**JURNAL FASILKOM**
Volume 14 No. 2 | Agustus 2024: 332-338

P-ISSN : 2089-3353
E-ISSN : 2808-9162

# Identifikasi *Digital Evidence* dalam *Transaction Fraud* pada WhatsApp Desktop berdasarkan NIST SP 800-86: Studi Kasus Bisnis Properti

Rayhan Ramdhany Hanaputra[1], Khoerina Sa'adah[2], Rahmat Purwoko[3]
[1]Rekayasa Perangkat Lunak Kripto, Politeknik Siber dan Sandi Negara
[2,3]Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara
[1]rayhan.ramdhany@student.poltekssn.ac.id *, [2]khoerina.saadah@student.poltekssn.ac.id, [3]rahmat.purwoko@poltekssn.ac.id

***Abstract***

*The global economic growth is closely linked to the continuous advancement of technology. This is because the existence of technology serves as a strategic key that brings convenience to the business world. In the business process, instant messaging (IM) applications help to directly bridge service providers with consumers. Fraud transaction attacks are one type of attack that can be carried out using IM media. To identify and provide legal responses to incidents of such attacks, a process of digital forensic analysis is required. The analysis process to obtain digital evidence must be carried out in accordance with recognized frameworks to ensure legal validity in legal proceedings. This study provides an overview of digital forensic analysis using live forensic techniques in the scenario of fraud transaction attacks occurring in the property business sector, utilizing the instant messaging service WhatsApp Desktop. The process of discovering digital evidence is based on the NIST SP 800-86 framework. The results obtained show that digital evidence in the form of conversation text and deleted image files can be found using live forensic techniques.*

*Keywords: digital forensic, transaction fraud, live forensic, NIST SP 800-86, whatsapp desktop*

**Abstrak**

Pertumbuhan ekonomi secara global memiliki keterkaitan erat terhadap kemajuan teknologi yang terus berkembang. Hal ini dikarenakan keberadaan teknologi menjadi kunci strategis yang membawa kemudahan bagi dunia bisnis. Pada proses bisnis aplikasi *instant messaging* (IM) membantu menjembatani langsung antara penyedia layanan dengan konsumen. Serangan *transaction fraud* merupakan salah satu serangan yang dapat dilakukan dengan media IM. Untuk dapat mengidentifikasi dan memberikan respon hukum atas insiden serangan ini maka diperlukan proses analisis forensik digital. Proses analisa untuk mendapatkan digital *evidence* harus dilakukan sesuai dengan kerangka kerja yang telah diakui untuk mendapatkan nilai legalitas pada proses hukum. Pada penelitian ini diberikan gambaran analisis digital forensik menggunakan teknik *live forensic* pada skenario serangan *fraud transaction* yang terjadi pada bidang bisnis properti dengan memanfaatkan layanan *instant messaging* WhatsApp Desktop. Proses penemuan *digital evidence* dilakukan berdasarkan kerangka kerja NIST SP 800-86. Hasil yang diperoleh menunjukkan bahwa *digital evidence* berupa teks percakapan dan *file* gambar yang telah dihapus dapat ditemukan menggunakan teknik *live forensic*.

Kata kunci: *digital forensic, fraud transaction, live forensic*, NIST SP 800-86, whatsapp desktop



## 1. Pendahuluan

Teknologi merupakan salah satu faktor yang mempengaruhi proses pertumbuhan ekonomi secara global [1]. Kemajuan teknologi tidak hanya menghadirkan inovasi baru, melainkan juga secara signifikan memberikan pandangan-pandangan baru terhadap cara bekerja, berkomunikasi, dan berinteraksi. Hal ini berkaitan erat terhadap perubahan metode layanan karena sifatnya yang mampu mengefisiensi baik dari segi waktu dan keterbatasan ruang. Apabila keunggulan tersebut dikelola dengan benar maka dapat menjadi peluang yang baik dalam menghadapi tantangan pertumbuhan ekonomi yang dinamis [2].

Keberadaan teknologi juga mendorong adanya transformasi digital di berbagai sektor untuk mampu bertahan dalam menghadapi dinamika tantangan bisnis [3]. Transformasi digital ini dapat mencakup berbagai aspek mulai dari dikembangkannya otomatisasi proses bisnis hingga penerapan teknologi informasi dalam pengambilan keputusan. Sejalan dengan hal tersebut, transformasi digitalisasi mulai dikembangkan secara gratis dari berbagai *platform* sumber terbuka seperti *Google Business* yang membantu penggunanya dalam melakukan pemasaran sehingga memungkinkan untuk menjangkau target pasar yang lebih luas. Kemudahan ini tentu memberikan dampak yang baik terhadap pemilik bisnis kecil dan menengah dalam mengembangkan usahanya.

