ANALISIS FORENSIK DIGITAL PADA PESAN WHATSAPP YANG TERENKRIPSI DENGAN PRETTY GOOD PRIVACY (PGP) MENGGUNAKAN FRAMEWORK DFRWS

Azis Fahrudin, Gufron Zaida Muflih
Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen
Jalan Raya Kutoarjo km 5 Jatisari, Kebumen, Indonesia
azizfahrudin43@gmail.com

ABSTRAK

Penyalahgunaan narkotika merupakan masalah serius yang mengancam masyarakat Indonesia, dengan peningkatan kasus sebesar 11,1% pada tahun 2022. Para pengedar narkoba semakin canggih dalam menggunakan teknologi komunikasi, terutama aplikasi WhatsApp dengan fitur enkripsi end-to-end, untuk melancarkan transaksi ilegal mereka. Penelitian ini bertujuan untuk menganalisis dan mengembalikan pesan WhatsApp yang terenkripsi dalam konteks investigasi kasus pengedaran narkoba menggunakan framework Digital Forensics Research Workshop (DFRWS). Metode yang digunakan adalah static forensic dengan tools MOBILedit Forensic Express dan Kleopatra untuk mengekstrak dan menganalisis data dari smartphone Android. Hasil penelitian menunjukkan bahwa framework DFRWS efektif dalam memulihkan dan menganalisis bukti digital berupa pesan terenkripsi PGP, private key, dan informasi kontak terkait transaksi narkoba. Hasil penelitian menunjukkan bahwa framework DFRWS efektif dalam memulihkan dan menganalisis bukti digital berupa mengekstraksi smartphone Redmi 6A milik tersangka, menemukan file Private Key dan file PGP Message, serta mengungkap detail transaksi narkoba. Temuan ini membuktikan bahwa teknik forensik digital modern dapat mengatasi tantangan enkripsi dalam investigasi kejahatan narkoba, memberikan kontribusi signifikan bagi penegakan hukum.

Kata kunci : *WhatsApp,* enkripsi *PGP,* forensik digital, *DFRWS framework, MOBILedit Forensic Express, Kleopatra*

1. PENDAHULUAN

Penyalahgunaan narkoba merupakan salah satu masalah utama yang membahayakan kehidupan manusia di mana pun, terutama di Indonesia. Penyalahgunaan dan peredaran gelap narkoba masih menimbulkan dampak buruk yang besar terhadap kesehatan, masyarakat, dan ekonomi [1].

Menurut Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika, narkotika didefinisikan sebagai obat kimia atau sintetis yang berasal dari tanaman atau bukan tanaman yang mempunyai kemampuan untuk mengubah kesadaran, menimbulkan rasa tidak sadar, mengurangi atau menghilangkan rasa nyeri, atau menimbulkan ketergantungan [2]**.**

Kasus penyalahgunaan narkoba di Indonesia mengalami peningkatan, berdasarkan data Badan Narkotika Nasional (BNN). Kasus penyalahgunaan narkoba meningkat 11,1% dari tahun 2021 yang hanya 766 kasus menjadi 851 kasus pada tahun 2022. Angka penyalahgunaan narkoba turun dari 1,95% pada tahun 2022 menjadi 1,73% pada tahun 2023. Masalah ini tetap perlu mendapat perhatian serius [3].

Menurut jajak pendapat nasional yang dilakukan pada tahun 2023, sekitar 3,3 juta penduduk Indonesia berusia antara 15 dan 64 tahun mengonsumsi narkoba. Yang lebih memprihatinkan adalah peningkatan signifikan kecanduan narkoba di kalangan penduduk berusia 15 hingga 24 tahun [4].

Perdagangan narkoba telah berkembang menjadi usaha terlarang yang sangat menguntungkan dan berbahaya dalam skala global. Kantor PBB untuk Narkoba dan Kejahatan (UNODC) merilis Laporan Narkoba Dunia terbarunya hari ini, yang memperkirakan bahwa 269 juta orang menggunakan narkoba secara global pada tahun 2018 dan lebih dari 35 juta orang mengalami gangguan penggunaan narkoba [5].

BNN melaporkan bahwa jaringan internasional yang semakin kompleks dan beragam adalah sumber sebagian besar narkoba yang beredar di Indonesia. BNN menemukan 49 jaringan narkoba pada tahun 2022, termasuk 23 jaringan internasional dan 26 jaringan nasional [3].

Kemajuan teknologi informasi dan komunikasi (TIK) telah membawa perubahan besar dalam kontak manusia dan penyebaran informasi. Teknologi informasi telah menjadi bagian penting dalam kehidupan sehari-hari. mempengaruhi berbagai aspek termasuk pendidikan, bisnis, pemerintahan, dan interaksi sosial. Dalam konteks komunikasi digital, aplikasi *instan messaging* (IM) telah menjadi salah satu inovasi yang paling berpengaruh. Salah satu Platformnya yang paling populer adalah WhatsApp [6].

Meski sangat bermanfaat sebagai alat komunikasi, aplikasi WhatsApp memiliki efek negatif yang tidak dapat diabaikan. Kecanggihan perangkat digital saat ini juga menyebabkan kejahatan semakin canggih dengan berbagai cara yang belum pernah terlihat sebelumnya, seperti peredaran narkoba [7].

