Pada tahap ini, perangkat penyimpanan komputer yang menjadi subjek investigasi akan diambil dan dihubungkan dengan komputer forensik untuk dilakukan proses akuisisi dan analisis lebih lanjut. Akuisisi dilakukan menggunakan FTK *Image*r untuk melakukan imaging data. Hasil imaging kemudian diekstraksi dan dianalisis untuk mengidentifikasi artefak yang ditemukan, seperti database pesan (*Signal.db*), *file cache, registry, event og, prefetch, amcache*, $MFT, dan $J. Hasil analisis kemudian dianalisis secara manual dengan membandingkan artefak yang ditemukan dari beberapa skenario yang telah dilakukan.

4. Preservasi

Tahapan Preservasi bertujuan untuk menjaga kelangsungan integritas dan keaslian data yang telah diperoleh. Data hasil akuisisi disimpan dalam ruang penyimpanan yang terisolasi atau dikhususkan untuk melindungi barang bukti digital. Sementara itu, barang bukti fisik juga disimpan di tempat khusus yang aman dan dijaga agar tidak diakses oleh pihak-pihak yang tidak berkepentingan.

5. Analisis

Tahap Analisis mencakup pemeriksaan barang bukti yang telah dikumpulkan untuk memperoleh pemahaman mendalam mengenai bukti digital yang ditemukan. Tujuannya adalah menghasilkan informasi yang dapat mendukung investigasi atau proses hukum yang sedang berlangsung.

6. Interpretasi

Tahap Interpretasi adalah proses penting setelah analisis bukti digital, yang melibatkan evaluasi

mendalam terhadap data yang telah dikumpulkan serta analisisnya dalam konteks situasi yang relevan. Data tersebut dikaji dan ditafsirkan untuk mengidentifikasi fakta-fakta yang signifikan, serta, dalam beberapa kasus, dilengkapi dengan opini yang relevan untuk menyempurnakan temuan.

7. Pelaporan

Tahap Pelaporan menyajikan hasil dari setiap analisis skenario yang telah dilakukan. Informasi terkait proses forensik dan data yang terdapat pada perangkat disampaikan dalam tahap ini. Laporan juga mencakup ringkasan bukti digital yang berhasil ditemukan.

2.3. Skenario Penelitian

Penelitian ini menerapkan pendekatan kualitatif yang berfokus pada pemahaman kejadian melalui kasus tertentu. Hasil dari objek penelitian akan dijelaskan secara deskriptif sesuai dengan skenario yang telah ditetapkan.

Tabel 2. Skenario Kasus

Skenario	Perlakuan
Skenario 1	Melakukan pengiriman 5 pesan, foto dan pdf tanpa dilakukan penghapusan pesan
Skenario 2	Melakukan penghapusan pesan, foto, dan pdf yang dikirimkan
Skenario 3	Melakukan *uninstall* pada aplikasi Signal Desktop

2.4. Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh aktivitas komunikasi digital yang dilakukan melalui aplikasi Signal Desktop pada sistem operasi Windows 11. Dari populasi tersebut, penelitian ini mengambil sampel berupa tiga skenario penggunaan yang telah dirancang, yaitu: (1) penggunaan normal tanpa penghapusan pesan atau file, (2) penghapusan pesan, foto, dan dokumen PDF, serta (3) proses *uninstall* aplikasi.

2.5. Validitas dan Reliabilitas Data

Validitas data dalam penelitian forensik digital ini dijaga dengan mengikuti standar internasional ISO/IEC 27037:2012 dan ISO/IEC 27042:2015 yang memberikan pedoman identifikasi, akuisisi, preservasi, analisis, dan interpretasi bukti digital. Proses akuisisi dilakukan dengan FTK Imager menggunakan metode bitstream imaging sehingga menghasilkan salinan yang identik dengan media asli. Untuk memastikan reliabilitas, setiap file hasil akuisisi diverifikasi menggunakan nilai hash MD5 dan SHA1. Kesesuaian hash antara data asli dan salinan menunjukkan bahwa tidak ada perubahan yang terjadi selama proses akuisisi dan analisis. Selain itu, proses analisis dilakukan dengan Autopsy yang menghasilkan laporan terstruktur sehingga dapat diulang (reproducible) oleh peneliti lain dengan kondisi serupa.

3. HASIL DAN PEMBAHASAN

3.1. Perbandingan Penelitian Terkait

Pada penelitian ini menunjukkan bahwa artefak digital pada aplikasi Signal Desktop di Windows 11 dapat ditemukan dan dianalisis menggunakan metodologi forensik digital berbasis ISO/IEC 27037:2012 dan ISO/IEC 27042:2015. Hasil ini sejalan sekaligus melengkapi temuan dari penelitian sebelumnya.

