Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute Of Standard And Technology (Nist Sp 800-86)

1st Mohammad Rifqi
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
mrifqii@student.telkomuniversity.ac.id

2nd Setia Juli Irzal Ismail
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
julismail@staff.telkomuniversity.ac.id

3rd Mochammad Fahru Rizal
Fakultas Ilmu Terapan
Universitas Telkom,
Bandung
mfrizal@staff.telkomuniversity.ac.id

Abstrak **-- Analisis forensik memiliki peran vital dalam penanganan kejahatan cyber pada aplikasi. Salah satu metode yang digunakan adalah metode National Institute of Standards and Technology (NIST) yang bertujuan untuk mengevaluasi bukti digital dalam aplikasi yang digunakan oleh pelaku kejahatan. Proses analisis dengan metode NIST melibatkan identifikasi, pengumpulan, analisis, interpretasi, dan dokumentasi bukti digital. Tim forensik menggunakan perangkat lunak dan peralatan khusus untuk mengakses informasi penting dari bukti digital. Metode NIST memiliki keunggulan dalam standarisasi proses, memfasilitasi kerja tim forensik, dan meningkatkan kualitas analisis. Ini juga memastikan integritas bukti digital yang dapat digunakan dalam pengadilan. Hasil analisis forensik dengan metode NIST penting dalam menangani kejahatan cyber pada aplikasi. Proses analisis yang terstruktur menjamin akurasi dan validitas bukti digital, menjadi dasar untuk tindakan hukum terhadap pelaku kejahatan. Dalam era di mana teknologi semakin merasuk ke berbagai aspek kehidupan, analisis forensik dengan metode NIST menjadi elemen krusial dalam menjaga keamanan digital dan menyediakan alat bukti yang kuat dalam persidangan.**

Kata Kunci -- Analisis Forensik, Penanganan cybercrime, WhatsApp, identifikasi, bukti digital.

I. PENDAHULUAN

A. Latar Belakang

Dikutip dari inakoran.com, Kabid Penmas Polda Sumut AKBP MP Nainggolan mengatakan, penggunaan aplikasi WhatsApp oleh sekelompok orang untuk menipu berkedok meminta uang di Indonesia bukan sebuah hal yang mengejutkan. Banyak pelaku penipuan yang tertangkap mengakui bahwa komunikasi antara pelaku dan korban dilakukan melalui aplikasi WhatsApp. Salah satunya perwira polisi menjadi korban penipuan oleh oknum polisi melalui aplikasi WhatsApp pada tahun 2020. Nainggolan menjelaskan ada sejumlah perwira polisi di Polda Sumut yang menjadi korban praktik yang dilakukan peretas *(hacker)* untuk meminta sejumlah uang melalui WhatsApp [1]. Dengan adanya ilmu forensik yang terus berkembang, kasus tersebut dapat diperiksa dengan menganalisa barang bukti digital dari perangkat *mobile* di aplikasi WhatsApp. Metode yang cocok untuk kasus tersebut ialah dengan menggunakan ilmu forensik pada perangkat Android aplikasi WhatsApp agar mendapatkan barang bukti digital.

Dalam pasal UU Nomor 19 Tahun 2016 mengenai Informasi dan Transaksi elektronik (“UU ITE”) terkandung pada pasal 5 menyebutkan bahwa informasi elektronik atau dokumen elektronik merupakan alat bukti yang sah secara hukum di negara Indonesia [2]. Terkandung dalam pasal 6 informasi elektronik atau dokumen elektronik dianggap sah informasinya bila di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggung jawabkan sehingga menerangkan suatu keadaan [3]. Penelitian ini melakukan Forensik Android di Internet pada aplikasi pesan WhatsApp. Perangkat yang di gunakan ialah Emulator Nox Player versi 7.0.5.7.

Penelitian ini, meliputi penggunaan user seperti install, login, memasukan/memperbaharui/menghapus kontak, pertukaran pesan, berbagi lokasi, serta penghapusan komunikasi.

Tools yang digunakan memakai software SQLite Browser v3.12.2 dan Root Explorer v4.10.3 untuk menganalisis file msgstore.db/.db yang jadikan bukti digital dan untuk *rooting device* menggunakan aplikasi Magisk v25.2 untuk Auto Root, serta untuk memastikan sudah diroot menggunakan aplikasi Root Checker Basic v6.5.3 dan skenario kasus yang di tangani adalah kasus penipuan yang dilakukan oleh pelaku terhadap korban untuk melakukan aksinya dengan mengajak main korban.

