Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 7 Nomor1, 2024
P-2655-710X e-ISSN 2655-6022

Submitted : 18/01/2024
Reviewed : 24/01/2024
Accepted : 29/01/2024
Published : 30/01/2024

Nugroho Adi Wibowo[1]
Khoerina Sa'adah[2]
I Gede Gilang Dharma Suputra[3]
Jeckson Sidabutar[4]

ANALISIS FORENSIK DIGITAL INSTANT MESSAGING TWINME PADA EMULATOR BERBASIS ANDROID BERDASARKAN NIST SP 800-101 REV 1

Abstrak

Penelitian ini menyelidiki aspek forensik digital dari aplikasi Instant Messaging (IM) Twinme pada emulator berbasis Android, dengan fokus khusus pada pemanfaatan kerangka kerja NIST 800-101 Revisi 1. Twinme, sebuah aplikasi IM yang mengedepankan keamanan melalui enkripsi mobile, memungkinkan pengguna untuk berkomunikasi tanpa harus bertukar informasi pribadi seperti nomor telepon atau email. Namun, kasus-kasus kriminal, seperti distribusi narkotika oleh narapidana yang menggunakan Twinme dari dalam lembaga pemasyarakatan, mengindikasikan adanya potensi penyalahgunaan yang dapat disembunyikan dari pihak berwenang. Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menganalisis artefak digital yang dapat berfungsi sebagai bukti yang dapat diterima secara hukum terkait penyalahgunaan Twinme. Proses analisis forensik mengikuti kerangka kerja NIST 800-101 Rev 1, yang memberikan landasan hukum yang kuat untuk hasil investigasi. Dengan memahami bahaya keamanan yang terkait dengan aplikasi IM, penelitian ini bertujuan untuk berkontribusi pada pengembangan praktik forensik digital yang efektif dan mendukung proses hukum dalam menanggapi aktivitas kriminal yang melibatkan aplikasi komunikasi serupa.

Kata Kunci: Android Emulator, Aplikasi Twinme, Forensik Digital, NIST Framework

Abstract

This research investigates the digital forensics aspects of the Twinme Instant Messaging (IM) application on an Android-based emulator, with a particular focus on utilizing the NIST 800-101 Revision 1 framework. Twinme, an IM application that promotes security through mobile encryption, allows users to communicate without having to exchange personal information such as phone numbers or emails. However, criminal cases, such as the distribution of narcotics by inmates using Twinme from inside correctional institutions, indicate the potential for abuse that can be hidden from authorities. The purpose of this research is to identify and analyze digital artifacts that could serve as legally admissible evidence of Twinme misuse. The forensic analysis process follows the NIST 800-101 R1 framework, which provides a strong legal foundation for the investigation results. By understanding the security hazards associated with IM applications, this research aims to contribute to the development of effective digital forensics practices and support legal proceedings in response to criminal activity involving similar communication applications.

Keywords: Android emulator, Twinme app, Digital forensics, NIST framework

PENDAHULUAN

Instant Messaging (IM) merupakan teknologi komunikasi yang semakin marak digunakan oleh masyarakat global karena kemudahan yang ditawarkan dalam komunikasi jarak jauh dan keamanannya (Larson, 2023). Aplikasi Twinme merupakan salah satu IM yang menawarkan keamanan komunikasi dengan mengadopsi teknik enkripsi end-to-end. Twinme

[1,2,3,4)]Rekayasa Keamanan Siber, Jurusan Keamanan Siber, Politeknik Siber dan Sandi Negara
email: nugroho.adi@student.poltekssn.ac.id, khoerina.saadah@student.poltekssn.ac.id, igede.gilang@student.poltekssn.ac.id , jeckson.sidabutar@poltekssn.ac.id

tidak hanya menyediakan layanan berikirim pesan melainkan juga panggilan suara dan video dengan kualitas tinggi. Uniknya, tidak seperti IM WhatsApp dan Telegram, Twinme memungkinkan berbagi konten tanpa harus melakukan registrasi menggunakan data pribadi seperti nomor telepon, email, maupun akses kontak perangkat selama proses aplikasi (Mascellino, 2023). Inovasi yang ditawarkan tersebut bertujuan untuk menjaga privasi dan informasi pribadi penggunanya. Namun di sisi lain, ini juga dapat menjadi potensi penyalahgunaan oleh pihak yang tidak bertanggungjawab untuk menyembunyikan aktivitas kriminal.