Riadi, Herman, dan Imam (2022) membuktikan bahwa metode forensik berbasis NIST mampu mengekstraksi riwayat percakapan, gambar, GIF, dokumen PDF, video, serta catatan panggilan pada Signal Messenger berbasis Android. Penelitian tersebut berfokus pada perangkat seluler dengan kondisi rooted, sehingga artefak dapat diakses secara penuh. Sebaliknya, penelitian ini menekankan analisis pada aplikasi Signal Desktop di Windows 11 tanpa kondisi root, sehingga lebih relevan untuk perangkat desktop.

Irawan dan Riadi (2022) menggunakan alat forensik seperti Belkasoft Evidence Center, Magnet AXIOM, dan MOBILedit Forensic untuk mengekstraksi artefak dari perangkat seluler. Penelitian ini memperlihatkan variasi alat bantu, sedangkan penelitian kami membatasi pada penggunaan FTK Imager untuk akuisisi dan Autopsy untuk analisis. Perbedaan ini menunjukkan bahwa meskipun alat yang digunakan berbeda, hasil yang diperoleh tetap konsisten: artefak digital dapat ditemukan selama tidak dihapus secara permanen.

Penelitian Riskiyadi (2020) menekankan kemampuan FTK Imager dan Autopsy untuk menganalisis file yang dihapus. Hasil penelitian ini memperkuat temuan tersebut, khususnya pada skenario kedua, di mana file gambar, video, dan dokumen PDF yang telah dihapus masih dapat dipulihkan sebagai *deleted files*. Temuan serupa diekspresikan dalam analisis forensik aplikasi desktop AI seperti ChatGPT (Wanniarachchige et al., 2025), memperkuat relevansi metodologi yang digunakan di sini terhadap aplikasi desktop modern.

Selanjutnya, penelitian El Hafidy (2024) mengenai Windows Subsystem for Android (WSA) menyoroti perubahan pada konfigurasi sistem, *registry*, serta rekaman aktivitas. Penelitian kami menemukan kesamaan pola, yakni adanya artefak residu setelah penggunaan aplikasi. Namun, berbeda dengan WSA yang masih meninggalkan jejak meskipun sudah dihapus, pada penelitian ini skenario *uninstall* pada Signal Desktop menghasilkan pembersihan artefak yang hampir menyeluruh.

Secara keseluruhan, penelitian ini memperluas cakupan studi forensik pada aplikasi Signal dengan fokus pada platform desktop terbaru, Windows 11. Dibandingkan penelitian terdahulu yang dominan pada perangkat seluler atau subsistem Android, penelitian ini memberikan kontribusi baru berupa bukti bahwa standar ISO/IEC 27037:2012 dan ISO/IEC 27042:2015 dapat diterapkan secara efektif pada analisis forensik aplikasi Signal Desktop.

3.2. Pembuatan Skenario

1. Skenario 1

Pada skenario pertama, dilakukan pengiriman pesan, foto, dan dokumen PDF melalui aplikasi Signal Desktop pada Windows 11 tanpa melakukan penghapusan pesan. Analisis dilakukan untuk mengidentifikasi lokasi penyimpanan data aplikasi dalam sistem *file* Windows 11 dan memastikan apakah data tersebut dapat diakses menggunakan teknik forensik digital.

2. Skenario 2

Pada skenario kedua, dilakukan pengiriman pesan, foto, dan dokumen PDF melalui aplikasi Signal Desktop pada Windows 11 dengan melakukan penghapusan pesan. Tujuan dari pengujian skenario ini adalah untuk menganalisis perubahan yang terjadi pada artefak digital setelah pengguna menghapus pesan secara manual.

3. Skenario 3

Pada skenario ketiga, dilakukan pengiriman pesan, foto, dan dokumen PDF melalui aplikasi Signal Desktop pada Windows 11 dan melakukan *uninstall* aplikasi signal. Tujuan dari pengujian skenario ini adalah untuk menganalisis jejak digital yang masih tersisa setelah aplikasi Signal Desktop dihapus dari perangkat. Pengujian ini akan melihat apakah artefak seperti pesan, foto, dan dokumen PDF tetap ada dalam sistem atau benar-benar terhapus secara permanen.

3.3. Pelaksanaan Skenario

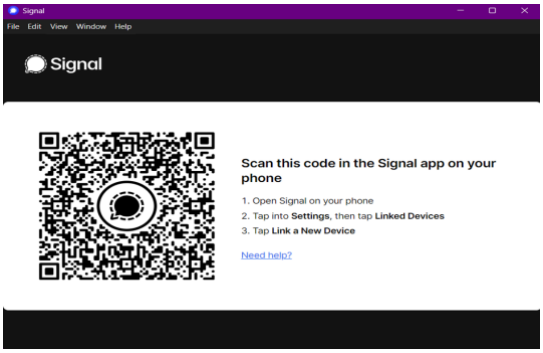
Pelaksanaan pengujian dilakukan di Indonesia dengan menggunakan aplikasi Signal Desktop pada sistem operasi Windows 11. Setiap skenario dijalankan pada perangkat dengan spesifikasi yang tercantum dalam Tabel 3.

