JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783

Analisis Bukti Digital Aplikasi Pesan Terenkripsi Signal Dekstop pada Windows 11 Menggunakan Metode IDFIF v2

Grace Friscilla Margaretha Karo-Karo[1*], Muhammad Hilal[1], Dimas Wahyu Utomo[1]

[1]Fakultas Keamanan Siber, Program Studi Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, Bogor, Indonesia
Email: [1*]grace.friscilla@student.poltekssn.ac.id, [2]muhammad.hilal@student.poltekssn.ac.id, [3]dimas.wahyu@student.poltekssn.ac.id

Abstrak− Aplikasi pesan Signal dikenal dengan tingkat keamanan dan enkripsi yang kuat. Namun, karakteristik ini dapat dimanfaatkan oleh pelaku kejahatan untuk menghapus jejak digital dari perangkat yang digunakan, terutama pada platform Windows. Penelitian ini bertujuan untuk melakukan analisis forensik terhadap bukti digital yang dihasilkan oleh aplikasi Signal Desktop pada platform Windows 11 dengan menerapkan metode IDFIF v2 yang menggunakan Access Data FTK Imager dan Autopsy sebagai alat bantu forensik. Pada penelitian ini, analisis forensik dilakukan terhadap aplikasi Signal Desktop berdasarkan tiga skenario yang telah ditentukan. Hasil penelitian menunjukkan bahwa tindakan penghapusan data pada aplikasi dan proses *uninstall* pada aplikasi berdampak pada hasil artefak digital yang diperoleh.

Kata Kunci: Bukti Digital; Forensik Komputer; Signal Desktop; Windows 11; IDFIF v2

Abstract− The Signal messaging application is renowned for its high level of security and strong encryption. However, these features can be exploited by perpetrators to erase digital traces from the utilized device, particularly on the Windows platform. This research aims to conduct forensic analysis on the digital evidence generated by the Signal Desktop application on Windows 11, utilizing the IDFIF v2 method that adopts Access Data FTK Imager and Autopsy as forensic tools. In this study, forensic analysis is carried out on the Signal Desktop application based on three predetermined scenarios. The research findings indicate that data deletion within the application and the uninstallation process significantly influence the results of obtained digital artifacts.

Keywords: Digital Evidence; Computer Forensics; Signal Desktop; Windows 11; IDFIF v2

1. PENDAHULUAN

Forensik digital merupakan suatu cabang ilmu forensik yang berfokus pada pemulihan, investigasi, pemeriksaan, dan analisis materi yang ditemukan dalam perangkat digital, khususnya terkait dengan kejahatan komputer dan perangkat mobile. Aplikasi chat yang dianggap aman seperti WhatsApp, Skype, dan Telegram menjadi fokus forensik digital karena data dalam aplikasi tersebut sering kali mengalami penguncian, penghapusan, atau penyembunyian (Wikipedia, 2023). Aplikasi-aplikasi tersebut menjadi sumber bukti yang signifikan bagi pemeriksa forensik, terutama di era keterhubungan digital saat ini (Uzun et al., 2015). Penelitian ini difokuskan pada aplikasi Signal Desktop yang beroperasi pada sistem operasi Windows 11. Signal dipilih karena merupakan aplikasi pesan instan yang menggunakan enkripsi *end-to-end* yang populer dan dikenal karena fitur keamanannya. Fitur-fitur privasi baru yang diperkenalkan oleh Signal semakin mempersulit identifikasi pengirim (Riadi et al., 2022). Meskipun Signal telah menjadi subjek penelitian, penelitian mengenai forensik pada aplikasi Signal Desktop yang berjalan di sistem operasi Windows masih terbatas, sementara mayoritas penelitian dilakukan pada platform *mobile* (Riadi et al., 2022) (Prayogo & Riadi, 2022; Riadi & Siregar, 2018).