Pada proses bisnis, tentu melibatkan komunikasi dua arah antara konsumen dan pemilik bisnis untuk mencapai kesepakatan bisnis. Salah satu aplikasi komunikasi *online* yang paling banyak digunakan adalah WhatsApp. Whatsapp secara resmi didirikan pada tahun 2009 oleh Jan Koum sebagai aplikasi *mobile* dan di tahun 2016 Whatsapp mulai memperluas jangkauan komunikasinya dalam bentuk WhatsApp desktop yang merupakan pengembangan dari WhatsaApp web di tahun 2015. Di Indonesia aplikasi Whatsapp banyak digunakan dari berbagai kalangan baik tua maupun muda untuk berkomunikasi. Hal ini

P-ISSN : 2089-3353
E-ISSN : 2808-9162

dikarenakan Whatsapp memiliki fitur yang sederhana sehingga lebih mudah digunakan bagi para pemula pengguna *smartphone* dengan internet [4]. Selain itu WhatsApp memiliki beberapa kelebihan lainnya yaitu diantaranya tersedianya percakapan yang interaktif dan memungkinkan penggunanya untuk berbagi konten baik berupa teks, panggilan suara, foto hingga video [5]. Dengan adnaya fitur-fitur tersebut WhatsApp menjadi bagian yang cukup penting dalam kehidupan sehari-hari di masyarakat [6].

Seiring dengan tingginya minat pengguna terhadap layanan teknologi komunikasi Whatsapp, ini menjadi kesempatan bagi para penjahat untuk melancarkan aksinya baik untuk kepentingan pribadi maupun suatu kelompok tertentu [7]. Serangan siber yang dilakukan menggunakan teknologi dapat berakibat fatal bagi korbannya karena dapat melibatkan data-data pribadi seperti data finansial transaksi keuangan, perusahaan yang berkaitan, dan sistem teknologi yang digunakan [3]. Untuk menghadapi ancaman ini analisis forensik menjadi suatu kebutuhan yang perlu dikembangkan untuk dapat mengidentifikasi, memahami, menangani, dan memberikan respons serangan yang terjadi pada lingkup digitalisasi [3].

Di tahun 2018, B. Actoriano dan I. Riadi melakukan investigasi forensik pada Whatsapp Web dengan menggunakan *Framework Integrated Digital Forensic Investigation Framework Version 2*. Hasil yang didapatkan pada penelitian ini yaitu berupa file yang terenkripsi dan dapat dibaca menggunakan ChromeCacheView [8].

Pada penelitian lain milik T. Ruslan, I. Riadi, dan Sunardi, dilakukan analisis terhadap aplikasi Whatsapp dan Facebook menggunakan metode NIST di tahun 2023 dengan hasil yang menunjukkan bahwa artefak digital pada aplikasi android dapat dikembalikan dan dilakukan *recovery data* [9].

Selanjutnya A. Soares pada tahun 2022 melakukan teknik forensik pada Whatsapp *Web* data dari *browser* dan dianalisis lebih lanjut. Adapun teknik yang dilakukan yaitu menggunakan kode Javascript yang mengekstrak data dari *browser* menjadi sebuah file JSON. Teknik ini dapat dilakukan juga pada *web chat client* lainnya [10].

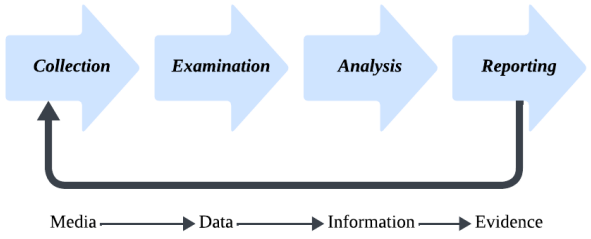
Sudiana dan Dodi juga menganalisis Whatsapp pada fitur *disappearing message* pada android yang tidak di lakukan *root-ing* dengan metodologi NIST SP 800-101r1. Hasil mengungkapkan bahwa penggunaan akses unroot pada Android dapat memulihkan 83,33% *disappearing message* dari file cadangan dan log notifikasi. Riwayat pesan ditemukan dalam pesan database berhasil merekonstruksi skenario yang telah dibuat sebelumnya [11].

Pada penelitian ini akan dilakukan skenario sebagai studi kasus dampak teknologi *instant messaging* (IM) terhadap bisnis properti. Bisnis properti yang dilakukan adalah transaksi pembayaran untuk sewa properti yaitu vila. Penelitian ini bertujuan untuk memperoleh bukti digital atas penipuan transaksi keuangan yang melibatkan aplikasi pesan online Whatsapp berbasis Desktop.