Dengan menggunakan enkripsi pesan, mereka dapat berkomunikasi secara tersembunyi, melakukan

transaksi, dan mengatur operasi mereka dengan lebih baik dan aman. Penyalahgunaan fitur-fitur WhatsApp ini menciptakan tantangan signifikan bagi penegak hukum dalam menginvestigasi dan memberantas jaringan narkoba. Enkripsi end-to-end, meskipun penting untuk privasi pengguna pada umumnya, menjadi hambatan dalam pengumpulan bukti digital. Hal ini mendorong perlunya pengembangan teknik digital forensik yang lebih canggih untuk menganalisis dan membuka pesan terenkripsi dalam konteks penyelidikan kasus narkoba yang sah secara hukum.

Penggunaan komputer untuk mengumpulkan bukti untuk proses peradilan dikenal sebagai forensik digital (pro justice) dan memerangi penjahat dengan bukti digital [8].

Di era digital saat ini, ketika kejahatan dunia maya meningkat dan sulit diberantas, sektor ini menjadi semakin penting. Subbidang ilmu forensik yang disebut "forensik digital" berkaitan dengan pengumpulan, analisis, dan tampilan bukti digital berbasis komputer, tablet, atau perangkat elektronik lainnya [9].

Dengan teknik dan alat yang tepat, para ahli forensik dapat menemukan jejak digital yang mungkin telah dihapus atau disembunyikan. Pihak berwenang dapat menemukan bukti bahwa pelaku mungkin telah mencoba menghapusnya dengan menggunakan forensik digital [10].

Dalam prosesnya, tidak hanya perangkat komputer yang diperhatikan, tetapi juga berbagai perangkat yang mampu menyimpan dan memproses data digital, seperti tablet, ponsel pintar, perangkat penyimpanan *eksternal*, serta perangkat *Internet of Things* (IoT) [11].

Hal ini menunjukkan bahwa digital forensik harus mencakup berbagai teknologi untuk mendapatkan gambaran lengkap dari bukti yang ada. Menggunakan analisis komputer atau perangkat lunak khusus, forensik digital juga menyelidiki metode untuk mengumpulkan, memverifikasi, menganalisis, menafsirkan, mendokumentasikan, dan menyajikan bukti digital [12].

Untuk memastikan *integrita*s dan *validitas* bukti digital yang dikumpulkan, para praktisi forensik digital menggunakan berbagai *framework* yang telah distandarisasi. Penggunaan *framework* ini tidak hanya membantu dalam menjaga kualitas bukti, tetapi juga memberikan panduan dalam menjalankan setiap tahap *investigasi* [13].

Dengan menggunakan *framework*, proses *investiga*si digital dilakukan secara sistematis, dapat direproduksi, dan memenuhi standar hukum untuk diterima di pengadilan. Dalam konteks investigasi kasus narkoba yang melibatkan aplikasi komunikasi terenkripsi, *framework* ini memberikan struktur untuk menangani tantangan teknis dan hukum yang muncul dari penggunaan teknologi canggih oleh pelaku kejahatan. Implementasi *framework* digital forensik dalam investigasi kasus narkoba yang melibatkan WhatsApp memerlukan pendekatan yang hati-hati untuk mengatasi tantangan *enkripsi end-to-end* dan sifat volatile dari data komunikasi digital. Metode yang digunakan harus cukup fleksibel untuk menanggapi dinamika teknologi yang terus berkembang. Suatu kerangka kerja yang disebut Lokakarya Penelitian Forensik Digital (DFRWS) dapat digunakan untuk prosedur forensik telepon pintar.

Tujuan penelitian ini adalah menggunakan metode DFRWS untuk melakukan forensik digital pada pengembalian dan menganalisis pesan WhatsApp sebagai barang bukti digital suatu kasus kejahatan dalam konteks kasus pengedaran narkoba dimana barang bukti digital telah di enkripsi menggunakan enkripsi *Pretty Good Privacy* (PGP). Diharapkan bahwa penelitian ini akan menawarkan saran untuk penciptaan metode forensik digital yang lebih kompleks dan taktik penyelidikan yang relevan. serta meningkatkan kesadaran akan pentingnya digital forensik dalam memberantas kejahatan narkoba.

2. TINJAUAN PUSTAKA

2.1. Digital Forensik

Digital forensik adalah salah satu cabang dari ilmu forensik yang berfokus pada penyelidikan, analisis, dan pemulihan bukti-bukti terkait pelanggaran hukum atau tindak kejahatan yang melibatkan perangkat digital atau media digital [14].

Bidang ini mencakup berbagai teknik dan metode untuk mengidentifikasi, mengumpulkan, memeriksa, dan memelihara integritas bukti digital agar dapat digunakan dalam proses hukum.

2.2. Bukti Digital

Data yang disimpan, diproses, atau dikirimkan melalui perangkat komputer maupun media digital yang dapat mendukung atau menentang teori tentang bagaimana suatu pelanggaran hukum terjadi disebut bukti digital [15].

Bukti digital merupakan salah satu elemen kunci dalam proses investigasi di bidang digital forensik, karena dapat memberikan informasi penting untuk mengungkap fakta-fakta terkait sebuah kasus.

2.3. WhatsApp

WhatsApp adalah aplikasi pesan instan yang dapat digunakan pada smartphone [16].