Berdasarkan pemberitaan oleh Kompas.com, sejumlah narapidana dalam jejaring narkoba menggunakan aplikasi Twinme untuk mendistribusikan narkoba dari dalam Lembaga Pemasyarakatan Jakarta Utara. Para narapidana tersebut memanfaatkan aplikasi Twinme untuk mempersulit kemungkinan pelacakan oleh pihak berwenang karena tidak adanya informasi nomor telepon yang dicantumkan (Farisi, Movanita, 2023). Berdasarkan kasus yang tersebut, ini menunjukkan adanya potensi berbahaya yang melibatkan aplikasi IM sebagai media komunikasi. Untuk menghadapi potensi kejahatan ini studi forensik digital merupakan langkah penting yang perlu dikembangkan untuk dapat mengidentifikasi artefak digital guna menjadikannya sebagai bukti digital yang sah dan memiliki legalitas di mata hukum. Untuk mendapatkan keabsahan bukti digital dibutuhkan proses analisis forensik digital pada perangkat barang bukti yang sesuai dengan kerangka kerja yang telah diakui oleh hukum (Hikmatyar, Sugiantoro, 2019). Penggunaan kerangka kerja atau framework juga membantu analis forensik dalam mengumpulkan bukti digital, menganalisis data, mengidentifikasi jejak, serta menyajikan temuan secara akurat.

Pada penelitian-penelitian terdahulu pernah dilakukan analisis forensik dengan menggunakan beberapa framework terkait. Penelitian oleh Bagus Pribadi, Sri Rosdiana, dan Samsul Arifin (Pribadi dkk, 2023) melakukan investigasi forensik terhadap kejahatan aplikasi Facebook Messenger untuk menentukan bukti digital menggunakan framework NIST 800-101 Rev 1. Hasil penelitian menujukkan adanya temuan artefak forensik aplikasi Facebook Messenger berupa kontak, riwayat pesan, panggilan, foto, file audio, file video, dan dokumen. Pada penelitian lain oleh Faris Febrian dan Jeckson Sidabutar (Febrian, Sidabutar 2023) dilakukan analisis forensik terhadap aplikasi WhatsApp Desktop pada Mac OS dan Windows menggunakan metode IDFIF V2. Dari penelitian tersebut menghasilkan prosedur forensik yang digunakan dalam melakukan investigasi aplikasi WhatsApp Desktop untuk mendapatkan bukti berupa sesi percakapan yang sudah dihapus, daftar nomor kontak, foto profil korban, dan lainnya. Pada penelitian (Menahil dkk, 2021), membahas analisis forensik terhadap lima platform media sosial, yakni Instagram, LINE, Whisper, WeChat, dan Wickr pada smartphone berbasis Android menggunakan framework NIST SP 800-101 Rev 1. Proses ekstraksi dan analisis data dilakukan dengan memanfaatkan tiga alat, yaitu Magnet AXIOM, XRY, dan Autopsy. Hasil eksperimen menunjukkan bahwa sejumlah besar data penting berhasil diekstraksi dari smartphone yang sedang diselidiki. Temuan dari penelitian ini mengindikasikan bahwa di antara ketiga alat tersebut, Magnet AXIOM menduduki peringkat pertama dengan indeks sebesar 76,0%, diikuti oleh Autopsy dengan indeks sebesar 71,5%, dan XRY menempati peringkat ketiga dengan indeks sebesar 65,5%.

Berdasarkan penelitian-penelitian tersebut dapat diketahui bahwa studi analisis forensik digital yang telah ada sebelumnya hingga saat ini masih belum ada pembahasan mengenai forensik pada aplikasi Twinme baik dengan memanfaatkan tools forensik maupun secara manual. Mayoritas penelitian-penelitian terdahulu menggunakan aplikasi IM yang umum digunakan oleh masyarakat. Aplikasi Twinme memiliki fitur keamanan yang tidak kalah dengan aplikasi IM pada umumnya. Dibutuhkan adanya studi lebih lanjut mengenai forensik aplikasi Twinme mengingat fitur keamanan yang dimiliki serta potensi penyalahgunaan berdasarkan laporan tindak kejahatan yang telah ada. Adanya penelitian ini bertujuan untuk membantu organisasi ataupun pihak-pihak terkait dalam mengembangkan kebijakan dan prosedur yang tepat untuk menangani insiden serupa.