## 2. Metode Penelitian

### 2.1. Metode

Metode yang digunakan dalam penelitian ini mengacu pada kerangka kerja NIST SP 800-86. Kerangka kerja ini diterbitkan oleh *National Institute of Standards and Techologies* (NIST) yang dirancang dengan tujuan memberikan panduan dalam proses forensik digital. NIST SP 800-86 berisikan beberapa tahapan meliputi *data collection*, *examination*, *analysis*, dan *reporting* [12]. Keempat tahapan tersebut memiliki keterkaitan satu sama lain dan memiliki peran penting dalam proses identifikasi, pengumpulan, analisis, dan pelaporan bukti digital. Dengan penerapan kerangka kerja NIST SP 800-86 memberikan kepercayaan bahwa prosedur yang digunakan pada proses forensik digital yang dilakukan konsisten, dimana ini menjadi aspek penting yang dibutuhkan dalam konteks hukum dan investigasi. Adapun tahapan metode yang digunakan pada penelitian ini ditunjukkan pada Gambar 1.




Gambar 1. Tahapan Metode NIST SP 800-86

a. *Collection*
Pada tahapan *collection* penyidik mengolektifkan barang bukti yang memungkinkan untuk dilakukan analisa lebih jauh untuk memperoleh bukti digital konkret yang dapat membantu dalam pemutusan hukum di persidangan [13].

b. *Examination*
Pada tahapan ini barang bukti yang berhasil diperoleh oleh penyidik perlu diekstraksi untuk mendapatkan data digital [13].

c. *Analysis*
Proses analisis dilakukan terhadap data mentah atau data digital untuk mengidentifikasi, memahami, dan menghasilkan sautu bukti digital yang dianggap sah dalam persidangan. Proses analisis dapat dilakukan dengan memperhatikan aspek-aspek, korelasi, *timeline*, *event of interest*, *corroboration*, *recovery of additional evidence*, dan *interpretation* [13].

d. *Reporting*

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Tahapan terakhir adalah laporan yang menyajikan hasil temuan selama proses analisis *digital evidence* untuk keperluan proses hukum selanjutnya [13].

2.2. Skenario Serangan

Pada penelitian ini dilakukan skenario serangan untuk memperoleh *digital evidence*. Skenario dibuat secara runtut yang menjabarkan terkait insiden serangan. Tujuan adanya skenario adalah untuk menjadi pedoman informasi yang akan diidentifikasi sebagai suatu serangan *transaction fraud*. Berikut dijelaskan skenario yang disimulasikan.

a. Membuat akun Whatsapp sebagai tersangka.
b. Membuat akun Whatsapp sebagai korban.
c. Tersangka mengirimkan pesan untuk bernegosiasi kepada korban.
d. Tersangka menannyakan nomor rekening untuk transfer sejumlah uang.
e. Korban menigirimkan pesan nomor rekening ke tersangka.
f. Tersangka mengirimkan bukti transakasi palsu yang menyatakan transfer sudah dilakukan.
g. Korban mengirim pesan nominal uang yang dikirimkan melebihi jumlah uang yang disepakati.
h. Tersangka meminta pengembalian uang sejumlah nominal awal yang disepakati.
i. Korban mengirimkan sejumlah uang kembalian.
j. Korban baru memeriksa mutasi rekening, namun ditemukan fakta bahwa tersangka tidak mengirimkan uang sama sekali ke rekening korban.
k. Tersangka menghapus pesan dan memblokir nomor korban.

Pesan pada Whatsapp yang telah dihapus dengan nomor yang diblokir diungkap melalui WhatsApp Desktop milik tersangka dengan menggunakan tools forensik, dalam hal ini yaitu FTK Imager. Skenario simulasi yang dilakukan pada penelitian ini ditunjukkan pada Gambar 2.


Gambar 2. Skenario Serangan *Transaction Fraud* Bisnis Properti

## 3. Hasil dan Pembahasan

Skenario penelitian dilakukan dengan menggunakan laptop dengan sistem operasi Windows 11 yang telah terinstalasi WhatsApp Desktop v 2.2347.1.0 sebagai tersangka dan laptop beristem operasi Windowss 11 yang telah terintalasi WhatsApp Desktop v 2.2348.2.0 sebagai korban. Pada studi kasus ini laptop tersangka ditemukan menyala ketika dilakukan penangkapan. Laptop tersangka dibiarkan menyala dan tidak dilakukan memulai ulang sistem untuk menghindari kehilangan data memori.