WhatsApp menawarkan berbagai fitur yang menjadikannya pilihan utama untuk komunikasi digital. Diantaranya fitur berbagi berbagai jenis berkas seperti dokumen, gambar, dan video, dan fungsi enkripsi ujung ke ujung menjamin bahwa hanya pengirim dan penerima yang dapat melihat file, panggilan, dan pesan yang ditransfer, menjaga privasi pengguna sekaligus menawarkan kenyamanan [17]

2.4. Digital Forensic Research Workshop (DFRWS)

Metode DFRWS (Digital Forensics Research Workshop) adalah framework yang dirancang untuk

memandu proses forensik digital secara sistematis dan terorganisir. Metode ini berfungsi untuk memfasilitasi proses pengumpulan barang bukti dan merekam informasi yang diperlukan, serta menggunakan data dengan mekanisme terpusat untuk meningkatkan efisiensi dan akurasi [18].

Topik yang dibahas dalam Lokakarya Penelitian Forensik Digital meliputi identifikasi, pelestarian, pengumpulan, analisis, dan presentasi (DFRWS) [19]

2.5. Static Forensic

Metode forensik statis memiliki keunggulan dalam mengungkap informasi dari bukti digital yang tidak aktif atau telah dihapus setelah kejadian [20].

Karena sifatnya yang tidak interaktif, metode ini lebih cocok digunakan ketika perangkat dapat diakses tanpa gangguan. Forensik statis menggunakan teknik konvensional yang menggunakan gambar sedikit demi sedikit untuk memproses data elektronik [21].

Setiap byte data asli ditangkap dengan cara ini, menjamin tidak ada informasi yang hilang selama proses pengumpulan. Forensik statis dilakukan pada media penyimpanan yang tidak terhubung ke jaringan internet, sementara forensik langsung dilakukan secara real-time ketika proses transaksi data berlangsung di internet [22].

2.6. Enkripsi

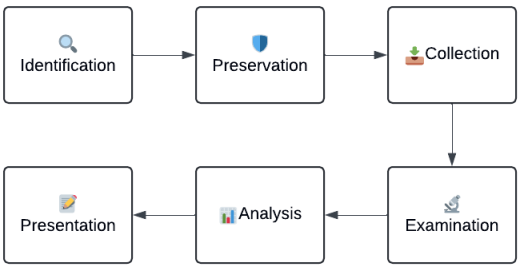
Enkripsi adalah komponen penting dalam keamanan komputer dan sistem informasi, yang bertujuan untuk melindungi data dari akses yang tidak sah dengan cara mengubah data asli yang dapat dibaca manusia (plaintext) menjadi bentuk terenkripsi yang tidak dapat dipahami tanpa kunci dekripsi yang benar (ciphertext) [23].

Proses ini melibatkan penggunaan algoritma enkripsi, yaitu serangkaian instruksi matematika yang dirancang untuk mengacak data, dan kunci enkripsi, yang bertindak sebagai parameter untuk mengontrol bagaimana algoritma tersebut bekerja.

3. METODE PENELITIAN

3.1. Digital Forensic Research Workshop (DFRWS)

Dalam penyelidikan ini, kerangka kerja yang dibuat oleh Lokakarya Penelitian Forensik Digital (DFRWS) digunakan, dan teknik forensik statis untuk melaksanakan investigasi forensik digital secara metodis. Sementara itu, metode *static forensic* memungkinkan analisis dilakukan tanpa mengubah kondisi asli perangkat, menjaga integritas data selama proses investigasi berlangsung. *Framework* DFRWS seperti pada gambar 1.



Gambar 1. Tahapan DFRWS

a. *Identification* (Identifikasi)
   Awal dari proses investigasi digital forensik yang bertujuan untuk menemukan dan mengumpulkan semua yang diperlukan untuk melakukan penyedikan dan pencarian barang bukti digital.
b. *Preservation* (Pemeliharaan)
   Menjaga integritas bukti digital yang berarti menjaga dan memelihara bukti dalam bentuk aslinya untuk menghindari perubahan atau kerusakan.
c. *Collection* (Pengumpulan)
   Pada tahap ini, barang bukti digital yang telah diidentifikasi sebelumnya dikumpulkan.
d. *Examination* (Pemeriksaan)
   Memverifikasi bukti yang telah dikumpulkan sebelumnya.
e. *Analysis* (Analisis)
   Melakukan penentuan tentang dimana data tersebut dihasilkan oleh siapa data tersebut dihasilkan, dan bagaimana data tersebut dihasilkan
f. *Presentation* (Presentasi)
   Tahap terakhir adalah menyajikan informasi dari hasil investigasi dan analisis.

3.2. Tools

MOBILedit Forensic adalah paket perangkat lunak yang menggabungkan *ekstraksi* ponsel, analisis data, dan pembuatan laporan dalam satu solusi. Dengan *MOBILedit Forensic*, pemeriksaan dapat dilakukan pada sebagian besar perangkat seluler, memungkinkan pemulihan dan analisis berbagai jenis data, termasuk pesan teks, kontak, foto, Termasuk lebih banyak file. Aplikasi ini juga dapat menghasilkan laporan dalam berbagai format tambahan, termasuk Excel, HTML, dan PDF, yang dapat disesuaikan dengan berbagai kebutuhan. *MOBILedit Forensic* menjadi alat yang sangat berguna bagi para profesional forensik digital [24].