METODE

Proses analisis forensik digital aplikasi Twinme pada emulator smartphone berbasis

Android dilakukan dengan menggunakan metode yang mengacu pada kerangka kerja NIST SP 800-101 Rev 1. Berdasarkan kerangka kerja tersebut tahapan-tahapan yang perlu dilakukan dalam proses analisis mobile forensic digital meliputi preservation, acquisition, examination and analysis, dan reporting (Ayers dkk, 2014).

Gambar 1. Tahapan analisis forensik berdasarkan NIST SP 800-101 Rev 1

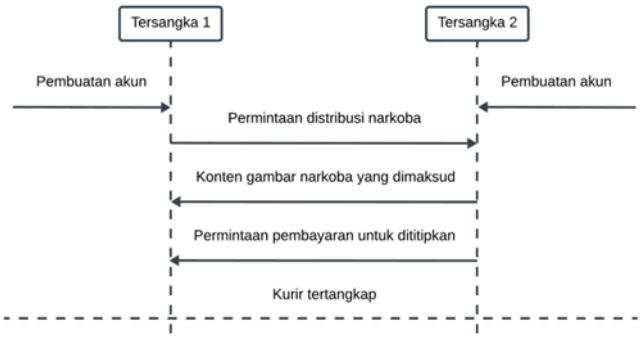
1. Preservation
   Pada tahapan ini melibatkan proses pelestarian terhadap bukti digital yang diperoleh dengan melalui pencarian, pendokumentasian, dan pengumpulan bukti digital.
2. Acquisition
   Bukti digital yang telah ditemukan oleh analis forensik perlu diakuisisi untuk menjaga integritas data pada bukti digital yang asli.
3. Examination and analysis
   Pada tahapan ini, bukti digital yang diperoleh digunakan analis keamanan untuk mengungkap artefak-artefak digital yang telah dihilangkan baik dengan cara menghapus ataupun menyembunyikannya.
4. Reporting
   Temuan-temuan yang diperoleh dan kinerja selama proses analisis forensik perlu dirangkum dan disajikan guna mendukung proses hukum. Isi laporan yang dibuat ini harus sesuai dengan data yang diperoleh selama proses analisis forensik berlangsung.

Skenario yang digunakan pada penelitian ini bertujuan untuk memberikan gambaran pada beberapa kondisi. Barang bukti pada studi kasus penelitian ini berupa perangkat laptop dengan emulator smartphone berbasis android dalam kondisi root. Skenario yang diujicobakan melibatkan dua kondisi dimana kondisi pertama yaitu pesan yang dikirim telah dihapus dan skenario kedua yaitu pesan yang tidak dilakukan penghapusan.

Tabel 1. Skenario penelitian

Simulasi kondisi dilakukan forensik		
Skenario	**Pesan dihapus**	**Pesan tidak dihapus**
Dilakukan backup data	Kondisi 1	Kondisi 3
Tidak dilakukan backup data	Kondisi 2	Kondisi 4

Skenario poin percakapan dari simulasi yang akan dilakukan forensik direpresentasikan pada gambar berikut.



Gambar 2. Skenario poin percakapan yang digunakan

Riwayat percakapan yang terdiri dari 22 pesan singkat dan 4 gambar tersebut diungkap melalui forensik pada barang bukti berupa perangkat laptop yang terinstal emulator dengan kondisi sesuai skenario tersangka 1 dan 2. Pengungkapan bukti digital dalam memperjelas kasus yang terjadi dilakukan dengan melakukan analisis forensik riwayat percakapan kedua tersangka pada akun Twinme yang dimiliki. Analisis forensik pada keempat kondisi yang dijelaskan pada tabel 1. dilakukan dengan menggunakan tools Magnet AXIOM 5.40 dan akuisisi data pada Emulator Android akan menggunakan perintah ADB (Android Debug Bridge) yang disediakan Platform-tool. Teknik tersebut mengekstrak data yang ada pada perangkat melalui interaksi terhadap sistem operasi dan akses filesystem (Tamma dkk, 2020).

.

HASIL DAN PEMBAHASAN

Data yang diambil pada emulator berbasis android dengan bantuan tools magnet AXIOM dan akuisisi manual digunakan sebagai bahan analisa. Pada proses penemuan bukti digital dari barang bukti dilakukan dengan menggunakan metode NIST SP 800-101 Rev 1.