3.1. *Collection*

Pada tahap *collection* penyidik mengumpulkan barang bukti yang mungkin digunakan oleh tersangka dalam melakukan *fraud attack* pada bisnis properti. Pada proses ini barang bukti yang ditemukan perlu diamankan menggunakan *faraday bag* untuk memastikan barang bukti tetap dalam kondisi baik dan tidak terhubung dengan jaringan manapun. Pengumpulan barang bukti bertujuan untuk menemukan barang yang dapat digunakan dalam penemuan *digital evidence* yang berkaitan dengan tindakan kejahatan. Barang bukti yang berhasil ditemukan adalah sebuah laptop dengan merk ASUS Vivobook X415EP yang memiliki sistem operasi Windows 11 dan terpasang aplikasi WhatsApp Desktop v 2.2347.1.0. Laptop yang ditemukan tersebut masih dalam kondisi dimana aplikasi WhatsApp Desktop masih menyala.

3.2. *Examination*

Pada proses ini, barang bukti berupa laptop yang telah diamankan kemudian diperiksa secara menyeluruh. Pada tahap pemeriksaan awal, tidak ditemukan adanya percakapan maupun media yang secara langsung mengarah pada kasus yang sedang diselidiki. Namun, satu hal yang mencolok adalah adanya nomor pengguna yang diblokir pada aplikasi komunikasi, yang ternyata merupakan nomor milik pemilik bisnis properti yang terlibat dalam kasus ini.

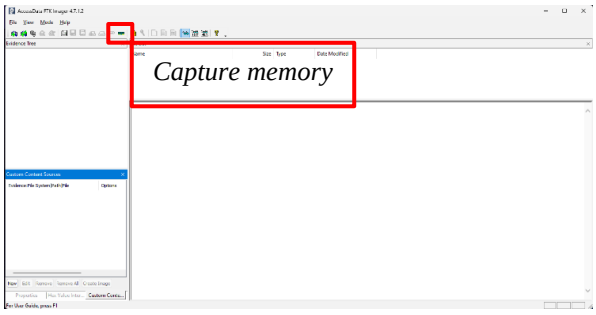
Korban melaporkan bahwa percakapan yang terkait dengan kasus tersebut dilakukan melalui pesan WhatsApp. Namun, setelah pemeriksaan mendalam, tidak ditemukan percakapan yang relevan pada perangkat tersebut, menimbulkan dugaan bahwa pesan-pesan tersebut mungkin telah dihapus oleh tersangka. Untuk mengatasi masalah ini, dilakukan investigasi dengan metode *live forensic* pada barang bukti.

Proses pengambilan bukti digital menggunakan teknik *live forensic* dipilih karena meskipun pesan WhatsApp telah dihapus dari aplikasi, data tersebut mungkin masih tersimpan sementara di RAM perangkat. Teknik ini memungkinkan penyidik untuk mengekstrak data dari memori sistem yang aktif, yang bisa mengungkap informasi penting yang belum sepenuhnya terhapus atau ditimpa.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

FTK Imager digunakan dalam proses ini karena perangkat lunak tersebut memiliki fitur yang memungkinkan untuk melakukan *capture memory* atau *memory dump* dengan efektif. Dengan melakukan *capture memory*, penyidik dapat memperoleh gambaran lengkap dari data yang sedang atau baru-baru ini digunakan oleh sistem, termasuk potensi jejak digital dari percakapan yang dihapus.

Proses *capture memory* ditunjukkan pada Gambar 3, yang menggambarkan langkah-langkah dalam pengambilan data dari RAM menggunakan FTK Imager. Dengan demikian, penyelidik dapat mengakses dan menganalisis data yang mungkin mengungkapkan aktivitas tersangka yang tidak terlihat selama pemeriksaan standar. Hal ini menjadi kunci dalam membangun kembali konteks percakapan yang relevan dengan kasus dan memastikan semua bukti yang tersedia dapat dieksplorasi secara menyeluruh..

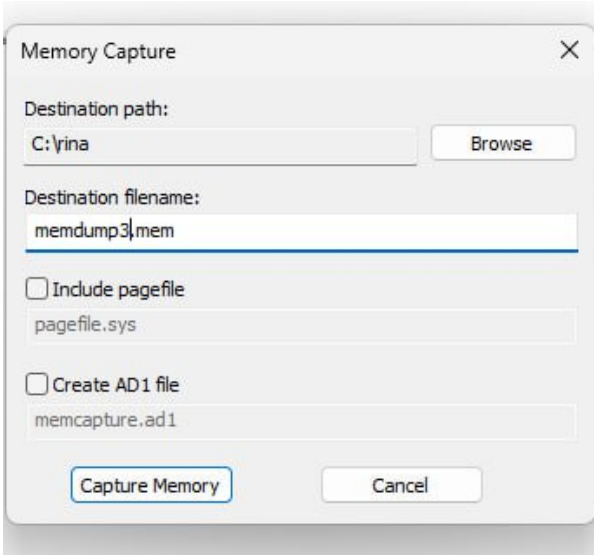



Gambar 3. *Capture Memory* pada FTK Imager

Proses *capture memory* menggunakan FTK Imager dapat memakan waktu yang bervariasi tergantung pada jumlah data yang tersimpan dalam RAM. Semakin besar kapasitas dan jumlah data yang ada di memori, semakin lama waktu yang dibutuhkan untuk menyelesaikan proses penyalinan. Sebaliknya, jika data yang ada relatif sedikit, proses *capture memory* dapat dilakukan dengan lebih cepat. Oleh karena itu, waktu yang dibutuhkan untuk proses ini perlu dipertimbangkan dalam perencanaan investigasi forensik, terutama ketika waktu merupakan faktor kritis.