II. KAJIAN TEORI

A. Digital Forensik

Dalam era yang didominasi oleh teknologi digital, pemahaman dan aplikasi forensik digital menjadi semakin penting dalam menangani beragam jenis kejahatan. Konsep dasar digital forensik melibatkan penyelidikan mendalam untuk mengungkap bukti digital yang dapat menguatkan atau melemahkan bukti fisik dari sebuah kasus. Awalnya diidentifikasi dengan istilah forensik komputer, namun saat ini lingkupnya telah meluas menjadi melibatkan analisis perangkat apapun yang mampu menyimpan data digital [8].

Dalam era dimana informasi digital merasuk dalam berbagai aspek kehidupan, penggunaan teknologi dalam tindak kriminal juga meningkat. Oleh karena itu, kemampuan untuk mengumpulkan, menganalisis, dan menguraikan bukti digital dengan cermat adalah esensial dalam menghadapi tantangan baru ini. Aktivitas forensik digital melibatkan penerapan metode ilmiah untuk mengidentifikasi, mengumpulkan, memeriksa, dan mempertimbangkan bukti digital, yang pada gilirannya dapat digunakan dalam proses hukum.

Ketika membahas forensik digital, aspek yang diperhatikan tidak hanya perangkat komputer, tetapi juga mencakup berbagai perangkat yang memiliki kapabilitas penyimpanan dan pemrosesan data digital, seperti ponsel pintar, tablet, perangkat penyimpanan eksternal, serta *Internet of Things* (IoT). Oleh karena itu, keahlian dalam menganalisis jejak digital dari berbagai sumber menjadi semakin penting.

Dalam konteks ini, pemahaman tentang prinsip – prinsip dasar digital forensik dan evolusinya menjadi aspek yang tak terpisahkan dari investigasi modern. Melalui penggalian bukti digital yang kuat dan sah, para penyidik dan praktisi hukum dapat membentuk dasar yang kokoh untuk mengungkap kebenaran di tengah kompleksitas dunia digital saat ini.

B. WhatsApp

Dalam era digital yang semakin berkembang, komunikasi telah mengalami transformasi signifikan. Aplikasi pesan instan telah menjadi tulang punggung komunikasi modern, memengkinkan pengguna untuk terhubung dan berkomunikasi dengan cepat melalui berbagai platform. Salah satu inovasi utama dalam ranah ini adalah Whatsapp, sebuah aplikasi pesan yang dirancang khusus untuk ponsel cerdas. Whatsapp telah memperkenalkan paradigma baru dalam berkomunikasi, yang melampui batasan geografis dan teknologi konvensional [9].

Whatsapp berfungsi sebagai aplikasi pesan lintas platform yang memungkinkan pertukaran pesan dengan mudah, mengeliminasi kebutuhan untuk pulsa melalui pemanfaatan paket data internet. Konsep ini telah merevolusi cara orang berkomunikasi, menghubungkan individu dari seluruh dunia tanpa hambaran fisik atau biaya yang signifikan. Dengan menggunakan teknologi data internet, whatsapp messenger memberikan kebebasan untuk berinteraksi secara real-time, berbagai informasi, dan mengirim pesan dalam berbagai format.

Pengenalan aplikasi ini membawa aspek-aspek teori komunikasi dan teknologi ke dalam fokus. Perpaduan antara aplikasi pesan instan dan pemanfaatan paket data internet menggambarkan bagaimana teknologi terus mengubah cara kita berinteraksi dan berkomunikasi. Konsep kecepatan, konektivitas global, dan aksesibilitas menjadi inti dari revolusi komunikasi yang WhatsApp bawa. Dalam konteks ini, pemahaman mendalam tentang aplikasi WhatsApp tidak hanya membantu kita menghargai dampaknya pada komunikasi, tetapi juga menerangi betapa pentingnya pengetahuan tentang teknologi dalam kehidupan sehari-hari yang semakin terhubung.

C. NIST (*National Institute of Standards Technology*)

Metode Forensik NIST adalah tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan menggunakkan metode NIST. Terjadi saat data yang dikumpulkan diperiksa, lalu mengekstrak data dari media dan mengubahnya menjadi format yang bisa diproses oleh alat forensik dan data transformasikan menjadi informasi melalui analisis. Tahap metode NIST yaitu media, data, analisa, dan bukti.