Kleopatra adalah *tools* manajemen kunci dan *enkripsi* yang merupakan bagian dari suite perangkat lunak Gpg4win, yang dirancang untuk menangani enkripsi dan tanda tangan digital menggunakan *OpenPGP*. Pengguna dapat dengan mudah mengelola kunci enkripsi dan menjalankan tugas terkait keamanan data lainnya dengan bantuan antarmuka pengguna grafis (GUI) alat ini [25]

3.3. Enkripsi PGP

PGP, atau Pretty Good Privacy Protocol, menggunakan skema kunci publik dan privat. Materi akan dienkripsi dan diubah menjadi ciphertext sebelum dikirim sebagai komunikasi plaintext. Untuk menguraikan teks terenkripsi, pengirim harus memiliki kunci privat penerima. Jika tidak, dekripsi akan gagal dan *ciphertext* tidak dapat didekripsi.

3.4. Kebutuhan Alat

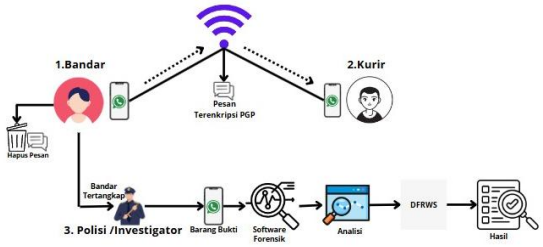
Perangkat keras, perangkat lunak, dan peralatan forensik digunakan dalam investigasi ini. Rincian instrumen dan perlengkapan yang digunakan ditunjukkan pada Tabel 1.

Tabel 1. Alat dan bahan

No	Nama	Keterangan
1	Laptop Lenovo Ideapad 330	Hardware
2	Smartphone Android Redmi 6A	Hardware
6	Windows 10 pro	Sistem Operasi
7	Mobiledit Forensik Express Pro versi 7,4,1,21502(64bit)	Tool forensik
8	Kleopatra versi 4.3.1	Tool

Penelitian ini memanfaatkan kombinasi perangkat keras dan lunak untuk melakukan investigasi forensik pada perangkat tersangka. Laptop Lenovo Ideapad 330 dengan prosesor AMD A4-9125 dan RAM 8GB cukup untuk menjalankan perangkat lunak analisis. *Mobiledit Forensic Express Pro* digunakan untuk mengekstrak data dari ponsel Android Redmi 6A, sementara Kleopatra digunakan untuk mengelola kunci enkripsi PGP dan mencoba mendekripsi pesan yang telah dihasilkan di WhatsApp.

3.5. Skenario Kasus



Gambar 2. Tahapan skenario

Dalam skenario yang ditampilkan pada Gambar 2, setiap tahapan dijelaskan secara terperinci sebagai berikut :

a. Bandar menggunakan *smartphone* dan aplikasi WhatsApp untuk mengirimkan pesan terenkripsi menggunakan *PGP (Pretty Good Privacy)* kepada kurir melalui jaringan internet. Pesan berisi perintah pengiriman paket narkoba. Setelah pesan berhasil dikirim, bandar melakukan penghapusan pesan dari perangkatnya dengan tujuan menghilangkan jejak atau bukti komunikasi.
b. Kurir menerima pesan rahasia yang dikirim oleh bandar narkoba melalui aplikasi WhatsApp di *smartphone* miliknya. Pesan yang diterima tetap dalam bentuk terenkripsi, Ini hanya dapat dibaca setelah melalui prosedur dekripsi dengan kunci PGP yang relevan.
c. Pihak kepolisian atau investigator melakukan operasi tangkap tangan terhadap bandar narkoba. Dalam operasi ini, polisi juga menyita *smartphone* milik bandar yang mungkin mengandung informasi penting, untuk analisis forensik digital lebih lanjut terhadap barang bukti tersebut menggunakan *tools Mobiledit Forensic Express Pro* dengan metodologi *DFRWS (Digital Forensic Research Workshop).*

4. HASIL DAN PEMBAHASAN

Hasil dari proses investigasi untuk menemukan barang bukti kejahatan pada skenario kasus penelitian, menggunakan *framework* DFRWS yang meliputi tahapan *identification*, *collection*, *preservation*, *examination*, *analysis*, dan *presentation*, adalah sebagai berikut :

4.1. *Identification*

Pada langkah ini, barang bukti dicari dan dikumpulkan yang berkaitan dengan skenario kasus yang ada. Ponsel pintar Redmi 6A yang ditemukan sebagai barang bukti dalam penelitian ini diduga digunakan untuk mengedarkan narkotika melalui aplikasi WhatsApp. Gambar 3. Merupakan barang bukti *smartphone* Redmi 6A.