Setelah proses *capture memory* selesai, hasil *imaging* perlu disimpan di lokasi folder yang telah ditentukan. Hal ini penting untuk memudahkan pencarian dan pengelolaan *file* selama melakukan proses forensik. Penyimpanan yang terorganisir juga membantu penyidik dalam menjaga integritas dan keamanan data selama proses analisis, sehingga meminimalkan risiko kehilangan atau kerusakan data.

*File* hasil *imaging* yang dihasilkan oleh FTK Imager memiliki format .mem. Format ini umumnya digunakan untuk menyimpan hasil *memory dump*, yang mencakup data biner yang terdapat dalam RAM. *File* dengan format .mem ini dapat memuat berbagai jenis data, termasuk proses yang sedang berjalan, data sementara, serta informasi lain yang relevan dengan aktivitas sistem pada saat *capture memory* dilakukan. Dalam konteks forensik, *file* .mem menjadi sumber informasi yang berharga untuk menganalisis dan merekonstruksi kejadian yang mungkin tidak terdeteksi melalui metode lain.



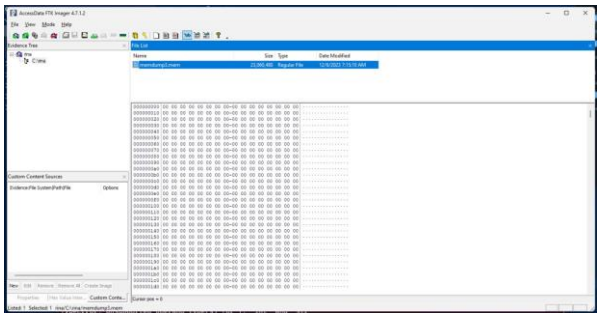

Gambar 4. Format *File* dari *Memory Imaging*

Fitur *capture memory* pada FTK Imager memungkinkan penyidik untuk menyalin data yang tersimpan pada RAM dari sistem yang masih aktif. RAM menyimpan informasi penting yang dapat hilang ketika sistem dimatikan, seperti proses yang sedang berjalan, data sementara, dan aktivitas jaringan. Oleh karena itu, menyalin data dari RAM merupakan langkah krusial dalam penyelidikan digital, karena memberikan gambaran yang mendalam mengenai aktivitas mencurigakan yang mungkin terjadi pada barang bukti yang sedang dianalisis.

Ketika melakukan penyalinan data dari RAM, penting bagi penyidik untuk memastikan bahwa *file imaging* memori yang dihasilkan adalah identik dengan data memori asli. Hal ini bertujuan untuk menghindari kesalahan selama proses forensik, yang bisa mengarah pada interpretasi yang keliru atau kehilangan data penting. Keakuratan *file imaging* dapat dipastikan dengan menggunakan teknik *hashing*, di mana nilai *hash* dari data asli dibandingkan dengan nilai *hash* dari *file imaging*. Jika nilai *hash* keduanya sama, maka *file imaging* dapat dianggap sebagai salinan yang akurat dari memori asli.

Proses *creating image* yang berhasil dilakukan dapat dilihat pada Gambar 5. Gambar ini menunjukkan langkah-langkah dalam proses *capture memory* menggunakan FTK Imager, dimulai dari identifikasi sistem yang sedang berjalan hingga pengambilan data dan verifikasi melalui *hashing*. Dengan menggunakan FTK Imager, penyidik dapat memastikan bahwa setiap bit data dari RAM telah disalin dengan akurat, sehingga setiap analisis yang dilakukan berdasarkan *file imaging* ini dapat dipercaya.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

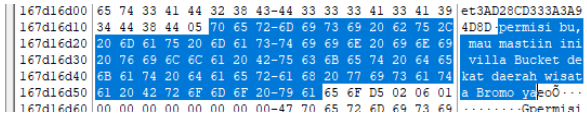


Gambar 5. Hasil Capture Memory FTK Imager

### 3.3. *Analysis*

Untuk memahami jejak digital, motivasi, dan mekanisme serangan yang telah terjadi, diperlukan analisis mendalam terhadap hasil *file imaging* yang telah dikumpulkan. *File imaging* ini merupakan salinan digital dari perangkat yang berisi *metadata* penting yang dapat memberikan gambaran detail tentang aktivitas digital yang terjadi. *Metadata* ini mencakup informasi seperti waktu dan lokasi komunikasi, perangkat yang digunakan, dan pola interaksi lainnya. Analisis *metadata* dapat mengungkapkan bagaimana tersangka berusaha menyembunyikan jejak digitalnya, termasuk teknik yang digunakan untuk menghapus atau memodifikasi data.