Dalam investigasi digital, Metode Forensik NIST adalah panduan yang membantu ahli forensik dalam mengumpulkan, menganalisis, dan mengamankan bukti digital secara ilmiah. Ini memastikan bahwa proses analisis bukti digital dilakukan dengan akurat dan terpercaya. Berikut adalah langkah-langkah dasar dalam metode ini:

1. Media: Identifikasi dan amankan media yang mengandung bukti digital, seperti hard drive atau kartu memori. Tujuannya adalah melindungi integritas bukti dan mencegah perubahan yang tidak sah.
2. Data: Ekstraksi data dari media yang ditemukan. Ini melibatkan isolasi data relevan dan memastikan integritasnya terjaga. Data yang dihapus atau diubah juga ditemukan pada tahap ini.
3. Analisa: Teliti dan interpretasikan data untuk mengungkap pola dan bukti yang mungkin ada. Gunakan alat dan teknik forensik yang terbukti untuk memahami informasi yang ditemukan.
4. Bukti: Hasil analisis diubah menjadi bukti yang sah dan dapat dipakai. Penting untuk menjaga integritas bukti sepanjang proses. Bukti disajikan dengan objektif dan sesuai standar hukum.

Dengan Metode Forensik NIST, ahli forensik digital dapat memastikan analisis bukti digital dilakukan dengan benar dan menghasilkan informasi yang valid. Ini membantu mengungkap fakta dalam investigasi dengan cara yang ilmiah dan dapat diandalkan.

D. Root Explorer

Root Explorer adalah aplikasi file manajer yang dapat untuk mengakses semua system file pada ponsel

Android yang sudah di root dan dapat memodifikasi aplikasi sistem , file sistem, mengubah pengaturan default, dan bahkan menghapus data yang tidak diinginkan.

Pada perangkat Android, sistem operasi dan data dibatasi oleh izin akses. Ini berarti beberapa bagian sistem dan file-file tertentu tidak dapat diakses atau diubah oleh pengguna biasa. Namun, proses "rooting" menghapus pembatasan ini dengan memberikan akses "root" kepada pengguna.

E. Nox Player

Nox Player adalah salah satu emulator yang digunakkan sebagai smartphone Android atau clone dari smartphone Android. Para pengguna bisa menggunakkan emulator ini dengan akses internet pada laptop atau computer.

Nox Player bekerja dengan menciptakan lingkungan virtual yang meniru sistem Android. Ini mencakup sistem operasi Android lengkap, sehingga aplikasi dan game yang dijalankan pada Nox Player berperilaku seperti pada perangkat Android sungguhan.

F. Artefak

Artefak adalah benda apapun yang dibuat atau dapat dimodifikasi. Contoh artefak yang digunakkan pada Proyek Akhir ini adalah database dan file yang ada pada smartphone.

Artefak merujuk pada objek atau benda yang dibuat oleh manusia atau dapat diubah dengan tujuan tertentu. Dalam konteks proyek akhir, artefak adalah elemen-elemen yang menjadi bagian dari proyek dan digunakan untuk mencapai tujuan tertentu.

G. Android

Dalam era di mana perangkat bergerak layar sentuh seperti telepon pintar dan komputer tablet telah menjadi begitu integral dalam kehidupan sehari-hari, sistem operasi yang mampu mengimbangi kebutuhan mobilitas dan fungsionalitas menjadi krusial. Di sinilah peran Android sebagai sistem operasi berbasis Linux muncul dengan segala potensi dan inovasi yang dibawanya. Android, yang awalnya dikembangkan oleh Android, Inc. dengan dukungan finansial dari Google sebelum akhirnya diakuisisi pada tahun 2005 [10], telah membuktikan diri sebagai solusi yang tangguh dalam ekosistem perangkat bergerak layar sentuh.

Android tidak hanya sekadar sebuah sistem operasi, tetapi juga merupakan fondasi bagi berbagai perangkat, termasuk di antaranya Galaxy J6, yang mampu menghadirkan kemampuan dan kenyamanan berbagai aplikasi dalam satu wadah yang bersifat mobile. Namun, dalam pengembangannya, beberapa pengguna mungkin memilih untuk memberikan akses rooting pada perangkat Android tertentu, seperti Galaxy J6, untuk mengakses lapisan lebih dalam dari sistem operasi. Proses rooting ini memiliki implikasi yang signifikan terhadap kontrol dan kustomisasi perangkat, namun juga memunculkan pertanyaan terkait aspek keamanan dan stabilitas.