Penelitian terkait telah dilakukan untuk menganalisis dan memahami bagaimana data diperoleh dari aplikasi *chat* ini. Penelitian oleh (Riadi et al., 2022) menunjukkan bahwa dari ponsel pelaku yang di-*root*, artefak digital berhasil diperoleh menggunakan alat forensik seperti Belkasoft Evidence Center, Magnet AXIOM, dan MOBILedit Forensic. Penelitian lain oleh (Riadi & Siregar, 2018) menunjukkan bahwa artefak pada aplikasi Signal Messenger yang diperoleh melalui proses forensik dengan metode NIST mencangkup data chat, gambar, GIF, dokumen PDF, video, *voice call*, dan *video call*. Penelitian menunjukkan bahwa ditemukan bukti digital sebesar 100% dari gambar, GIF, dokumen PDF, dan video pada *smartphone* yang di-*root*. Temuan penelitian mencakup bukti digital sebesar 100% dari gambar, GIF, dokumen PDF, dan video pada smartphone yang di-root. Identifikasi berhasil dilakukan terhadap riwayat pesan, gambar terkirim dan diterima, lokasi file video di kartu memori, daftar kontak, dan detail panggilan. Penelitian oleh (Ayunita

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783

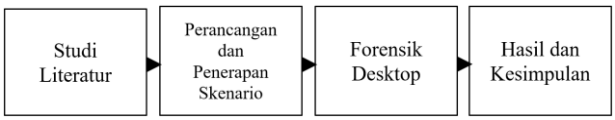
Kinasih et al., 2020) menyatakan bahwa FTK Imager merupakan aplikasi forensik digital yang digunakan dalam penyidikan dengan menerapkan teknik *live*, *static*, atau kombinasi keduanya. Fungsinya mencakup akuisisi data yang melibatkan pengambilan, pengumpulan, dan persiapan data untuk diproses menjadi data yang diinginkan. Autopsy, sebagai alat bantu forensik digital, mendapatkan pengakuan di komunitas forensik digital karena kemampuannya menjaga integritas dan legalitas bukti digital. Keefektifan, produktivitas, efisiensi, keamanan dari kesalahan, dan beban kognitif adalah aspek-aspek yang dinilai dalam mengukur kinerja Autopsy (Domingues et al., 2022). Penelitian oleh (Riskiyadi, 2020) menunjukkan bahwa penggunaan FTK Imager dan Autospy memiliki kemampuan untuk mengakuisisi dan menganalisis file yang dihapus permanen maupun file yang tersimpan.

Meskipun telah dilakukan penelitian pada platform Android, penelitian lebih lanjut diperlukan pada platform lain seperti Windows. Tantangan utama adalah menghadapi enkripsi yang kuat yang diterapkan oleh aplikasi ini. Oleh karena itu, penelitian lebih lanjut diperlukan untuk memahami cara mendapatkan data dari aplikasi ini di bawah enkripsi yang kuat pada sistem operasi Windows.

2. METODE

2.1 Desain Penelitian

Penelitian ini dilakukan berdasarkan beberapa tahapan, yaitu studi literatur, perancangan dan penerapan skenario, forensik desktop yang mengacu pada IDFIF v2, hasil, dan kesimpulan.



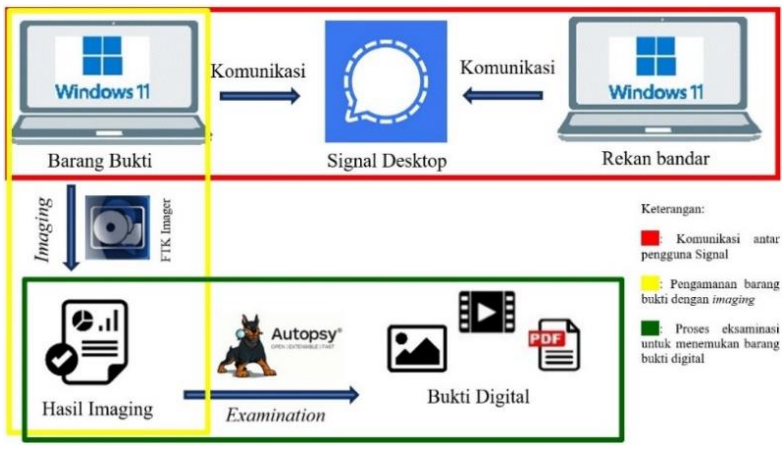
Gambar 1. Desain Penelitian

2.2 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 dalam Tabel 1 dan Gambar 1.