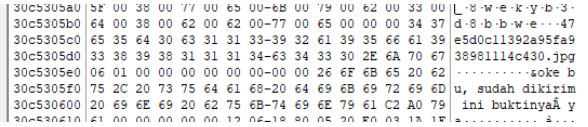
Proses sebelumnya berhasil mengidentifikasi dan mengumpulkan data digital berupa riwayat percakapan antara tersangka dan korban yang dilakukan melalui aplikasi WhatsApp Desktop. Riwayat ini mencakup percakapan teks yang mengindikasikan interaksi antara kedua belah pihak. Data ini sangat penting dalam proses investigasi karena dapat digunakan untuk mengidentifikasi motif, pola komunikasi, serta potensi kolaborator yang mungkin terlibat. Analisis lebih lanjut terhadap percakapan ini memungkinkan penyelidik untuk membangun kronologi kejadian dan memahami konteks dari percakapan tersebut. Data digital yang dimaksud dapat dilihat pada Gambar 6, yang memberikan representasi visual dari percakapan antara tersangka dan korban, membantu penyelidik untuk lebih memahami dinamika dan relasi yang terjadi.




Gambar 6. Bukti Percakapan pada FTK Imager

Dalam proses investigasi lebih lanjut, ditemukan dua file gambar yang tercantum dalam riwayat percakapan antara tersangka dan korban. Percakapan ini tidak disertai catatan yang menjelaskan waktu pengiriman atau penerimaan gambar tersebut, sehingga menambah tantangan dalam analisis kronologi peristiwa. Kedua file gambar yang ditemukan memiliki format .jpg, namun tidak memiliki format penamaan yang spesifik atau deskriptif. Hal ini disebabkan oleh sistem penamaan file otomatis yang diterapkan oleh WhatsApp, di mana gambar yang dikirim melalui aplikasi ini biasanya diberi nama dengan kombinasi karakter acak. Kombinasi tersebut tidak mudah dikenali dan seringkali tidak memberi petunjuk langsung mengenai isi atau asal-usul file.

Namun, ada pengecualian dalam kasus di mana *file* gambar dikirim sebagai dokumen. Dalam skenario ini, WhatsApp mempertahankan nama asli dari *file* gambar tersebut, sehingga memudahkan identifikasi dan analisis lebih lanjut. Pengiriman gambar dalam bentuk dokumen dapat memberikan keuntungan dalam investigasi, karena nama asli *file* sering kali mencerminkan isi atau konteks gambar, serta dapat menyertakan informasi tambahan yang relevan seperti tanggal atau deskripsi yang berkaitan dengan gambar tersebut.




Gambar 7. Bukti File Lampiran Tersangka

Dalam proses penemuan data digital, ditemukan teks percakapan yang menunjukkan adanya tindakan penipuan transaksi (*transaction fraud*) yang dilakukan oleh tersangka. Percakapan tersebut mengindikasikan upaya tersangka untuk meyakinkan korban agar percaya terhadap validitas transaksi yang dilakukan. Tersangka melampirkan bukti transaksi palsu sebagai alat untuk mengelabui korban, membuatnya yakin bahwa pembayaran telah dilakukan. Korban, merasa yakin dengan bukti yang diberikan, tidak melakukan verifikasi terhadap mutasi rekening bank, yang merupakan langkah penting untuk mengonfirmasi kebenaran transaksi yang dilaporkan.