Preservation

Proses preservation dilakukan terhadap perangkat Laptop HP Pavilion yang telah terinstal emulator LDP Player dengan tipe perangkat mobile Samsung A805N. Emulator dan barang bukti tersebut memiliki spesifikasi sebagai berikut.

Tabel 2. Spesifikasi perangkat

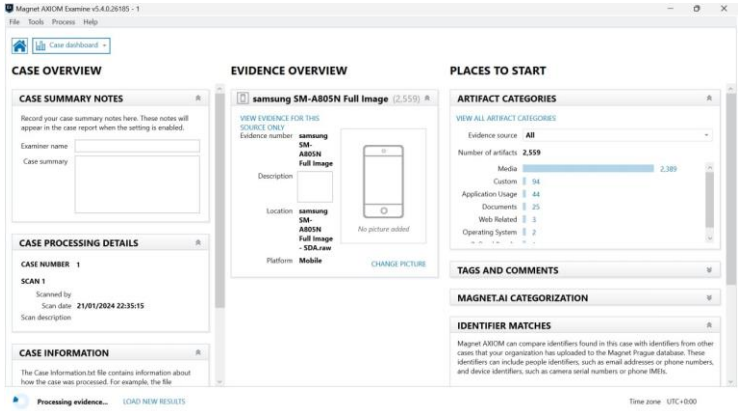
Kategori	Environment	Spesifikasi	Informasi
Emulator	LDP Player Samsung A805N	RAM	4 GB
		Penyimpanan internal	64 GB
		Operating system	Android 9
Barang bukti	Laptop HP Pavilion	RAM	16 GB
		Penyimpanan internal	512 GB
		Operating system	Windows 11

Untuk mengetahui informasi lainnya seperti IMEI dapat melalui tab models pada pengaturan emulator, sedangkan secara terpisah untuk mengetahui penyimpanan internal dari jenis perangkat smartphone yang digunakan emulator dapat melalui menu setting pada android. Perangkat mobile yang digunakan oleh emulator telah terpasang aplikasi instant messaging bernama Twinme dengan versi 22.4.

Acquisition

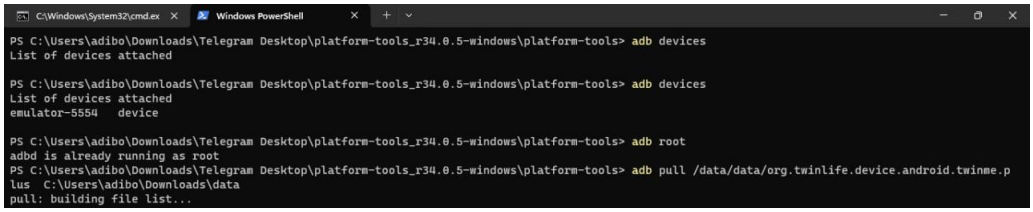
Tahap akuisisi dilakukan dengan full imaging pada emulator android untuk memperoleh semua konten informasi yang masih tersimpan. Metode forensik yang digunakan selama proses akuisisi ini yatu live forensics dimana proses dilakukan pada emulator dengan kondisi sistem berjalan dan kondisi hidup (Interpol, 2019). Hak akses pada emulator yang digunakan dalam kondisi root.