Dalam konteks ini, pemahaman tentang dasar-dasar Android, sejarah perkembangannya, dan konsep seperti rooting menjadi sangat penting. Artikel ini akan membahas lebih lanjut tentang sistem operasi Android, sejarahnya, serta dampak dan implikasi dari memberikan akses rooting pada perangkat Android. Dengan pemahaman yang lebih mendalam, pembaca akan dapat menjelajahi dunia Android dengan wawasan yang lebih luas dan kritis, mengenai bagaimana sistem operasi ini telah membentuk dan terus membentuk cara kita berinteraksi dengan perangkat bergerak dan teknologi sekitar kita.

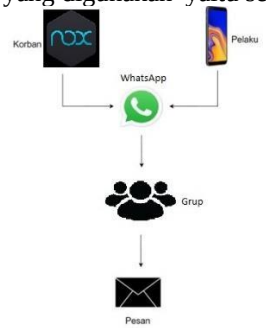
H. SQLite Browser

SQLite Browser adalah alat sumber terbuka, visual, dan berkualitas tinggi untuk membuat, merancang, dan mengedit file database yang kompatibel dengan SQLite. SQLite Browser sendiri berfungsi database SQl opensource yang menyimpan data ke file teks diperangkat android dengan database SQLite bawaan.

Dalam pengembangan aplikasi Android, alat ini berperan penting dalam membangun dan mengelola basis data yang efisien dan efektif, mendukung fungsionalitas aplikasi dengan menyimpan dan mengelola data dengan baik.

III. METODE

Pengujian pada Implementasi Forensik Digital di WhatsApp pada Sistem Operasi Android ini dilakukan dengan menggunakkan pengujian keseluruhan. Proses pengujian akan dilakukan terhadap semua kebutuhan fungsional yang telah dirancang sebelumnya. Sistem perancangan yang digunakan yaitu sebagai berikut :

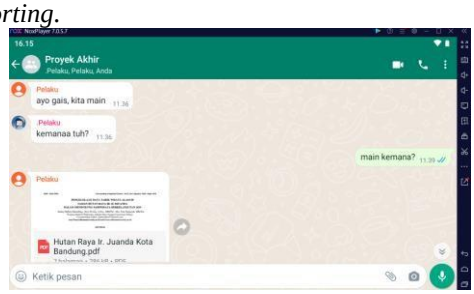


GAMBAR 1
perancangan Sistem untuk dilakukan pengujian

Pada gambar 1 *scenario* rencana pengujian kali ini ada 2 akun yaitu akun ‘Pelaku’ dan akun ‘Korban’. Kedua akun ini saling bertukar pesan melalu aplikasi WhatsApp. Pertukaran pesan grup oleh pelaku dan korban, lalu pelaku mengirimkan pesan penipuan untuk mengajak main korban berupa pesan teks, gambar, video, pesan suara dan file PDF. Barang bukti digital diambil melalui WhatsApp pada akun korban. Sehingga pada tahap analisisnya menggunakkan barang bukti digital dari akun korban untuk mengetahui isi pertukaran pesan, pesan yang di hapus dan informasi kontak yang pernah menghubungi korban.

IV. HASIL DAN PEMBAHASAN

Pada pengujian dengan metode NIST SP 800-86, terdapat empat unsur yang wajib untuk diuraikan pada proyek akhir ini yaitu proses koleksi, proses pemeriksaan, proses analisis, dan proses laporan / *reporting*.



GAMBAR 2
Menerima pesan File PDF

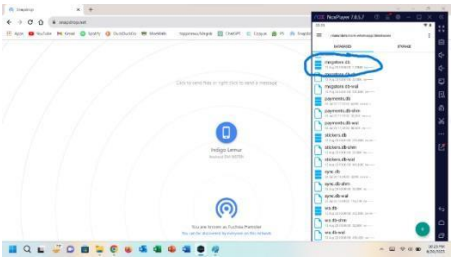
Pada gambar 2 adalah tampilan whatsapp korban yang sudah menerima pesan teks dan File PDF yang berformat "Media/WhatsApp Documents/Hutan Raya Ir. Juanda Kota Bandung.pdf "dari penyerang.