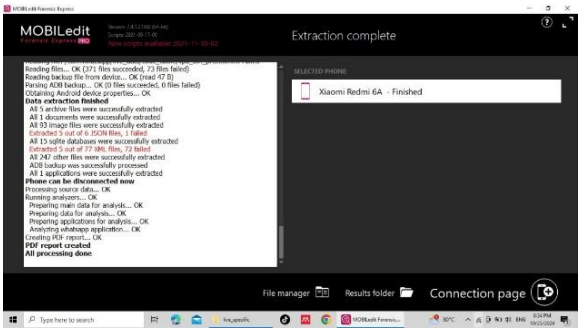
Gambar 3. Barang Bukti *Smartphone*

4.2. *Preservation*

Tahap *preservation* atau pemeliharaan ini dilakukan untuk menjaga integritas bukti digital dari *smartphone* tersangka dengan menerapkan serangkaian prosedur dan protokol keamanan yang ketat. Perangkat segera diisolasi dari jaringan internet dengan mengaktifkan mode pesawat untuk mencegah perubahan atau penghapusan data lebih lanjut, jika dilakukan oleh orang yang tidak berwenang dengan sengaja atau tidak sengaja. Dengan menghindari tindakan yang dapat membahayakan atau membahayakan integritas data, fase pemeliharaan ini menjamin validitas bukti dan membantah tuduhan pemalsuan bukti digital, seperti *interferensi* elektromagnetik, kerusakan fisik, atau manipulasi data yang tidak sah.

4.3. *Collection*

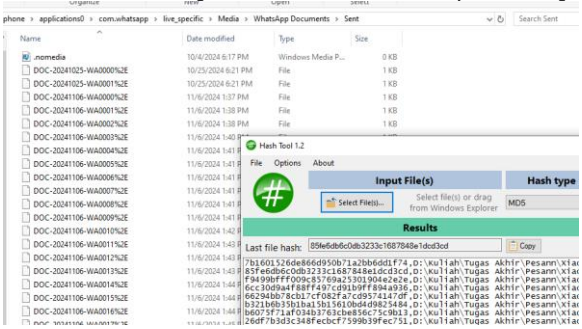
Pada tahapan ini dilakukan *identifikasi* sumber data dan bukti digital dalam aplikasi WhatsApp. Menggunakan telepon pintar untuk menangkap bukti digital sangatlah berisiko karena data dapat rusak atau terhapus, sehingga tidak dapat dibaca [8]. Tahapan menggunakan perangkat lunak forensik untuk membuat salinan digital (*image file*)atau *backup* dari data dalam perangkat yang mungkin berhubungan dengan transaksi narkoba. Proses akusisi dilakukan dengan *MOBILedit Forensic Express*. Sebelum proses pemeriksaan dan analisis dimulai, langkah ini memastikan bahwa semua bukti potensial tersedia. Pada Gambar 4**.** MOBILedit Forensic Express digunakan dalam prosedur akuisisi.



Gambar 4. Proses Akusisi Data Menggunakan *Mobiledit Forensic Express*

4.4. *Examination*

Tahap *examination* dilakukan dengan menelusuri dan memeriksa semua data yang telah dikumpulkan untuk menemukan bukti yang *relevan*. Riwayat pesan di WhatsApp diperiksa untuk mendeteksi pola komunikasi dengan kurir. Proses selanjutnya yaitu ekstraksi dari *file backup*, yang bertujuan untuk menguraikan semua data yang ada dari *smartphone* agar dapat *dianalisis* lebih lanjut. Melalui tahap *ekstraksi* ini, berbagai jenis *file* yang tersimpan di dalam perangkat, Misalnya, file teks obrolan, file kontak, file gambar, file audio, file video, dan file dokumen, disusun dan dikumpulkan secara sistematis. Alat hashing digunakan untuk verifikasi bukti digital, memastikan bahwa bukti tersebut tidak berubah. Untuk membantu tim forensik melacak informasi spesifik yang mungkin menjadi bukti penting dalam penyelidikan, hasil ekstraksi sangat penting. Pada Gambar 5. menampilkan hasil ekstrasi dari *file backup.*



Gambar 5. Hasil Ekstrasi *Backup File*

Pada Tabel 2. adalah hasil ekstraksi dan validasi barangbukti. Hasil ekstraksi dan validasi menunjukkan bahwa ditemukanya *file Privat Key* dan *file PGP Message* yang disimpan di direktori aplikasi WhatsApp. *File Privat Key*, dengan hash unik, dibutuhkan untuk mendekripsi pesan terenkripsi *(PGP Message)* yang memiliki hash berbeda, menandakan bahwa *file* tersebut belum dimodifikasi dan tetap asli. Semua file ini menjadi barang bukti penting karena berisi informasi yang relevan dalam penyelidikan dan dapat dibuka hanya jika kunci *privat* tersedia.

Tabel 2. Hasil Ektrasi dan Validasi Barang Bukti

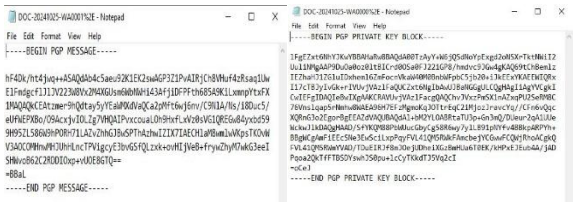
Barang Bukti	***Directory***	***File Name***	***Hashing File***
Privat Key	phone_files\phone\applications0\ com.whatsapp\live_specific\ Media\WhatsApp Documents\Sent	DOC-20241025-WA0000%2E	85fe6db6c0db3233c1687848e1dcd3cd
PGP Massage	phone_files\phone\applications0\ com.whatsapp\live_specific\ Media\WhatsApp Documents\Sent	DOC-20241106-WA0000%2E	f9499bfff009c85769a25301904e2e2e
PGP Massage	phone_files\phone\applications0\ com.whatsapp\live_specific\ Media\WhatsApp Documents\Sent	DOC-20241106-WA0001%2E	6cc30d9a4f88ff497cd91b9ff894a936
PGP Massage	phone_files\phone\applications0\ com.whatsapp\live_specific\ Media\WhatsApp Documents\Sent	DOC-20241106-WA0002%2E	66294bb78cb17cf082fa7cd9574147df