Gambar 3. Barang bukti laptop HP Pavilion

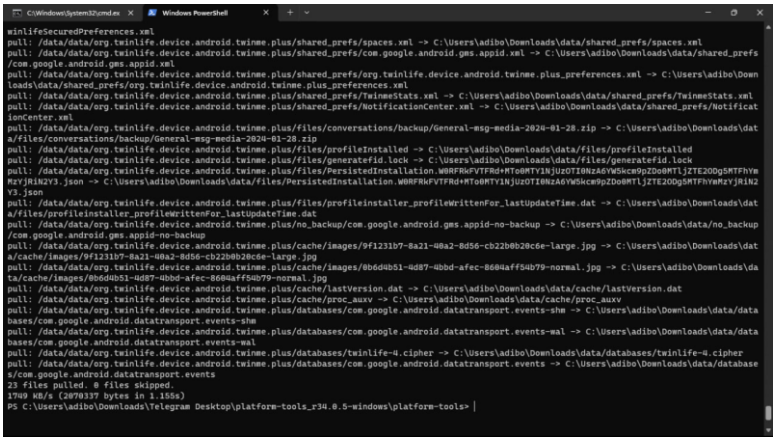


Gambar 4. Full imaging akuisisi emulator menggunakan Axiom Process

Proses acquisition juga dilakukan dengan menggunakan metode software-based pada emulator berbasis android yang terpasang pada perangkat barang bukti dan melalui akuisi ekstraksi data ADB Pull dari emulator android ke penyimpanan laptop. (Tamma, dkk, 2020). Perintah ini dapat menyalin satu file atau satu folder directory ke perangkat peneliti. Penggunaan perintah ini disertai dengan opsi -a yang akan menjaga mode tulis dan juga waktu pembuatan file maupun folder yang disalin. Target folder yang diakuisisi pada perangkat adalah direktori /data/ yang berisi data aplikasi Twinme yang terpasang.



Gambar 5. Proses akuisisi ekstraksi data emulator menggunakan ADB Pull

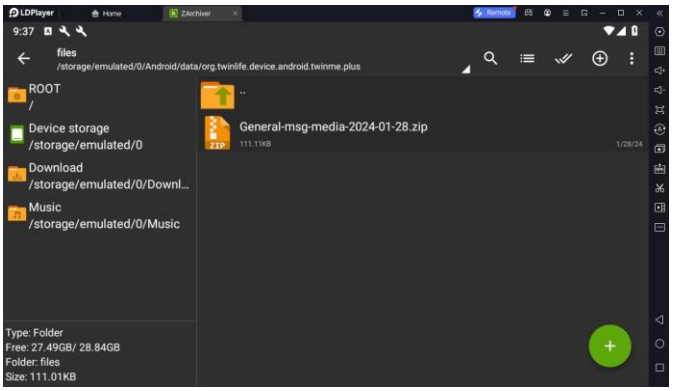


Gambar 6. Proses akuisisi ekstaksi data ADB Pull sukses dilakukan

Proses tersebut dilakukan sebelum pesan dihapus dan setelah pesan dihapus dengan masing-masing skenario dilakukan backup data dan tidak dilakukan backup data. Dengan demikian, penelitian ini dijalankan dengan empat kondisi berbeda.

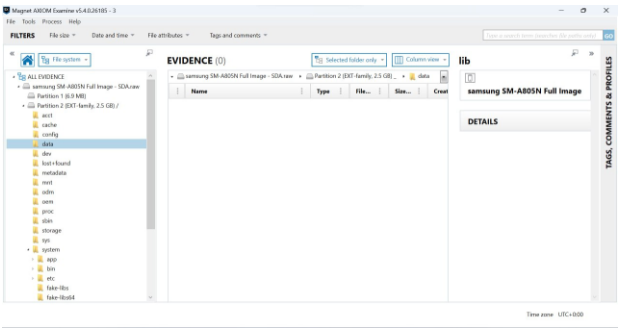
Examination and Analysis

Proses examination pada data digital menggunakan bantuan tools Magnet AXIOM. Pada beberapa kondisi yang dilakukan dalam skenario diperoleh informasi bahwa backup data aplikasi Twinme versi 22.4 pada emulator android terletak dalam direktori folder /storage/emulated/0/Android/data/org.twinlife.device.android.android.twinme dengan nama file General-msg-media-2024-01-28.zip.



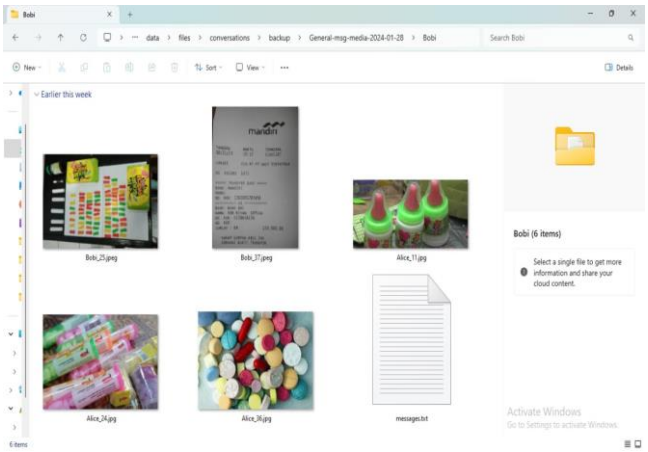
Gambar 7. Lokasi folder backup percakapan aplikasi Twinme

File backup data aplikasi Twinme berisikan seluruh riwayat pesan baik berupa pesan tertulis maupun media yang dikirimkan melalui pesan pada ruang percakapan milik pengguna. Tools Magnet Axiom versi 5.4 digunakan pada tahap akuisisi untuk mengumpulkan data digital. Berdasarkan dari data digital yang diperoleh ketika ditelusuri dengan tools AXIOM Examine, folder backup data tersebut tidak berhasil diakuisisi oleh tools Magnet AXIOM sehingga ketika dilakukan pencarian folder backup tersebut tidak ada.