GAMBAR 3
Tampilan Serial Monitor Arduino Dari LoRa Receiver

Gambar 3 menampilkan visual antarmuka WhatsApp yang terbuka pada perangkat korban setelah berhasil menerima pesan video yang dikirim oleh penyerang. Dalam gambar tersebut, terlihat dengan jelas pesan video yang muncul di layar WhatsApp korban, memperlihatkan konten video yang telah masuk dari penyerang melalui serangan yang dilakukan. Tampilan gambar tersebut memberikan bukti yang jelas bahwa pesan video telah masuk dan menjadi bagian dari jejak serangan yang diarahkan oleh penyerang.

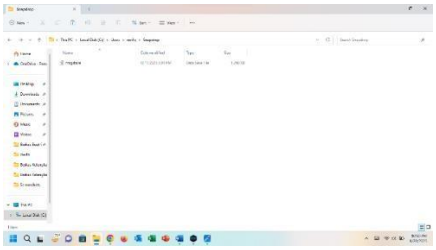
GAMBAR 4
Menerima pesan audio

Gambar 4 menampilkan secara visual antarmuka WhatsApp yang terbuka pada perangkat korban setelah berhasil menerima pesan audio yang dikirim oleh penyerang. Dalam gambar tersebut, terlihat dengan jelas pesan audio yang muncul di layar WhatsApp korban, memperlihatkan konten audio yang telah diterima dari penyerang melalui serangan yang dilakukan.



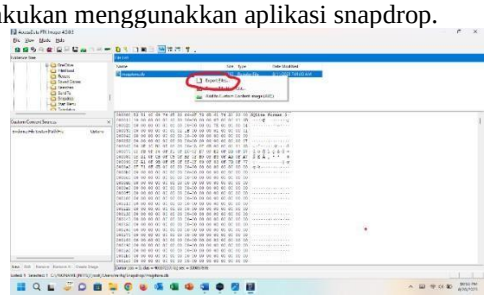
GAMBAR 5
Proses Transfer Untuk mendapatkan Barang Digital

Pada Gambar 5 tahap memindakan dengan cara mentransfer barang digital yaitu file msgstore.db menggunakkan aplikasi snapdrop melalui direktori root explorer /data/data/com.whatsapp/databases maka ketika folder databases terbuka disitu tertera file msgstore.db yang akan kita analisis melalui aplikasi SQL DB Browser.



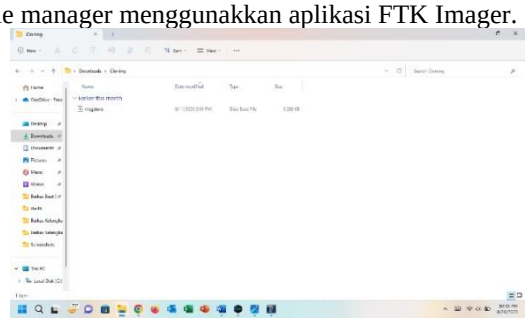
GAMBAR 6
Proses mendapatkan barang digital

Pada Gambar 6 adalah hasil transfer data yang dilakukan menggunakkan aplikasi snapdrop.



GAMBAR 7
Proses Cloning menggunakkan aplikasi FTK Imager

Pada gambar 7 adalah tahap melakukan cloning dari file manager menggunakkan aplikasi FTK Imager.

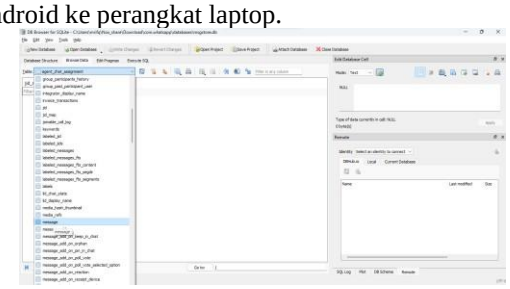


GAMBAR 8
Tampilan Hasil Cloning menggunakkan aplikasi FTK Imager

Pada Gambar 8 adalah hasil dari tahap cloning menggunakan aplikasi FTK Imager dan file tersebut untuk dilakukan proses analisis.