Tabel 3. Deskripsi Barang Bukti

Atribut	Deskripsi
Hostname	Pengguna1
System Model	VivoBook_ASUSLaptop X415JP_A416JP
Processor	Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz, 1190 Mhz, 4 Core(s), 8 Logical Processor(s)
RAM	16.0 GB (15.7 GB usable)
Architecture	64-bit operating system, x64-based processor
OS Name Version	Microsoft Windows 11 Pro 10.0.26100 Build 26100
BIOS Version/Date	American Megatrends Inc. X415JP.303, 03/06/2021

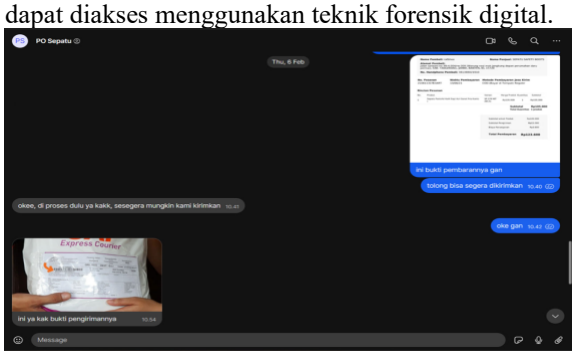
1. Skenario 1

Skenario dimulai dengan instalasi aplikasi Signal Desktop pada sistem operasi Windows 11. Pemasangan aplikasi dilakukan seperti instalasi perangkat lunak pada umumnya, mengikuti prosedur standar yang ditetapkan oleh pengembang aplikasi. Setelah instalasi selesai, konfigurasi awal dilakukan dengan menghubungkan Signal Desktop ke akun pengguna melalui proses pemindaian kode QR menggunakan aplikasi Signal pada perangkat seluler.

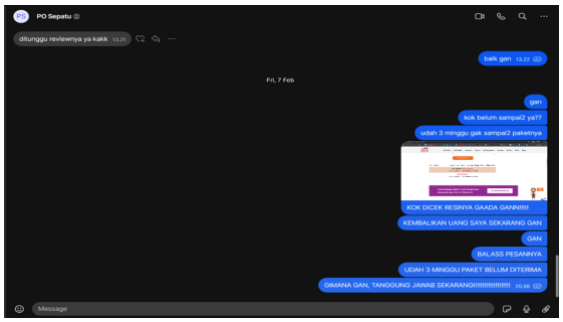


Gambar 2. Halaman Awal Aplikasi Signal Desktop

Setelah aplikasi siap digunakan, dilakukan pengiriman pesan, foto, dan dokumen PDF melalui Signal Desktop tanpa melakukan penghapusan pesan. Analisis dilakukan untuk mengidentifikasi lokasi penyimpanan data aplikasi dalam sistem *file* Windows 11 dan memastikan apakah data tersebut dapat diakses menggunakan teknik forensik digital.



Gambar 3. Bukti Chatting



Gambar 4. Bukti Chatting

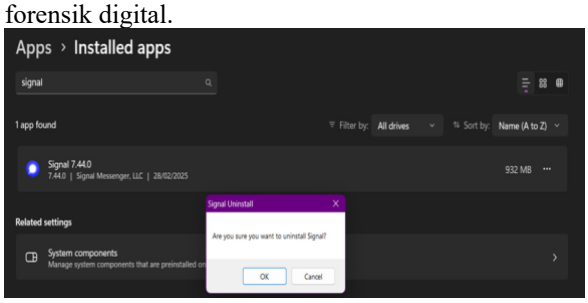
2. Skenario 2

Pada skenario kedua, setelah aplikasi Signal Desktop berhasil diinstal dan dikonfigurasi, dilakukan pengiriman pesan, foto, dan dokumen PDF seperti pada skenario pertama. Namun, dalam skenario ini, pengguna secara aktif menghapus pesan yang telah dikirim dan diterima dari dalam aplikasi Signal Desktop. Analisis dilakukan untuk melihat perubahan yang terjadi pada artefak digital setelah pengguna menghapus pesan secara manual, serta apakah data yang telah dihapus masih dapat dipulihkan menggunakan teknik forensik digital atau benar-benar hilang dari sistem.