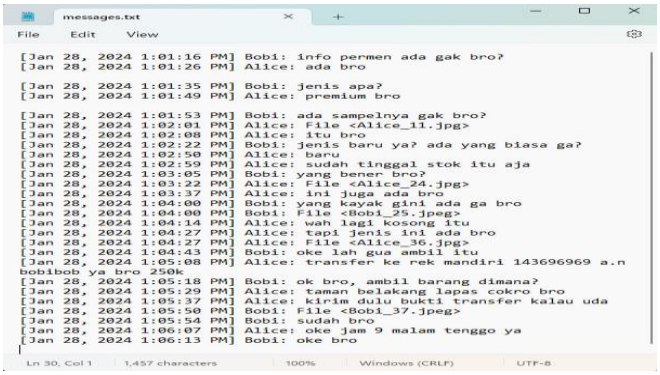


Gambar 8. Proses pemeriksaan pada file imaging data digital

Penelitian dilanjutkan dengan menganalisis hasil ujicoba akuisisi ekstraksi data menggunakan ADB Pull pada backup data yang kemudian dibuktikan keintegritasannya melalui nilai hash, data bukti digital berhasil diakuisisi dan diperoleh bukti digital berupa riwayat pesan dan media yang dimuat dalam ruang percakapan.



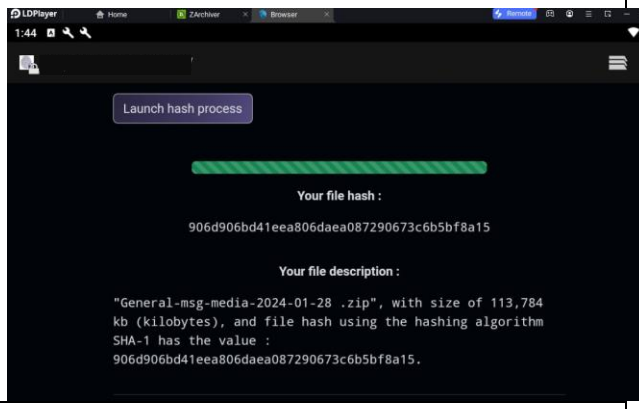
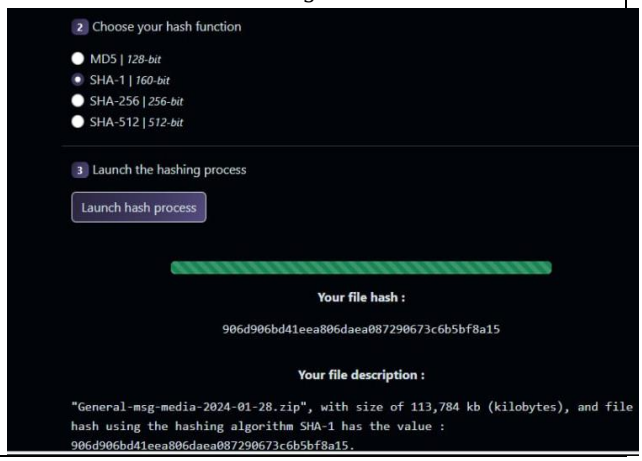
Gambar 9. Bukti digital yang didapatkan proses ekstraksi data ADB Pull



Gambar 10. Bukti digital percakapan yang ditemukan

Kemudian untuk memastikan data yang telah diekstraksi dapat disimpan dan memiliki nilai hash yang sama atau tetap, dilakukan dokumentasi terhadap nilai hash file backup yang didapatkan baik sebelum maupun sesudah dilakukan ekstrasi data sebagai berikut.

Tabel 3. Nilai hash file backup

File Backup	Nilai Hash SHA1	Dokumentasi
Asli	da39a3ee5e6b4b0d3255bfef95601890afd80709	
Ekstraksi Data	da39a3ee5e6b4b0d3255bfef95601890afd80709	s 

Report

Berdasarkan proses yang dilakukan pada tahapan sebelumnya tidak diperoleh hasil sesuai harapan dengan menggunakan tools Magnet AXIOM, namun proses akuisisi justru berhasil dilakukan menggunakan akuisisi ekstraksi data dengan ADB Pull.