Tabel 1. Skenario Kasus

Skenario 1	Melakukan pengiriman 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.

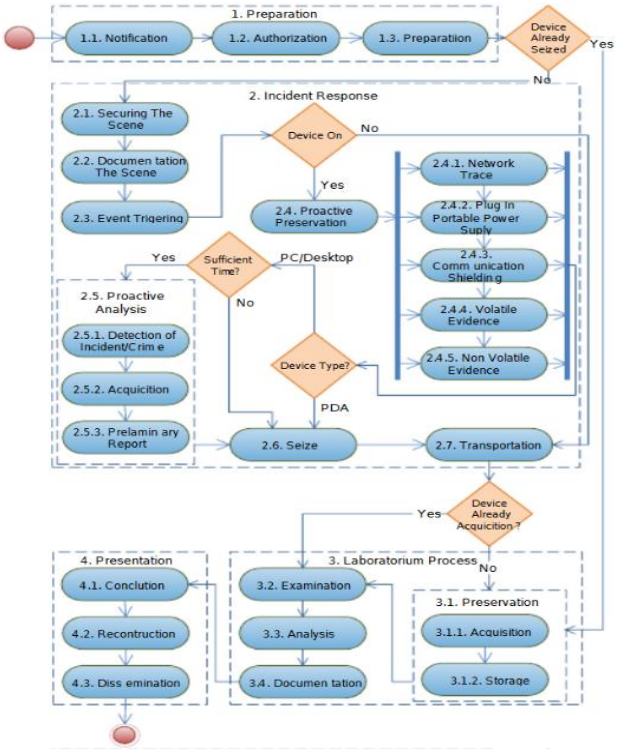


Gambar 2. Tahapan Skenario Penelitian

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783

2.3 Metode Peneitian

Penelitian ini menggunakan metode IDFIF v2, versi terbaru dari IDFIF yang diklaim memiliki tahapan yang lebih fleksibel daripada versi sebelumnya (Ayunita Kinasih et al., 2020). Secara garis besar, metode ini terdiri dari 4 tahap, yaitu *Preparation*, *Incident Response*, *Laboratorium Process*, dan *Presentation*. Rincian setiap tahap dapat dilihat pada Gambar 3.



Gambar 3. Metode IDFIF v2

a. *Preparation*

Tahap awal persiapan investigasi dimulai dari olah tempat kejadian perkara hingga pembuatan laporan (Ruuhwan et al., 2016). Tahap *preparation* dibagi menjadi 3 sub tahapan, yaitu:

1. *Notification*
   Pemberitahuan pelaksanaan investigasi atau melaporkan kejahatan kepada penegak hukum.
2. *Authorization*
   Memperoleh hak akses terhadap barang bukti dan status hukum proses penyelidikan.
3. *Preparation*
   Persiapan yang melibatkan ketersediaan alat, personel, dan kebutuhan penyelidikan.

b. *Incident Response*

Kegiatan yang dilakukan di tempat kejadian untuk mengamankan barang bukti digital agar tidak terkontaminasi (Ruuhwan et al., 2016). Tahap ini terdiri dari 7 subtahap, yaitu

1. *Securing The Scene*
   Mekanisme untuk mengamankan tempat kejadian dan melindungi integritas barang bukti.
2. *Documentation The Scene*
   Pengolahan tempat kejadian untuk mencari sumber kejadian, sambungan komunikasi, dan mendokumentasikan.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783