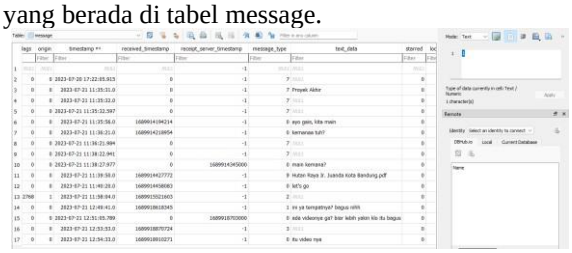
GAMBAR 9
Pengujian Hash

Fungsi Hash dalam autentikasi pesan, hash dirancang untuk melindungi pesan yang sudah di hash mengembalikan teks aslinya. Hash ini di cek menggunakan aplikasi yang bernama *command prompt* (CMD), FTK Imager dan Visual Studio Code. Hasil dari pengujian hash ini nilai md5 dan sha1 itu samayaitu sha-1 "3a04ab940b71d6a1e8df3a0e8da4829c8fd88126" dan md5 "ad93dadefd44b015cb1f67501c9abd21" sehingga hasil dari pengujian ini adalah dibuktikan bahwa barang bukti digital antara user tidak ada yang berubah semenjak proses duplikasi dari perangkat android ke perangkat laptop.



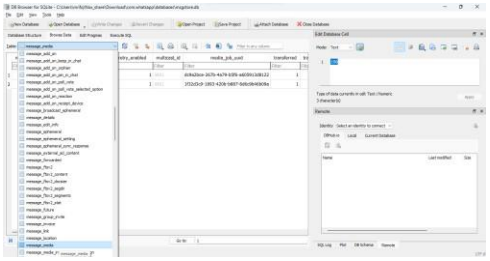
GAMBAR 10
Tampilan Table Databases untuk tampilan teks pesan

Setelah itu pesan teks akan tersimpan pada database whatsapp yang berada di file manager. Data pesan teks otomatis tersimpan di database msgstore.db yang berada di tabel message.



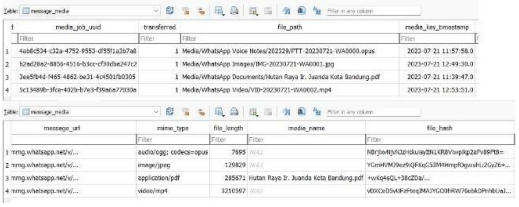
GAMBAR 11
Tampilan Databases untuk tampilan teks pesan

Pada gambar 11 menunjukkan bahwa pesan teks yang sudah di kirim oleh penyerang untuk korban telah tersimpan di dalam table text_data.



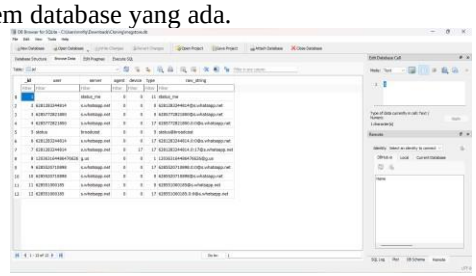
GAMBAR 12
Tampilan Database Untuk Mencari Pesan PDF, Gambar, Audio, dan Video

Setelah proses tersebut pesan file PDF, Gambar, Audio, Dan Video yang telah diterima akan diarsipkan dan tersimpan dengan aman dalam database WhatsApp yang terletak di file manager perangkat. Data pesan gambar tersebut secara otomatis akan tercatat dan tersimpan di dalam tabel message_media yang terdapat di database msgstore.db, memastikan integritas dan keterjangkauan data pesan gambar yang dikirim oleh penyerang kepada korban.



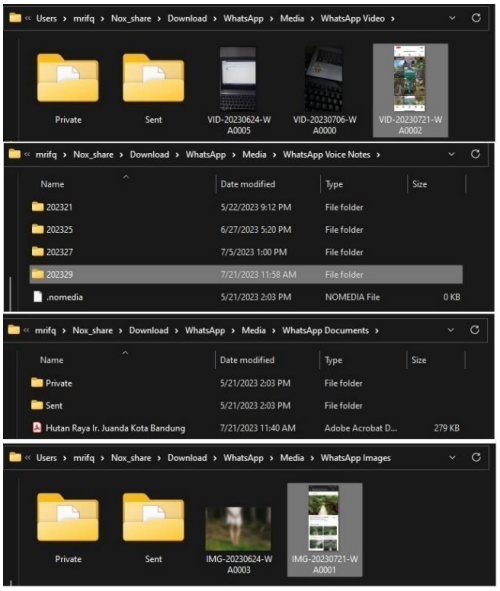
GAMBAR 13
Tampilan Data Pesan Gambar pada Tabel message_media