Gambar 5. Penghapusan Pesan

3. Skenario 3

Pada skenario ketiga, setelah proses pengiriman pesan, foto, dan dokumen PDF melalui aplikasi Signal Desktop selesai dilakukan, aplikasi kemudian dihapus (*uninstall*) dari sistem operasi Windows 11. Pengujian dilakukan untuk melihat apakah artefak seperti pesan, foto, dan dokumen PDF tetap ada dalam sistem atau benar-benar terhapus secara permanen. Selain itu, analisis juga dilakukan terhadap kemungkinan pemulihan data menggunakan teknik forensik digital.



Gambar 6. Proses *Uninstall* Aplikasi

3.4. Pengujian

1. Identifikasi

Tahapan pertama setelah pelaksanaan skenario adalah pelaksanaan proses identifikasi. Pada tahapan ini dilakukan pencarian, pengenalan, dan dokumentasi bukti digital yang dapat diperoleh berkaitan dengan penggunaan aplikasi Signal Desktop serta memiliki potensi sebagai barang bukti digital.

Pada tahapan ini ditemukan barang bukti berupa satu perangkat laptop yang digunakan oleh pengguna dengan aplikasi Signal Desktop terinstal. Perangkat tersebut ditemukan dalam kondisi perangkat tidak aktif dan tidak menyambung ke perangkat lain. Identifikasi dilakukan terhadap sistem operasi, file sistem, serta artefak digital yang terkait dengan aktivitas aplikasi Signal Desktop. Hasil identifikasi terhadap perangkat tersebut dapat dilihat pada Tabel 4.

Tabel 4. Hasil Identifikasi Perangkat

Atribut	Deskripsi
Merek dan Model	ASUS VivoBook A416JP
Nomor Seri Warna	VIPS556
Ukuran Layar Kondisi Fisik	14 inci Layar utuh tanpa gores
Port dan Slot	3x USB 3.0 1x USB-C HDMI
Indikator Daya Kondisi Baterai	Tidak ada lampu indikator daya saat ditemukan
Catu Daya Eksternal	Tidak ada lampu indikator daya saat ditemukan
Media Penyimpanan	Tidak ada media penyimpanan yang terpasang
Kunci atau Kunci USB	Tidak ada kunci atau kunci USB yang terpasang
Striker Lisensi/Sertifikasi	Tidak ada stiker lisensi
Tanda-tanda Penggunaan	Terdapat sidik jari dan noda kecil di sekitar keyboard dan trackpad
Striker Garansi/Perbaikan	Tidak ada stiker garansi
Lokasi dan Konteks Penemuan	Laptop ditemukan di meja kerja kantor

2. Koleksi

Tahapan kedua setelah melakukan identifikasi adalah mengumpulkan barang bukti yang berkaitan dengan aplikasi Signal Desktop. Barang bukti yang sudah diidentifikasi selanjutnya dipindahkan ke laboratorium analisis untuk dilakukan proses akuisisi.

Pada penelitian ini, perangkat komputer yang telah terinstal aplikasi Signal Desktop dipindahkan dari lokasi aslinya menuju tempat analisis barang bukti. Pemindahan ini harus dilakukan tanpa mengubah data yang ada pada perangkat. Dalam kasus ini, karena perangkat dalam kondisi mati dan tidak terhubung ke jaringan internet, maka pemindahan dapat dilakukan tanpa menggunakan faraday bag. Pada Gambar 3.6 ditunjukkan proses koleksi yang dilakukan dalam penelitian ini.

Gambar 7. Barang Bukti

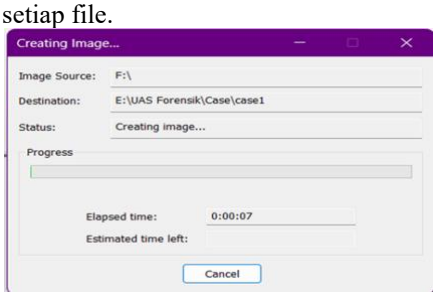
Pada proses koleksi ini juga dilakukan pemisahan barang bukti yang berpotensi mengandung data forensik terkait aplikasi Signal Desktop dari barang bukti lain yang tidak relevan. Barang bukti potensial yang telah dipilih kemudian diputus dari sumber daya listrik, diberi label sesuai dengan kondisinya, dan dipindahkan ke laboratorium untuk proses akuisisi lebih lanjut. Media penyimpanan dari perangkat menjadi barang bukti utama yang memiliki potensi informasi tinggi. Dalam penelitian ini, dilakukan pemisahan media penyimpanan berupa SSD, yang nantinya akan diakuisisi datanya untuk menganalisis artefak yang tersimpan dari aplikasi Signal Desktop.