3. *Event Trigerring*
   Analisis awal terhadap proses kejadian. Barang bukti dalam *Device Mode On* untuk melanjutkan ke tahap *Proactive Preservation.*
4. *Proactive Preservation*
   Proses pengamanan barang bukti digital dan penonaktifan komunikasi data untuk mencegah perubahan data dari luar.
5. *Proactive Analysis*
   Pada tahap ini, dilakukan deteksi pelanggaran hukum, akuisisi data, dan pembuatan *Preliminary Report* sebagai laporan awal dari penyelidikan proaktif.
6. *Seize*
   Melakukan proses penyitaan terhadap barang bukti digital yang telah ditemukan untuk dianalisis lebih lanjut.
7. *Transportation*
   Melakukan proses pemindahan barang bukti digital dari tempat kejadian perkara menuju laboratorium digital forensik.

c. *Laboratorium Process*

Setelah penanganan barang bukti digital di tempat kejadian perkara, dilakukan analisis data terhadap barang bukti yang telah didapatkan sebelumnya guna mengidentifikasi jenis kejahatan yang terjadi (Ruuhwan et al., 2016). Tahap Proses Laboratorium terdiri dari 4 sub tahapan, yaitu:

1. *Preservation*
   Menjaga integritas barang bukti dengan *chain of custody* dan penerapan fungsi hashing. Barang bukti berupa *image* akan disimpan untuk digunakan dalam tahapan pemeriksaan.
2. *Examination*
   Pengolahan barang bukti untuk menemukan keterkaitannya dengan kejadian yang terjadi.
3. *Analysis*
   Tahap untuk menganalisis secara teknis dan merangkai keterkaitan antara temuan-temuan yang ada. Hasil dari temuan forensik digunakan untuk menghubungkan peristiwa yang terjadi.
4. *Documentation*
   Melakukan dokumentasi terhadap seluruh kegiatan, mulai dari awal proses penyelidikan hingga akhir proses analisis di laboratorium forensik.

d. *Presentation*

Tahap akhir dalam proses investigasi digital. Pada tahap ini, dilakukan pembuatan laporan berdasarkan hasil analisis yang telah dilakukan pada tahap sebelumnya serta memastikan bahwa setiap proses yang dilakukan sesuai dengan aturan hukum yang berlaku (Ruuhwan et al., 2016). Tahapan presentasi terbagi menjadi 3 sub tahapan sebagai berikut:

1. *Conclusion*
   Menguraikan hasil dari investigasi yang telah dilakukan sebagai bahan pertimbangan dalam pengambilan keputusan investigasi.
2. *Reconstruction*
   Menganalisis dan mengevaluasi keseluruhan hasil investigasi. Investigator melakukan rekonstruksi hasil temuan untuk memahami aktivitas tersangka.
3. *Dissemination*
   Mencatat proses penyelidikan yang dapat disebarluaskan kepada penyelidik lain sebagai referensi dalam penanganan kasus serupa.

3. ANALISA DAN PEMBAHASAN

Berdasarkan penjelasan pada bagian metode, penelitian ini menggunakan metode sesuai tahapan pada IDFIF v2 pada aplikasi Signal Desktop pada Windows 11. Hasil penelitian dijabarkan sesuai penjelasan pada tahapan dibawah ini:

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783

a. *Preparation*

1. *Notification*
   Pihak kepolisian daerah XYZ menerima laporan dari warga setempat terkait aktivitas mencurigakan salah satu warga yang diduga sebagai bandar narkoba. Kemudian pihak kepolisian melakukan penyelidikan berdasarkan laporan tersebut.

2. *Authorization*

   Status hukum naik ke proses penyidikan. Pihak kepolisian menangkap tersangka saat hendak pergi dari rumahnya dan menyita barang bukti berupa laptop Lenovo Legion 5 Pro yang diduga digunakan untuk berkomunikasi dengan kelompoknya.

3. *Preparation*

   Di lab forensik pada markas kepolisian telah disiapkan alat dan personel forensik untuk kebutuhan penyelidikan lebih lanjut terhadap barang bukti yang telah didapatkan. Akses telah didapatkan karena digunakan laptop milik peneliti. Selanjutnya, telah disiapkan barang bukti oleh peneliti berupa teks, multimedia, dan dokumen.