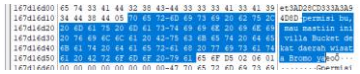
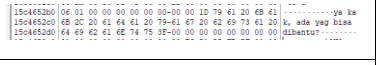
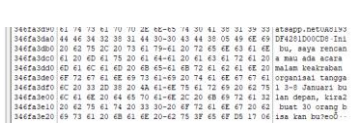
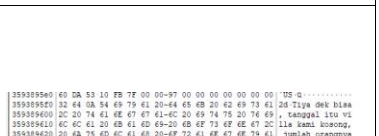
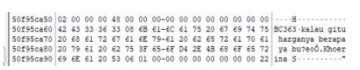
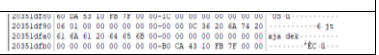
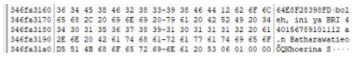
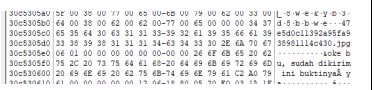
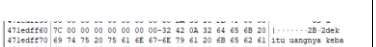
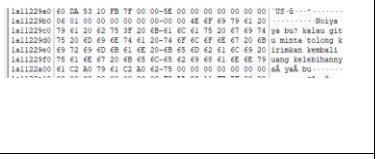
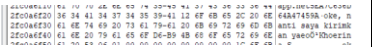
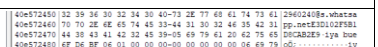
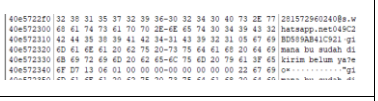
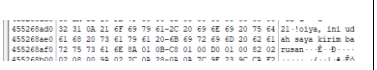
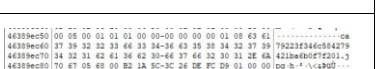
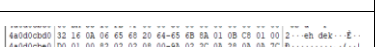
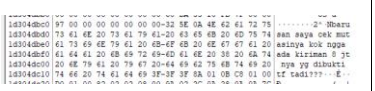
Dalam riwayat percakapan yang berhasil ditemukan, tidak terdapat catatan waktu dan tanggal yang dapat digunakan untuk menyusun kronologi kejadian dengan tepat. Namun, ditemukan dua file gambar yang dikirimkan selama percakapan tersebut. Berdasarkan konteks percakapan, dua file gambar ini merupakan bukti transaksi yang dikirimkan, di mana satu file berasal dari tersangka dan satu lagi dari korban. Bukti ini penting karena memberikan gambaran mengenai metode yang digunakan oleh tersangka untuk meyakinkan korban. Gambar yang dikirim oleh tersangka diduga kuat merupakan bukti transaksi palsu, sementara gambar dari korban menandakan bukti transaksi yang telah dilakukan dengan catatan yang sebenarnya.

Kasus ini terungkap ketika korban akhirnya menyadari adanya tindakan penipuan setelah melakukan pengecekan mutasi rekening. Korban menemukan bahwa dana yang seharusnya diterima tidak pernah masuk ke rekeningnya, meskipun ia telah mengirimkan sejumlah uang kembalian sesuai permintaan tersangka. Kesadaran korban akan penipuan ini terjadi setelah pengecekan terhadap mutasi menunjukkan ketidaksesuaian antara klaim transaksi dan realitas keuangan.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Struktur riwayat percakapan yang berhasil ditemukan digambarkan dalam bentuk tabel, dengan huruf A merepresentasikan tersangka dan B sebagai korban. Tabel ini membantu penyelidik dalam menguraikan dialog antara kedua belah pihak, menyoroti bagaimana tersangka membangun narasi penipuan dan bagaimana korban akhirnya menyadari kebohongan tersebut. Analisis lebih lanjut terhadap percakapan ini dapat mengungkap pola komunikasi yang digunakan dalam penipuan, serta langkah-langkah strategis yang dilakukan oleh tersangka untuk mendapatkan kepercayaan korban.

Tabel 1. Bukti Digital Percakapan

| Pihak | Percakapan | Bukti Digital |
|---|---|---|
| A | permisi bu, mau mastiin ini villa Bucket dekat daerah wisata Bromo ya |  |
| B | ya kak, ada yag bisa dibantu? |  |
| A | Ini bu, saya rencana mau ada acara malam keakraban organisai tanggal 3-8 Januari bulan depan, kira2 buat 30 orang bisa kan bu? |  |
| B | iya dek bisa, tanggal itu villa kami kosong, jumlah orangnya juga masih memungkinkan |  |
| A | kalau gitu harganya berapa ya bu? |  |
| B | 6 jt aja dek |  |
| A | oke bu, boleh minta nomor rekening untuk kirim uangnya? |  |
| B | boleh, ini ya BRI 440156789 101112 a.n Batharawatie |  |
| A | 47e5d0c11392a95fa938981114c430.jpg.....&oke bu, sudah dikirim ini buktinya |  |
| B | dek itu uangnya kebanyakan 2 jt, harusnya kan 6 jt |  |
| A | oiya ya bu? kalau gitu minta tolong kirimkan kembali uang kelebihannya ya bu |  |
| B | oke, nanti saya kirimkan ya |  |
| A | iya bu |  |
| A | gimana bu sudah dikirim belum ya? |  |
| B | oiya, ini udah saya kirim barusan |  |
| B | Image Kembalian 2jt.jpg |  |
| B | Eh dek |  |
| B | barusan saya cek mutasinya kok ngga ada kiriman 8 jt nya yg dibukti tf tadi??? |  |
| B | ini beneran udah kirim apa belum yaa?? |  |

## 4. Kesimpulan

Analisis forensik yang dilakukan untuk mengidentifikasi serangan *transaction fraud* pada studi kasus penelitian dapat dilakukan dengan menggunakan teknik *live forensic* yang berdasarkan pada kerangka kerja NIST SP 800-86. *Digital evidence* yang diperoleh berupa teks yang mengindikasikan percakapan tersangka kepada korban. Bukti digital tambahan juga dihasilkan berupa temuan adanya file gambar yang terbaca pada *data memory imaging*. Bukti digital berupa riwayat percakapan dan indikasi gambar *transaction fraud* dapat dijadikan sebagai bukti tindak kejahatan dalam proses bisnis properti.