4.5. *Analysis*

Tahap analisis melibatkan pemeriksaan mendalam dan sistematis terhadap data yang relevan dengan kasus, mengikuti prosedur dan protokol forensik yang telah ditetapkan secara ketat untuk menjamin *validitas* temuan. Tim forensik mengidentifikasi pola komunikasi yang mencurigakan antara tersangka dan pihak lain yang diduga terlibat

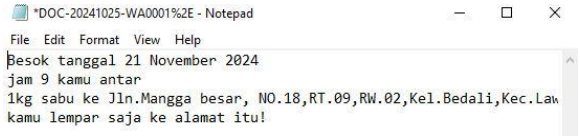
dalam transaksi narkoba, dengan memperhatikan frekuensi komunikasi, waktu pengiriman pesan, dan konten yang dipertukarkan. Untuk menciptakan bukti digital yang kuat dan dapat dipertanggungjawabkan secara hukum, setiap materi yang ditemukan selama tahap pemeriksaan dihubungkan secara sistematis berdasarkan metodologi penelitian dan studi kasus.

Pada tahap analisis yang dilakukan secara mendalam, tim forensik berhasil menemukan dua *file* dokumen yang menjadi bukti penting dan sangat signifikan dalam pengungkapan kasus ini, *yaitu private key* dan pesan yang dienkripsi menggunakan protokol *PGP (Pretty Good Privacy). Private key* yang ditemukan ini memainkan peran krusial karena memungkinkan proses dekripsi pesan terenkripsi sehingga konten asli dapat diakses dan dianalisis lebih lanjut oleh tim investigasi. Gambar 6. menunjukkan isi detail dari *file privat key* dan pesan yang terenkripsi menggunakan protokol PGP.



Gambar 6. *Privat key* dan *Message* yang terenkripsi PGP

Berdasarkan Gambar 6. Barang bukti digital yang diperoleh adalah dokumen yang berisi pesan terenkripsi menggunakan protocol *PGP (Pretty Good Privacy).* pesan enkripsi yang dikirim 20 pesan dengan 1 kunci privat, yang di temukan *tools MOBILedit Forensik Exspres* 20 pesan terenkripsi dan 1 kunci *privat*. Tingkat keberhasilan secara keseluruhan adalah 100%. Selanjutnya pesan terenkripsi melalui proses dekripsi yang dilakukan dengan menggunakan *private key* yang ditemukan, pesan terenkripsi tersebut berhasil diuraikan dan mengungkap rincian transaksi yang sangat detail dan komprehensif, termasuk spesifikasi jenis narkoba yang diperdagangkan, jumlah atau kuantitas barang terlarang yang ditransaksikan, koordinat lokasi, serta waktu pengiriman yang telah direncanakan dengan cermat. Informasi yang berhasil didekripsi ini memberikan bukti konkret dan tidak terbantahkan yang secara signifikan memperkuat dugaan keterlibatan tersangka dalam jaringan aktivitas penjualan narkoba ilegal dan membantu tim investigasi dalam menyusun kronologi peristiwa secara detail dan terstruktur dalam kasus ini. Hasil pesan yang berhasil didekripsi secara lengkap ditunjukkan pada Gambar 7. yang memperlihatkan informasi asli antara tersangka dengan jaringannya.



Gambar 7. Hasil *decrypt* pesan

Selain *private key* dan pesan terenkripsi PGP yang berhasil ditemukan, tim forensik juga mengidentifikasi nomor telepon yang menjadi tujuan pengiriman pesan-pesan tersebut. Nomor telepon ini menjadi bukti vital yang memperjelas struktur dan jaringan komunikasi tersangka serta memberikan bukti tambahan yang dapat menghubungkan tersangka dengan para kurir narkoba yang terlibat dalam jaringan peredaran tersebut. Temuan studi forensik mampu memberikan rincian lengkap tentang nomor telepon tujuan yang digunakan dalam percakapan terenkripsi, seperti yang terlihat pada Gambar 8.