Tabel 2. *Spesifikasi Perangkat*

Nama Perangkat	Lenovo Legion 5 Pro
Sistem Operasi	Windows 11
Serial Number	PF3CTQ82
Total Storage	1 TB

Tabel 3. Deskripsi Barang Bukti

Teks	30 item
Gambar	10 item
Video	5 item
.pdf	10 tem

b. *Incident Response*

1. *Securing The Scene*

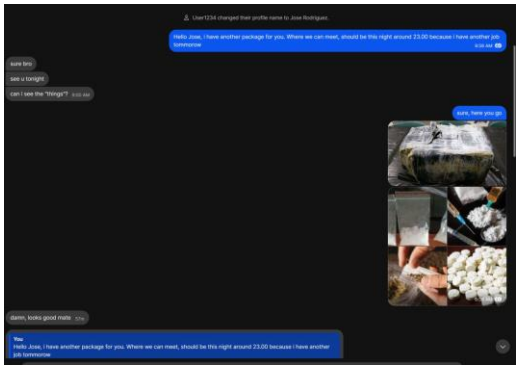
   Tempat kejadian diamankan dengan garis polisi agar orang yang tidak berkepentingan tidak dapat mengakses tempat tersebut dan dijaga agar keadaan tidak berubah dari saat ditemukan. Selanjutnya barang bukti diamankan menggunakan plastik khusus agar tidak rusak, kemudian diberikan label agar tidak hilang atau tertukar.

Gambar 3. Barang Bukti Laptop

2. *Documentation The Scene*

   Dokumentasi terhadap laptop sebagai barang bukti dan percakapan antara pelaku dan rekannya. Hal ini dilakukan untuk menggambarkan situasi sebelum analisis digital terhadap barang bukti sehingga dapat dijadikan acuan apabila ada ketidaksesuaian terhadap barang bukti.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783



Gambar 4. Bukti Percakapan pada Aplikasi Signal Desktop

3. *Event Trigerring*

   Kondisi saat barang bukti ditemukan adalah *Device Mode On* sehingga diputuskan melalui *proses Proactive Preservation.*

4. *Proactive Preservation*

   Sub tahapan *Network Trace* dan *Volatile Evidence* tidak dilakukan karena masuk dalam ranah forensik jaringan. Selanjutnya sesuai sub tahapan *Plug in Portable Power Supply*, dilakukan pengisian daya pada perangkat agar dapat selalu dalam kondisi hidup selama proses forensik. Kemudian sesuai sub tahapan *Communication Shielding*, pengaturan mode pesawat pada perangkat diaktifkan untuk mencegah perubahan pada barang bukti. Sesuai sub tahapan terakhir, *Non-Volatile Evidence*, barang bukti diamankan dengan melakukan tangkapan layar percakapan yang ada di aplikasi.

5. *Proactive Analysis*

   Pada subtahapan *Detection of Incident/Crime*, ditetapkan hipotesis terhadap tindak kejahatan yang dilakukan dengan melihat barang bukti percakapan pada aplikasi Signal Desktop, yakni telah terjadi proses komunikasi terkait distribusi narkoba melalui aplikasi Signal Desktop. Sesuai subtahapan *Acquicition*, dilakukan proses *imaging* data menggunakan alat bantu FTK Imager. Selanjutnya, disusun *Preliminary Report* sebagai laporan awal atas kegiatan analisis proaktif yang telah dilakukan.

6. *Seize*

   Dilakukan penyitaan barang bukti berupa laptop untuk diamankan untuk selanjutnya dikirim ke laboratorium untuk dianalisis.

7. *Transportation*

   Selanjutnya, barang bukti berupa laptop dipindahkan oleh pihak berwenang dari tempat kejadian perkara ke laboratorium untuk melakukan proses *Laboratorium Process*.

c. *Laboratorium Process*

Tahap ini akan diuraikan sesuai dengan 3 skenario yang telah ditetapkan sebelumnya.