3. Akuisisi

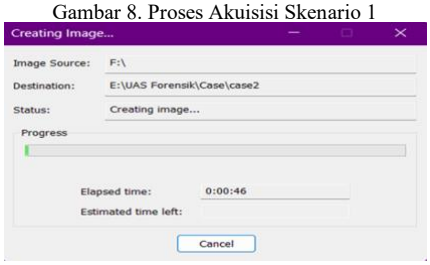
Tahapan selanjutnya adalah akuisisi, yaitu pembuatan salinan data dari sistem yang sudah teridentifikasi, yaitu komputer dengan aplikasi Signal Desktop yang telah digunakan dalam skenario penelitian.

Proses akuisisi ini dilakukan dengan mengambil data dari sistem penyimpanan komputer yang menjadi subjek investigasi dan menghubungkannya dengan komputer forensik. Akuisisi dilakukan menggunakan FTK *Image*r untuk melakukan imaging

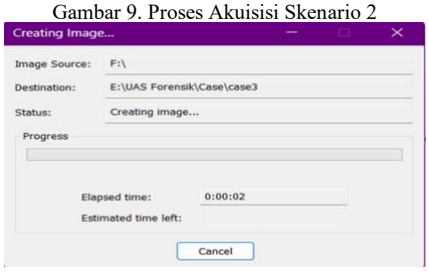
data. Proses ini dilakukan dengan membuat *image* secara *physical* dengan format E01 seperti yang ditampilkan berturut-turut pada Gambar. Format ini memuat salinan bitstream fisik yang disimpan dalam satu atau beberapa file yang dilengkapi dengan metadata, termasuk informasi kasus, nama pemeriksa, catatan, checksum, dan *hash* MD5. Keunggulan utamanya terletak pada kemampuan kompresi, perlindungan sandi, dan adanya checksum untuk setiap file.



Gambar 8. Proses Akuisisi Skenario 1



Gambar 9. Proses Akuisisi Skenario 2



Gambar 10. Proses Akuisisi Skenario 3

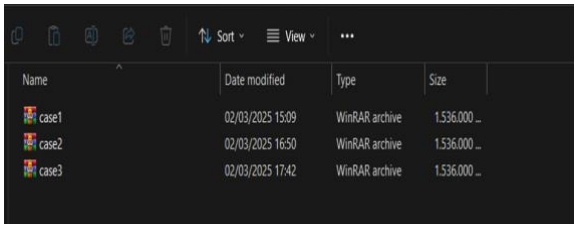
Data hasil akuisisi dapat dilihat pada Tabel 5

Tabel 5. Data Hasil Akuisisi

Skenario	Nama file	Ukuran Akuisisi	Ukuran Asli	Mulai	Selesai
1	Case1	1.53 GB	10 GB	2 Mar 2025 14:53:43	2 Mar 2025 15:09:23
2	Case2	1.53 GB	10 GB	2 Mar 2025 16:31:32	2 Mar 2025 16:50:02
3	Case3	1.53 GB	10 GB	2 Mar 2025 17:23:13	2 Mar 2025 17:42:31

4. Preservasi

Pada tahap preservasi, bukti digital yang diperoleh dari aplikasi Signal Desktop diamankan untuk memastikan integritas dan keaslian informasi yang terkandung di dalamnya. Bukti fisik, seperti perangkat yang digunakan dalam pengujian, disimpan dengan akses terbatas untuk mencegah modifikasi atau gangguan yang tidak sah.



Gambar 11. Bukti Digital

Untuk bukti digital, setelah dilakukan akuisisi data dari sistem yang menjalankan Signal Desktop, langkah selanjutnya adalah melakukan *hash*ing terhadap file hasil akuisisi guna memastikan integritasnya. Pada penelitian ini, penghitungan nilai *hash* dilakukan menggunakan alat *Hash*My*files*.

Tabel 6. Data Hasil Akuisisi

Skenario	Direktori	Nilai hash SHA1	Nilai Hash MD5
1	E:\Forensik\Case\case1.001	file Asli 0c74c52fbd9a5320c2dbba45cf9fdb29	3bcc9d9cb99ccbf39e3e6c7c7b569a959d9354ee
	E:\Forensik\Case\case1.001	file Salinan 0c74c52fbd9a5320c2dbba45cf9fdb29	3bcc9d9cb99ccbf39e3e6c7c7b569a959d9354ee
2	E:\Forensik\Case\case1.002	file Asli f571dc7256250189ab093a07731c9420	d97649482159f76d7eb390d0eda72d082122b09a
	E:\Forensik\Case\case1.002	file Salinan f571dc7256250189ab093a07731c9420	d97649482159f76d7eb390d0eda72d082122b09a
3	E:\Forensik\Case\case1.003	file Asli 463a68fb3eefad639693994e93f1e394	d97649482159f76d7eb390d0eda72d082122b09a
	E:\Forensik\Case\case1.003	file Salinan 463a68fb3eefad639693994e93f1e394	d97649482159f76d7eb390d0eda72d082122b09a

Setelah penghitungan *hash* selesai, dilakukan proses kloning atau pembuatan salinan dari file akuisisi. Proses kloning ini bertujuan untuk menjaga integritas data asli selama proses investigasi, dengan memastikan bahwa analisis forensik hanya dilakukan pada salinan, bukan pada data asli. Hal ini penting untuk meminimalkan risiko perubahan atau kerusakan bukti digital yang dapat memengaruhi validitas hasil investigasi.