Gambar 8. Informasi nomor tujuan

4.5. *Presentation*

Pada tahap presentasi, dilakukan laporan mengenai informasi yang diperoleh dari hasil analisis forensik berdasarkan barang bukti yang ditemukan dalam proses investigasi. Smartphone Android Redmi 6A yang menjadi sumber bukti utama penelitian ini, tim investigasi telah melakukan serangkaian proses forensik digital yang mengikuti prosedur dan metodologi standar sesuai dengan *framework Digital Forensic Research Workshop (DFRWS)*. Proses akuisisi data dilaksanakan menggunakan tools forensik MOBILedit Forensik Express, menghasilkan file *backup* yang komprehensif dengan nama file "Xiaomi Redmi 6A (2024-10-25 18h25m43s)". File backup ini menjadi sumber data utama yang memuat seluruh informasi digital yang berhasil diekstrak dari perangkat tersangka, termasuk data-data yang telah dihapus namun masih dapat dipulihkan. Tabel 3 menampilkan ringkasan informasi barang bukti yang didapat dari hasil analisis *forensic.*

Tabel 3. Ringkasan Laporan Informasi

Barang Bukti	Directory	Informasi	Keterangan
Redmi 6A	-	Smartphone Android	ditemukan
Nomor handphone Tujuan	phone/applications0/com.whatsapp/live_data/databases/wa.db : 0x814ce (Table: wa_contacts)	+6281236303243	ditemukan
Nama Akun	phone/applications0/com.whatsapp/live_data/databases/wa.db : 0x814ce (Table: wa_contacts)	AZIS	ditemukan

Barang Bukti	Directory	Informasi	Keterangan
File Privat Key	phone\applications0\com.whatsapp\live_specific\Media\WhatsApp Documents\Sent	DOC-20241025-WA0000%2E	ditemukan
File Pesan Rahasia	phone\applications0\com.whatsapp\live_specific\Media\WhatsApp Documents\Sent	DOC-20241025-WA0001%2E	Ditemukan dan berhasil dideskripsikan

5. KESIMPULAN

Melalui analisis forensik digital aplikasi WhatsApp, penelitian ini secara efektif menggambarkan kemanjuran metodologi Digital Forensics Research Workshop (DFRWS) dalam mengidentifikasi kasus perdagangan narkoba. Framework DFRWS terbukti menyediakan pendekatan sistematis yang efektif dalam menganalisis dan memulihkan pesan WhatsApp yang terenkripsi, mulai dari identifikasi hingga presentasi bukti digital.

Dalam penelitian ini, kombinasi perangkat lunak MOBILedit Forensic Express dan Kleopatra berhasil mengekstrak data dari perangkat Android Redmi 6A milik tersangka bernama AZIS. Proses investigasi menghasilkan temuan kunci berupa satu file Private Key dengan hash unik "85fe6db6c0db3233c1687848e1dcd3cd" dan tiga file PGP Message yang masing-masing memiliki hash berbeda, menandakan keaslian data yang ditemukan.

Digital forensic ini berhasil mendekripsi 20 pesan terenkripsi dengan tingkat keberhasilan 100%, mengungkap detail transaksi narkoba yang komprehensif. Bukti digital yang diperoleh mencakup nomor telepon tujuan +6281236303243, yang memberikan informasi penting tentang jaringan komunikasi tersangka. Proses dekripsi menghasilkan informasi mendetail tentang transaksi, termasuk jenis narkoba, kuantitas, lokasi pengiriman, dan waktu transaksi yang direncanakan.

Framework DFRWS terbukti dapat diimplementasikan secara efektif untuk kasus-kasus yang melibatkan aplikasi pesan instan terenkripsi, memberikan pendekatan sistematis dalam pengumpulan dan analisis bukti digital. Temuan penelitian ini memperkuat penerapan teknik forensik digital dalam penegakan hukum, khususnya dalam menghadapi kasus kejahatan yang memanfaatkan teknologi enkripsi.

Metodologi yang diterapkan membuktikan bahwa teknik forensik modern mampu mengimbangi perkembangan teknologi yang digunakan oleh pelaku kejahatan. Keberhasilan dalam mendekripsi dan menganalisis pesan rahasia menjadi bukti konkret kemampuan investigasi digital dalam mengungkap aktivitas ilegal yang tersembunyi di balik lapisan enkripsi canggih.

DAFTAR PUSTAKA

[1] E. Dewi, K. Ulfa, and S. Safirussalim, "STRATEGI BADAN NARKOTIKA NASIONAL DALAM PENANGGULANGAN NARKOTIKA DI MASA PANDEMI COVID-19 DI INDONESIA," *Al-Ijtima`i: International Journal of Government and Social Science*, vol. 7, no. 2, pp. 143–156, Apr. 2022, doi: 10.22373/JAI.V7I2.1659.

[2] R. Saragih and M. F. E. Simanjuntak, "Penegakan Hukum Terhadap Penyalahgunaan Narkotika Di Indonesia," *Journal of Education, Humaniora and Social Sciences (JEHSS)*, vol. 4, no. 1, pp. 98–105, Jun. 2021, doi: 10.34007/jehss.v4i1.590.

[3] "BNN Catat 851 Kasus Narkoba di Indonesia pada 2022." Accessed: Oct. 20, 2024. [Online]. Available: https://dataindonesia.id/varia/detail/bnn-catat-851-kasus-narkoba-di-indonesia-pada-2022

[4] "HANI 2024: Masyarakat Bergerak, Bersama Melawan Narkoba Mewujudkan Indonesia Bersinar." Accessed: Oct. 20, 2024. [Online]. Available: https://bnn.go.id/hani-2024-masyarakat-bergerak-bersama-melawan-narkoba-mewujudkan-indonesia-bersinar/

[5] "UNODC World Drug Report 2020: Global drug use rising; while COVID-19 has far reaching impact on global drug markets." Accessed: Oct. 20, 2024. [Online]. Available: https://www.unodc.org/unodc/press/releases/2020/June/media-advisory---global-launch-of-the-2020-world-drug-report.html

[6] I. W. Putra, A. Suharso, and C. Rozikin, "Akuisisi Bukti Digital Dan Deteksi Keaslian Citra Pada Whatsapp Menggunakan Metode NIST Dan ELA," *Jurnal Sains Komputer & Informatika (J-SAKTI)*, vol. Volume 5, Sep. 2021.