Berdasarkan studi kasus yang diangkat pada penelitian ini, terdapat beberapa fokus atau area yang bisa dikembangkan dalam penelitian di masa depan guna

P-ISSN : 2089-3353
E-ISSN : 2808-9162

memenuhi keterbaruan pada pengembangan ilmu pengetahuan. Ini mencakup kompleksitas dan kombinasi skenario serangan yang lebih dapat menggambarkan *cybercrime* sesungguhnya di bidang bisnis. Selain itu eksplorasi lebih lanjut bisa dilakukan dengan usulan teknik, metode forensik yang lebih baik, hingga penggunaan tools pada kasus layanan lain pada aplikasi *Instant Message*.

## Daftar Rujukan

[1] I. M. L. M. Jaya, "The Impact of Financial Inclusion on Public Financial Services Education through Financial Technology in Sleman Regency, Indonesia," *Esensi: Jurnal Bisnis dan Manajemen*, vol. 9, no. 2, pp. 155–174, Dec. 2019, doi: 10.15408/ess.v9i2.13576.

[2] A. Anggono and M. Riskiyadi, "Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review," *Jurnal Manajemen dan Organisasi (JMO)*, vol. 12, no. 3, pp. 239–251, 2021.

[3] B. Nikkel, "Fintech forensics: Criminal investigation and digital evidence in financial technologies," *Forensic Science International: Digital Investigation*, vol. 33. Elsevier Ltd, Jun. 01, 2020. doi: 10.1016/j.fsidi.2020.200908.

[4] T. Liedfray, F. J. Waani, and J. J. Lasut, "Peran Media Sosial Dalam Mempererat Interaksi Antar Keluarga Di Desa Esandom Kecamatan Tombatu Timur Kabupaten Minahasa Tenggara," *Jurnal Ilmiah Society*, vol. 2, no. 1, 2022.

[5] A. Wirara, B. Hardiawan, M. Salman, and B. Siber dan Sandi Negara, "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan 'WhatsApp,'" *Teknoin*, vol. 26, no. 1, pp. 66–74, 2020.

[6] J. Fernandes Andry and V. Jessica Angelina, "Analisis Kepuasan Pengguna WhatsApp Web Menggunakan Metode Webqual 4.0 dan IPA," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 13, no. 3, pp. 546–553, Dec. 2023, [Online]. Available: https://web.whatsapp.com

[7] I. Riadi and dan Muhamad Ermansyah Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *Jurnal Teknik Elektro*, vol. 10, no. 1, pp. 18–22, 2018.

[8] B. Actoriano and I. Riadi, "Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2," *International Journal of Cyber-Security and Digital Forensics*, pp. 410–419, 2018, [Online]. Available: https://www.researchgate.net/publication/327592240

[9] I. Riadi and T. Ruslan, "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 13, no. 2, pp. 286–292, Aug. 2023.

[10] A. M. Muniz Soares, "WhatsApp Web Client Live Forensics Technique," in *International Conference on Information Systems Security and Privacy*, Science and Technology Publications, Lda, 2022, pp. 629–636. doi: 10.5220/0011006400003120.

[11] D. Sudiana, C. H. Nuruddin, M. Rizkinia, and D. Husna, "Forensic Analysis of WhatsApp Disappearing Message on Unrooted Android Using Mobile Device Forensics Methodology NIST SP 800-101r1," *Evergreen*, vol. 11, no. 1, pp. 516–524, Mar. 2024, doi: 10.5109/7172316.

[12] M. W. Indriyanto, D. Hariyadi, M. Habibi, U. J. Achmad, and Y. Yogyakarta, "Investigasi dan Analisis Forensik Digital pada Percakapan Grup Whatsapp Menggunakan NIST SP 800-86 Dan Support Vector Machine," *CyberSecurity dan Forensik Digital*, vol. 13, no. 2, pp. 34–38, 2020.

[13] R. A. Ramadhan, P. Rachmat Setiawan, and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework," *IT Journal Research and Development*, pp. 162–168, Feb. 2022, doi: 10.25299/itjrd.2022.8968.