Selain itu, proses kloning mendukung prinsip *chain of custody* dan forensik yang dapat dipertanggungjawabkan, dengan memastikan bahwa data asli tetap utuh dan tidak terpengaruh selama proses investigasi. Setelah salinan dibuat, dilakukan verifikasi integritas dengan mencocokkan nilai *hash* antara file asli dan salinannya. Jika nilai *hash* keduanya sama, maka dapat dipastikan bahwa salinan benar-benar identik dengan data asli, dan tidak ada perubahan yang terjadi selama proses kloning. Pembuatan salinan dan nilai *hash* dapat dilihat pada Tabel 5.

5. Analisis

Barang bukti berupa *image* selanjutnya akan dianalisis menggunakan alat bantu Autopsy. Hasil

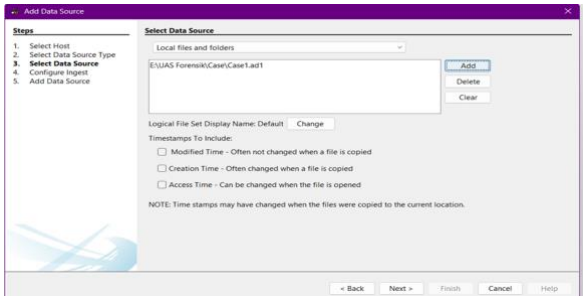
image pada tahap akuisisi akan digunakan sebagai input sumber data untuk proses analisis. Proses ini bertujuan untuk menemukan keterkaitan antara penemuan dengan hipotesis yang telah dibuat dari hasil akuisisi guna mendapatkan informasi yang lebih rinci terkait aktivitas pengguna dalam aplikasi Signal Desktop.

a. Hasil Eksperimen Skenario 1

Pada skenario 1 dilakukan analisis menggunakan alat Autopsy, dengan menggunakan barang bukti berupa *image* sebagai inputan. Hasilnya dapat dilihat pada Tabel 6 berikut.

Tabel 6. Hasil Akuisisi pada Skenario 1

Variabel	Data digunakan (item)	Data yang didapatkan	
Teks	31	0	0%
Video	4	4	100%
Gambar	8	8	100%
file PDF	7	7	100%
Total	20	20	100%



Gambar 12. Proses Akuisisi dengan *Autopsy*

Hasil analisis menggunakan autopsy ditemukan terdapat 107 gambar dengan terdapat 8 gambar yang digunakan dalam skenario percakapan. Selain itu juga terdapat 4 gambar yang tersimpan.

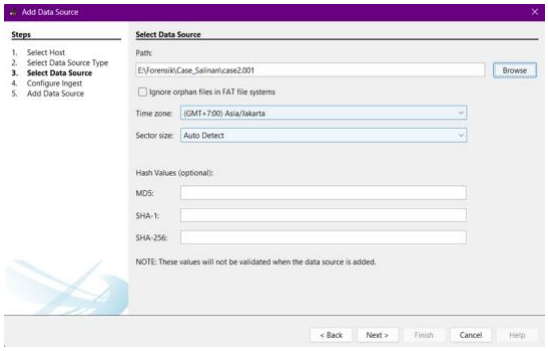
Semua data yang digunakan dalam percakapan seperti teks, gambar, video, dan dokumen PDF berhasil diidentifikasi dalam kondisi utuh. Hal ini menunjukkan bahwa selama data belum dihapus atau aplikasi belum di-*uninstall*, artefak digital masih dapat ditemukan dalam sistem.

b. Hasil Eksperimen Skenario 2

Pada skenario 2 akan dilakukan perlakuan yang sama seperti skenario 1. Hasilnya dapat dilihat pada Tabel 7

Tabel 7. Hasil Akuisisi pada Skenario 7

Variabel	**Data digunakan (item)**	**Data yang didapatkan**	
Teks	31	0	0%
Video	4	4 (deleted file)	100%
Gambar	8	8 (deleted file)	100%
file PDF	7	7 (deleted file)	100%
Total	20	20 (deleted file)	100%