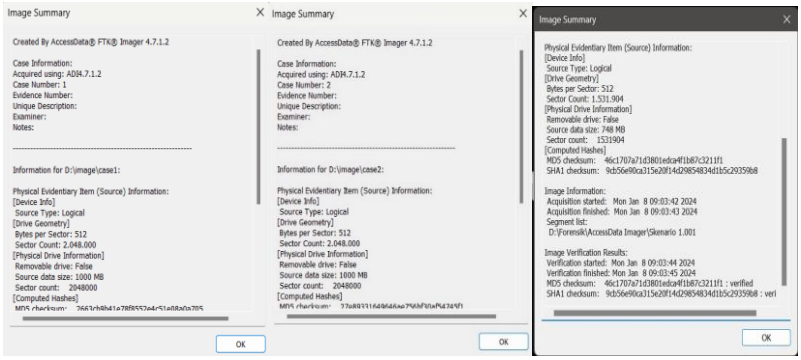
1. *Preservation*

   Dilakukan penyitaan barang bukti berupa laptop untuk diamankan untuk selanjutnya dikirim ke laboratorium untuk dianalisis.

   a) *Acquisition*

      Tahap akuisisi sudah dilakukan pada proses *Proactive Analysis* menggunakan alat bantu FTK Imager untuk proses *imaging* data dari aplikasi Signal Desktop.

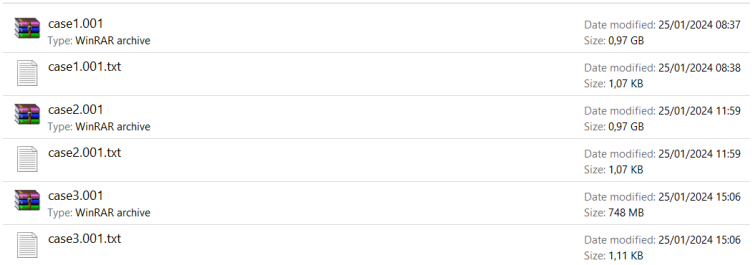
JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783



Gambar 5. *Imaging* Skenario 1, 2, dan 3

b) *Storage*

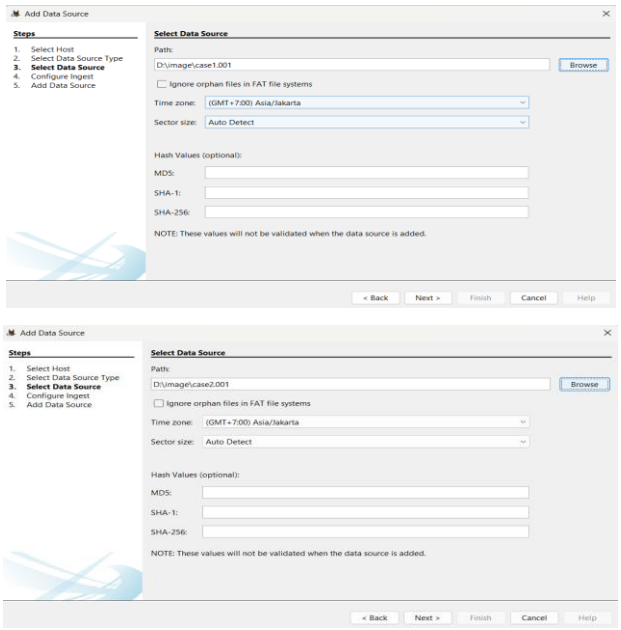
Setelah proses akuisisi, laptop dan barang bukti digital berupa *image* disimpan ke tempat yang aman. Hal ini dilakukan untuk mencegah agar barang bukti tidak berubah, rusak, atau hilang. Laptop disimpan di lemari barang bukti dan barang bukti digital disimpan pada partisi terpisah.