Berdasarkan dari hasil yang didapat selama proses analisis forensik aplikasi Twinme pada skenario penelitian dengan kondisi-kondisi yang telah ditentukan diperoleh hasil sebagai berikut.

Tabel 4. Hasil proses forensik digital

Hasil forensik		
Skenario	**Pesan dihapus**	**Pesan tidak dihapus**
Dilakukan backup data	Tidak didapatkan bukti digital	Didapatkan bukti digital
Tidak dilakukan backup data	Tidak didapatkan bukti digital	Tidak didapatkan bukti digital

Dengan menggunakan tools Magnet AXIOM aplikasi Twinme pada emulator berbasis Android tidak memberikan hasil sesuai dengan apa yang diharapkan. Namun, hal seperti ini mungkin saja terjadi mengingat setiap tools forensik memiliki modul akuisisi yang berbeda-beda sehingga masing-masing tools memiliki hasil yang berbeda.

SIMPULAN

Proses forensik yang dilakukan dengan bantuan tools Magnet Axiom 5.4 pada aplikasi Twinme yang berjalan di emulator berbasis android tidak dapat memberikan hasil sesuai dengan harapan, namun di sisi lain dari proses studi kasus yang dilakukan diperoleh informasi bahwa backup folder pada aplikasi Twinme tidak dapat diakuisisi dengan menggunakan logical imaging melalui tools yang diusulkan dan justru proses akuisisi ekstraksi data dapat memberikan hasil yang lebih baik. Berdasarkan hasil yang diperoleh pada penelitian ini terdapat peluang bagi penelitian di masa mendatang untuk daapt lebih mendalami dan melakukan eksplorasi dalam penggunaan tools forensik serta teknik-teknik yang digunakan untuk mendapatkan data digital aplikasi Twinme.

DAFTAR PUSTAKA

Alessandro, M. (5 April 2023). 8 Best Encrypted Messaging Apps. (https://www.androidpolice.com/best-encrypted-messaging-apps), diakses 15 Desember 2023.

Baharudin, A. F., Ambaranie, N. K. M. (13 Oktober 2023). Napi Kendalikan Narkoba dari Dalam Lapas di Jakarta, Komunikasi Lewat Aplikasi "Twinme". (https://megapolitan.kompas.com/read/2023/10/13/18572021/napi-kendalikan-narkoba-dari-dalam-lapas-di-jakarta-komunikasi-lewat), diakses 15 Desember 2023.

Febrian, F.F., & Sidabutar, J. (2023). Comparative Analysis of Forensic for Whatsapp Desktop on Mac OS and Windows Using IDFIF V2. IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, Indonesia, 2023, pp. 327-331, doi:10.1109/ICoCICs58778.2023.10276727.

Hikmatyar, F. G., & Sugiantoro, B. (2019). Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases. IJID (International Journal on Informatics for Development), 7(2), 64–67. https://doi.org/10.14421/ijid.2018.07204.

INTERPOL. (2019). Global Guidelines for Digital Forensics Laboratories. INTERPOL Glob. Complex Innov., no. May, pp. 1–80. (https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelines DigitalForensicsLaboratory.pdf), diakses 28 Januari 2024.

Larson, G. W. (2023, November 24). instant messaging. Encyclopedia Britannica. (https://www.britannica.com/topic/instant-messaging), diakses 15 Desember 2023.

Menahil, A., Iqbal, W., Iftikhar, M., Bin Shahid, W., Mansoor, K. & Rubab, S. (2021) Forensic Analysis of Social Networking Applications on an Android Smartphone," Wirel Commun Mob Comput, vol. 2021, doi: 10.1155/2021/5567592.

Pribadi, B., Rosdiana, S. & Arifin, S. (2023). Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases. Procedia Computer Science. 216. 10.1016/j.procs.2022.12.123.

R. Ayers, W. Jansen, dan S. Brothers. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). NIST Special Publication, vol. 1, no. 1, hlm. 85. (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf), diakses pada 15 Desember 2023

Tamma, R., Skulkin, O., Mahalik, H. & Bommisetty, S. (2020). Practical Mobile Forensics 4th edition: Forensically investigate and analyze iOS, Android, and Windows 10 devices. Birmingham: Packt Publishing Ltd.