Gambar 13. Proses Akuisisi Skenario 2

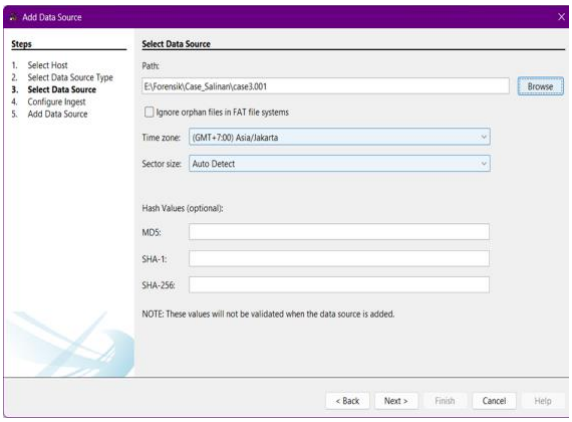
Data yang telah dihapus masih dapat dipulihkan dengan menggunakan metode forensik digital. file seperti gambar, video, dan dokumen PDF yang dihapus masih tersedia dalam bentuk *deleted files*, yang menunjukkan bahwa penghapusan dalam aplikasi Signal tidak sepenuhnya menghilangkan data dari sistem. Namun, teks pesan tidak dapat dipulihkan, hal ini dimungkinkan karena mekanisme penghapusan yang lebih ketat untuk jenis data ini.

c. Hasil Eksperimen Skenario 3

Pada skenario 3 akan dilakukan perlakuan yang sama seperti skenario 1 dan 2. Hasilnya dapat dilihat pada Tabel 8

Tabel 8. Hasil Akuisisi pada Skenario 1

Variabel	Data digunakan (item)	Data yang didapatkan	
Teks	31	0	0%
Video	4	0	0%
Gambar	8	0	0%
file PDF	7	0	0%
Total	20	0	0%



Gambar 18. Proses Akuisisi Skenario 3

Pada pengujian skenario 3, tidak ditemukan artefak digital yang tersisa setelah aplikasi Signal dihapus dari sistem. *Uninstall* aplikasi menghapus hampir semua jejak aktivitas aplikasi dari sistem, sehingga sulit untuk mendapatkan kembali data tanpa metode pemulihan tingkat lanjut.

6. Interpretasi

Investigasi terhadap Signal Desktop pada Windows 11 menunjukkan bahwa keberadaan artefak digital sangat bergantung pada skenario pengujian. Pada skenario 1, semua artefak (teks, gambar, video, dan dokumen PDF) dapat diperoleh utuh selama tidak ada penghapusan. Pada skenario 2, meskipun pesan dan file dihapus, artefak masih ditemukan dalam

bentuk deleted files yang dapat dipulihkan dan dibuka kembali, menandakan metode penghapusan standar tidak sepenuhnya menghilangkan data. Sebaliknya, pada skenario 3, setelah aplikasi di-uninstall, artefak digital tidak lagi ditemukan dengan teknik forensik yang digunakan.

Secara keseluruhan, hasil ini menegaskan bahwa proses forensik digital pada Signal Desktop efektif selama data belum dihapus permanen atau aplikasi belum dicopot. Untuk kasus uninstall, dibutuhkan metode pemulihan lanjutan guna mengekstraksi bukti digital yang mungkin masih tersembunyi.

7. Reporting

Pada penelitian ini, dokumen laporan diawali dengan deskripsi kasus yang dirincikan dengan skenario yang diterapkan. Dengan demikian, skenario 1 merupakan kasus 01, skenario 2 adalah kasus 02, dan skenario 3 merupakan kasus 03. Selanjutnya setiap kasus akan dijelaskan dan didokumentasi setiap tahapannya. Bukti digital yang ditemukan setiap skenarionya akan disusun dan diurutkan dengan urutan kejadian sehingga dapat membentuk urutan kejadian yang dapat ditarik kesimpulan setiap kasusnya. Berikut merupakan hasil bukti digital yang ditemukan dari setiap skenario yang dijalankan disusun pada Tabel 9

Tabel 9. Laporan Hasil

No	Bukti	Skenario 1	Skenario 2	Skenario 3
1	Teks Chat	0	0	0
2	Video	4	4	0
3	Gambar	8	8	0
4	file PDF	7	7	0

4. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengidentifikasi artefak digital dari aktivitas Signal Desktop pada Windows 11, seperti teks, gambar, video, dan file PDF. Artefak yang dihapus masih dapat dipulihkan dalam kondisi tertentu, sedangkan setelah aplikasi di-uninstall sebagian besar artefak tidak lagi ditemukan. Dengan mengacu pada standar ISO/IEC 27037:2012 dan ISO/IEC 27042:2015, penelitian membuktikan bahwa metodologi forensik digital mampu mengumpulkan dan menganalisis bukti secara sistematis untuk mendukung investigasi kejahatan digital.