Pada gambar 13 terlihat dengan jelas bahwa pesan file PDF, gambar, audio, video berformat "Media/WhatsApp Documents/Hutan Raya Ir. Juanda Kota Bandung.pdf ", "Media/WhatsApp Images/IMG-20230721-WA0001.jpg", " Media/WhatsApp Voice Notes/202329/PTT-20230721-WA0000.opus", "Media/WhatsApp Video/VID-20230721-WA0002.mp4" yang telah berhasil dikirim oleh penyerang kepada korban telah sukses tersimpan di dalam database, memperkuat bukti bahwa data pesan gambar tersebut telah diarsipkan dengan baik dan dapat diakses melalui sistem database yang ada.



GAMBAR 14
Tampilan Data Sign Up

didapatkan bahwa untuk mengetahui data sign up user untuk diketahui username dan nomer telepon yang terdaftar pada aplikasi WhatsApp yaitu untuk membuka database tersebut menggunakan aplikasi SQLite Browser pada database msgstore.db yang ada pada table jid.



GAMBAR 15
Tampilan Gambar Bukti Digital

Pada gambar 15 didapatkan bahwa barang bukti yang dikirimkan oleh pelaku seperti file PDF, Gambar, Video dan Pesan Suara sudah tersimpan untuk di jadikan barang bukti cukup kuat di pengadilan.

V. KESIMPULAN

Dari hasil implementasi analisis forensik pada aplikasi whastapp, maka dapat disimpulkan:

1. Hasil Penerapan Metode Android forensic yang dilakukan barang bukti dapat ditemukan file mgstore.db terletak pada direktori yang sama dan diperlukan akses root pada Android agar file mgstore.db tersebut dapat ditemukan pada saat proses rooting diperlukan langkah yang sangat hati-hati jika terjadi kesalahan langkah pada saat rooting akan mengakibatkan bootloop atau mati total.
2. Setelah dilakukan investigasi, hasil identifikasi file barang bukti digital dan analisa telah berhasil dilakukan data tidak ada yang dirubah oleh user sehingga ketika identifikasi file berlangsung tidak ditemukan kejanggalan data yang diambil dari WhatsApp.

REFERENSI

[1] AKBP MP Nainggolan, “Minta Pelaku Hacker Nomor WHATSAPP-nya Segera Ditangkap, Relasinyapun Jadi Korban,” *Inakoran.com*, 2020. https://inakoran.com/akbp-mp-nainggolan-minta-pelaku-hacker-nomor-WhatsApp-nya-segera-ditangkap-relasinyapun-jadi-korban/p21724.

[2] Republik Indonesia, “Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,” *Lembaran Negara Republik Indones. Tahun 2016 Nomor 251*, pp. 1689–1699, 2016.

[3] R. F. Aushaf, S. J. I. Ismail, and ..., “Implementasi Forensik Digital Di Telegram Pada Sistem Operasi,” *eProceedings …*, vol. 7, no. 6, pp. 2767–2778, 2021, [Online].Available:https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/16975%0Ahttps://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/16975/16691

[4] G. B. Satrya, P. T. Daely, M. Arief, and M. A. Nugroho, “Digital Forensic Analysis of WHATSAPP Messenger on Android Devices Creative Capstone Design Using LoRa Wireless Communication View project Color Temperature Varying LED StreetLight and Control/Monitoring SW Development using Weather Big Data View project Digital Forensic Analysis of WHATSAPP Messenger on Android Devices,” *ieeexplore.ieee.org*, doi: 10.1109/ICTS.2016.7910263.

[5] Imam Riadi, “Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit,” Institute Of Justice (NIJ). JURTI, 3(1), 2579-8790.

[6] Feryan Lutfie Nafila, “Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android Menggunakan metode NIST,” dspace.uii.ac.id. https://dspace.uii.ac.id/handle/123456789/38688.

[7] C. Anglano, “Forensic analysis of whats app messenger on Android smartphones,” *Digit. Investig.*, vol. 11, no. 3, pp. 201–213, 2014, doi: 10.1016/j.diin.2014.04.003.

[8] Verihubs, “Ketahui Kegunaan Digital Forensik dan 4 Tahapannya.” Accessed: Feb. 14, 2023. [Online]. Available: https://verihubs.com/blog/digital-forensik/.