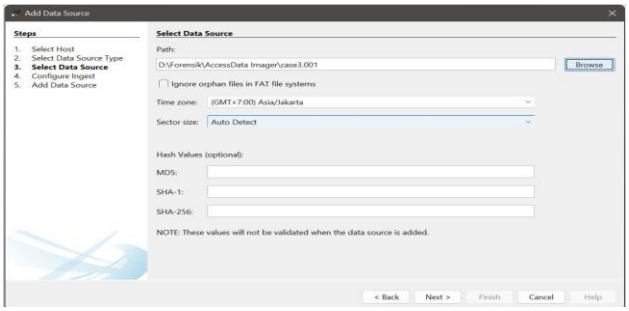
Gambar 6. Penyimpanan *image* barang bukti

2. *Examination*

Barang bukti berupa *image* selanjutnya akan dieksaminasi menggunakan alat bantu Autopsy. Hasil *image* pada tahap akuisisi akan digunakan sebagai *input* sumber data untuk proses eksaminasi.



JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783



Gambar 7. Proses *Examination* dengan Autopsy

3. *Analysis*

Setelah melakukan eksaminasi, dilakukan analisis untuk meneukan keterkatian antara penemuan dengan hipotesis yang telah dibuat. Hasil analisis selanjutnya dapat digunakan untuk bukti pendukung dan bahan pertimbangan dalam persidangan.

Tabel 4. Hasil Eksperimen Skenario 1

Variabel	Data digunakan (item)	Data yang didapatkan	
Teks	30	0	0%
Video	5	5	100%
Gambar	10	10	100%
File PDF (.pdf)	10	10	100%
Total	26	25	75%

Tabel 5. Hasil Eksperimen Skenario 2

Variabel	Data digunakan (item)	Data yang didapatkan	
Teks	30	0	0%
Video	5	1	20%
Gambar	10	9	90%
File PDF (.pdf)	10	5	50%
Total	26	15	40%

Tabel 6. Hasil Eksperimen Skenario 3

Variabel	Data digunakan (item)	Data yang didapatkan	
Teks	30	0	0%
Video	5	0	0%
Gambar	10	0	0%
File PDF (.pdf)	10	0	0%
Total	26	0	0%

Tabel 4. menjelaskan bahwa pada skenario 1, ditemukan sebagian besar artefak digital dengan persentase 75%. Pada Tabel 5. dijelaskan bahwa artefak digital yang ditemukan adalah 40%. Sedangkan pada Tabel 6. Dijelaskan bahwa tidak ditemukan artefak digital, yaitu 0%.

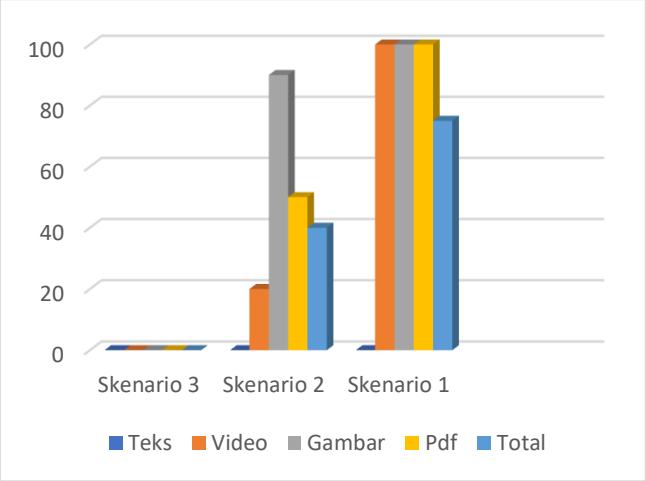
4. *Documentation*

Pada tahap dokumentasi akan dibuat laporan yang mencangkup hasil dari proses analisis. Laporan ini dapat digunakan sebagai bukti dukung dalam ranah hukum.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783

d. *Presentation*

Tahap akhir dilakukan dengan melakukan presentasi dari hasil investigasi yang didaptakn dari tahap eksaminasi dan analisis artefak digital yang didapatkan. Ringkasan hasil dapat dilihat pada grafik di Gambar 9.