Saran untuk penelitian selanjutnya yaitu dengan mengembangkan metode pemulihan lanjutan pasca-uninstall, memperluas kajian ke sistem operasi lain, serta menggunakan skala data yang lebih besar agar hasil lebih komprehensif dan aplikatif.

DAFTAR PUSTAKA

Statcounter GlobalStats, 2025. *Desktop Operating System Market Share Worldwide*. [online] Available at: https://gs.statcounter.com/os-market-share/desktop/worldwide [Accessed 1 Mar. 2025].

Irawan, T. and Riadi, I., 2022. Mobile *Forensic* Signal Instant Messenger Services in Case of Web Phishing using National Institute of Standards and Technology Method. *International Journal of Computer Applications*, 184(32), pp.30–40. doi:10.5120/ijca2022922394.

Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L. and Stebila, D., 2020. A Formal Security *Analysis* of the Signal Messaging *Protocol*. *Journal of Cryptology*, 33(4), pp.1914–1983. doi:10.1007/s00145-020-09360-1.

Bestari, N.P., 2025. *Pengguna Aplikasi Signal Cek HP Sekarang, Atau Bermasalah!*. [online] CNBC Indonesia. Available at: https://shorturl.at/dSEpN [Accessed 1 Mar. 2025].

Faruq, A.M., Andri, S.M. and Yudi, P., 2020. Clustering Storage Method for Digital Evidence Storage Using Software Defined Storage. *IOP Conference Series: Materials Science and Engineering*, 722(1), p.012063. doi:10.1088/1757-899X/722/1/012063.

Subektiningsih, 2016. *Bukti Digital Definisi Bukti Digital dan Contoh Kasus (Witness, Tools, Victim, Accomplice, Guardian)*. [repository] [Accessed 1 Mar. 2025].

Sunardi, Riadi, I. and Akbar, M.H., 2020. Penerapan Metode Static *Forensic*s untuk Ekstraksi file Steganografi pada Bukti Digital Menggunakan Framework DFRWS. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 4(3), pp.576–583.

Prayogo, A.G. and Riadi, I., 2022. Digital *Forensic* Signal Instant Messages Services in Case of Cyberbullying using Digital *Forensic* Research Workshop Method. *International Journal of Computer Applications*, 184(32), pp.21–29. doi:10.5120/ijca2022922393.

Valjarevic, A. and Venter, H., 2013. A Harmonized Process Model for Digital *Forensic* Investigation Readiness. *IFIP Advances in Information and Communication Technology*, 410, pp.67–82. doi:10.1007/978-3-642-41148-9_5.

Montasari, R., 2016. A comprehensive digital *forensic* investigation process model. *International Journal of Electronic Security and Digital Forensics*, 8(4), pp.285–302. doi:10.1504/IJESDF.2016.079430.

Paulino, G., 2025. Extracting digital evidence from Signal Desktop for Windows. Forensic Science International: Digital Investigation, 46, p.301783. doi:10.1016/j.fsidi.2025.301783.

Riadi, I., Herman and Imam, N.H.S., 2022. Forensik Mobile Pada Kasus Cyber Fraud Layanan Signal Messenger Menggunakan Metode

NIST. *Jurnal Informasi Teknologi dan Ilmu Komputer*, 3(28), pp.137–144.

Wanniarachchige, M.W.K., et al., 2025. Digital Forensic Investigation of the ChatGPT Windows Application. arXiv preprint. [online] Available at: https://arxiv.org/abs/2505.23938 [Accessed 23 Aug. 2025].

Onik, M.M.H., 2025. A Systematic Literature Review of Secure Instant Messaging Forensics. Proceedings of the ACM on Asia Conference on Computer and Communications Security, pp.1–15. doi:10.1145/3727641.

Cyber Engage, 2024. Forensic Differences Between Windows 10 and Windows 11. Medium. [online] Available at: https://medium.com/%40cyberengage.org/forensic-differences-between-windows-10-and-windows-11-be7bc22a2639 [Accessed 23 Aug. 2025].

Riskiyadi, M., 2020. Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime. *Cyber Security dan Forensik Digital*, 3(2), pp.12–21. doi:10.14421/csecurity.2020.3.2.2144.

El Hafidy, A., 2024. *Analisis Artefak Digital pada Hyper-V berbasis Windows Subsystem for Android (WSA) berdasarkan ISO/IEC 27037:2012 dan ISO/IEC 27042:2015*. [repository] [Accessed 1 Mar. 2025].

Wikipedia, 2025. Digital forensics. [online] Available at: https://en.wikipedia.org/wiki/Digital_forensics [Accessed 23 Aug. 2025].

ISO/IEC, 2012. *Information technology — Security techniques — Guidelines for identification, collection, acquisition*. ISO/IEC 27037:2012.

ISO/IEC, 2015. *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*. ISO/IEC 27042:2015.