[7] K. A. Latif, R. Hammad, T. T. Sujaka, K. Marzuki, and A. S. Anas, "Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method With ACPO Standard," *International Journal of Information System & Technology Akreditasi*, vol. 5, no. 3, pp. 331–338, 2021.

[8] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 2, p. 1263, Apr. 2022, doi: 10.30865/mib.v6i2.3946.

[9] A. S. Rido and F. Fachri, "IDENTIFIKASI BUKTI DIGITAL WHATSAPP PADA SISTEM OPERASI PROPRIETARY MENGGUNAKAN LIVE FORENSICS," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 2, pp. 1043–1051, Jun. 2024, doi: 10.29100/jipi.v9i2.5238.

[10] I. A. Plianda and R. Indrayani, "Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 1, p. 500, Jan. 2022, doi: 10.30865/mib.v6i1.3487.

[11] M. Rifqi, S. J. I. Ismail, and M. F. Rizal, "Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute Of Standard And Technology (Nist Sp 800-86)," Dec. 2023.

[12] Y. Prawira and Samsudin, "Live Forensics Analysis Of Malware Identified Email Crimes To Increase Evidence Of Cyber Crime," *Jurnal Teknologi Informasi dan Komunikasi*, vol. 13, Nov. 2022, doi: 10.31849/digitalzone.v13i2.11570.

[13] "Tahapan dan Teknik Forensik Digital dalam Dunia Maya - IDS Digital College." Accessed: Oct. 20, 2024. [Online]. Available: https://ids.ac.id/tahapan-dan-teknik-forensik-digital-dalam-dunia-maya/

[14] R. Novrianda Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial Digital Forensics Deleted Cyber Crime Evidence on Social Media Instant Messaging," 2021.

[15] A. M. Afdal, Y. Salim, and A. Rachman Manga', "Analisis Bukti Digital Forensik pada Discord Menggunakan Metode National Institute of Standards Technology INFORMASI ARTIKEL ABSTRAK," *Buletin Sistem Informasi dan Teknologi Islam*, vol. 3, no. 4, pp. 293–300, 2022.

[16] R. Y. Prasongko, A. Yudhana, and I. Riadi, "Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp," 2022.

[17] G. Yafi, D. Hariyadi, and T. Febrianto, "ANALYSIS OF ENCRYPTED NETWORK TRAFFIC FROM SECURE INSTANT MESSAGING APPLICATION: CASE STUDY ON SYNOLOGY CHAT INSTANT MESSAGE APPLICATION," Nov. 2022.

[18] A. El Hafidy, D. Relikson, and M. L. P. Sopian, "Analisis Bukti Digital pada Fitur Edit WhatsApp Desktop menggunakan Metode Digital Forensic Research Workshop (DFRWS)." [Online]. Available: https://jurnalmahasiswa.com/index.php/jriin

[19] M. N. Fadillah, R. Umar, A. Yudhana, A. Dahlan, Y. Jalan, and S. H. Soepomo, "ANALISIS FORENSIK APLIKASI DOMPET DIGITAL PADA SMARTPHONE ANDROID MENGGUNAKAN METODE DFRWS."

[20] R. Badillah, A. Y. Muniar, Abd. Rahman, F. H. Saputra, Mansyur, and S. Sahibu, "Digital Forensic Evidence Analysis In Revealing Defamation On Social Media (Twitter) Using The Static Forensics Method," *Ceddi Journal of Information System and Technology (JST)*, vol. 2, no. 2, pp. 22–33, Dec. 2023, doi: 10.56134/jst.v2i2.45.

[21] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *Jurnal Informatika: Jurnal pengembangan IT (JPIT)*, vol. 7, no. 1, Jan. 2022.

[22] I. Riadi and I. Ainur Rafiq, "Mobile Forensics on Social Media Using Digital Forensics Research Workshop Methods," *Engineering and Applied Technology*, vol. 1, no. 2, p. 2023, [Online]. Available: https://pubs.ast-ptm.or.id/index.php/eat

[23] A. Wijoyo, T. Rahmawati, W. Agustin, and B. Muhammad Saputra, "PERLINDUNGAN DATA SENSITIF : ENKRIPSI SEBAGAI PILAR UTAMA KEAMANAN KOMPUTER", [Online]. Available: https://jurnal.publikasimahasiswa.id/index.php/chipset

[24] D. Yuliana, T. Yuniati, and B. P. Zen, "ANALISIS FORENSIK TERHADAP KASUS CYBERBULLYING PADA INSTAGRAM DAN WHATSAPP MENGGUNAKAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)," *CyberSecurity dan Forensik Digital*, 2022.

[25] "Menandatangani dan mengenkripsi file menggunakan sertifikat OpenPGP dengan Kleopatra. | Howto 2024." Accessed: Oct. 20, 2024. [Online]. Available: https://id.technology-news-hub.com/8603-sign-and-encrypt-files-kleopatra