Gambar 8. Grafik Data Hasil Forensik

1. *Conclusion*

   Pada skenario 1 diperoleh artefak digital sebesar 75%. Selanjutnya, pada skenario 2 diperoleh artefak digital sebesar 40%. Sedangkan pada skenario 3, tidak dapat ditemukan artefak digital. Pada ketiga skenario tidak dapat ditemukan *log chat.*

2. *Reconstruction*

   Dari hasil forensik digital dapat direkonstruksi kejadian krimnal yang terjadi, yaitu terjadi percakapan antara bandar narkoba dan rekannya yang berupaya mendistribusikan narkoba pada calon pelanggannya. Pada hari itu tersangka dan rekannya sudah melakukan perjanjian untuk bertemu di suatu tempat untuk melakukan distribusi narkoba. Hasil forensik ini dapat digunakan sebagai bukti dukung dalam persidangan terhadap tersangka dan calon pelanggan.

3. *Dissemination*

   Pada tahap ini akan dibuat laporan terkait proses penyelidikan forensik digital pada kasus distribusi narkoba yang sudah dilakukan sebagai referensi dalam penanganan kasus serupa.

4. KESIMPULAN

Setelah melakukan berbagai tahapan dan skenario percobaan, maka peneliti dapat menyimpulkan hasil penelitian digital forensik pada Signal Desktop menggunakan IDFIF v2. Pada skenario 1 diperoleh artefak digital sebesar 75%. Hal ini dikarenakan hanya ditemukan foto, video, dan dokumen tanpa ditemukan *log chat*. Pada skenario 2 diperoleh artefak digital sebesar 40%, dimana data yang ditemukan tidak sebanyak pada skenario 1 karena data pada scenario 2 sudah dihapus. Pada skenario 3 tidak dapat ditemukan artefak digital karena aplikasi Signal Desktop sudah di *uninstall*. Penelitian ini menunjukkan dampak forensik terhadap bukti digital yang difokuskan pada aplikasi Signal Desktop dimana penghapusan data pada aplikasi dan *uninstall* pada aplikasi memengaruhi hasil artefak digital yang didapatkan. Penelitian selanjutnya dapat dilakukan menggunakan alat bantu forensik digital lainnya dengan harapan dapat menemukan lebih banyak artefak digital, khususnya *log chat*.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 7, Januari 2024
ISSN 3025-0919 (media online)
Hal 774-783

REFERENCES

Ayunita Kinasih, R., Wirawan Muhammad, A., Adi Prabowo, W., Panjaitan No, J. DI, Kidul, P., Purwokerto Selatan, K., & Banyumas, K. 2020. Analisis Keamanan Browser Menggunakan Metode National Institute of Justice (Studi Kasus: Facebook dan Instagram). *Jurnal Teknologi Informasi & Komunikasi*, *11*, 174–184. https://doi.org/10.31849/digitalzone.v11i2.4678ICCS

Domingues, P., Andrade, L., & Frade, M. 2022. A Digital Forensic View of Windows 10 Notifications. *Forensic Sciences*, *2*(1), 88–106. https://doi.org/10.3390/forensicsci2010007

Prayogo, A. G., & 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), 21–29. https://doi.org/10.5120/ijca2022922393

Riadi, I., & Siregar, N. H. 2018. Forensik Mobile Pada Kasus Cyber Fraud Layanan Signal Messenger Menggunakan Metode NIST. *JOINTECS (Journal of Information Technology and Computer Science)*, *3*(1), 137–144. http://publishing-widyagama.ac.id/ejournal-v2/index.php/jointecs

Riadi, I., Herman, & Siregar, N. H. 2022. Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework. *Ingénierie Des Systèmes d Information*, *27*(6), 903–913. https://doi.org/10.18280/isi.270606

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

Ruuhwan, R., Riadi, I., & Prayudi, Y. 2016. Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(1). https://doi.org/10.26418/jp.v2i1.14369

Uzun, T., Manager, P., & Forensics, M. 2015. *Mobile Chat And Social App Forensics*. Webinar: Mobile Chat And Social App Forensics. https://www.forensicfocus.com/webinars/mobile-chat-and-social-app-forensics/

Wikipedia. 2023. *Digital Forensics*. Wikipedia. https://en.wikipedia.org/wiki/Digital_forensics