Volume 21 Nomor 01 (2026) 73-82
E – Link P-ISSN 1858-2109 E-ISSN 2656-5676
Jurnal Teknik Elektro dan Informatika

ANALISIS PEMULIHAN BUKTI DIGITAL WHATSAPP BERBASIS WEB MENGGUNAKAN METODE *DIGITAL FORENSIC RESEARCH WORKSHOP* (DFRWS)

Lifany Naza Dewi[1)] , Fahmi Fachri[2)]
[1,2)] Jurusan Teknik Informatika, Fakultas Teknik, Universitas Ma'arif Nahdlatul Ulama Kebumen
Jln. Kutoarjo Km. 05, Jatisari, Kebumen, Jawa Tengah, Indonesia.
E-mail : [1)]faninaza04@gmail.com , [2)]fahmifachriumnu@gmail.com

ABSTRAK

Perkembangan teknologi komunikasi digital memberikan dampak positif dalam mempe-rmudah pertukaran informasi melalui aplikasi pesan instan. Salah satu aplikasi yang banyak digunakan masyarakat adalah *WhatsApp*, termasuk layanan WhatsApp Web yang memungkinkan akses melalui *browser* komputer. Namun, platform ini juga sering dimanfaatkan dalam tindak kejahatan siber seperti penipuan online. Pelaku biasanya menghapus pesan percakapan dan file pendukung untuk menghilangkan jejak digital. Penelitian ini bertujuan untuk menganalisis kemampuan tools digital forensik *FTK Imager* dan *Autopsy* dalam memulihkan bukti digital yang telah dihapus pada WhatsApp Web dengan menggunakan metode *Digital Forensic Research Workshop* (DFRWS). Penelitian ini dilakukan melalui simulasi kasus penipuan online pada perangkat laptop berbasis *Windows* dengan dengan pendekatan *live forensic* Dimana proses akuisis data dilakukan saat *system* dalam keadaan aktif (on).Tahapan penelitian yang meliputi *identification, preservation, collection, examination, analysis,* dan *presentation. FTK Imager* digunakan dalam proses akuisisi data sekaligus untuk memulihkan pesan teks, sedangkan *Autopsy* dimanfaatkan untuk mengekstraksi file gambar yang telah dihapus. Hasil penelitian menunjukkan bahwa seluruh pesan teks yang berjumlah 11 berhasil dipulihkan dengan tingkat keberhasilan mencapai 100%. Sementara itu, dari total 8 file gambar bukti transaksi digital yang dianalisis, sebanyak 7 file berhasil dipulihkan dengan persentase keberhasilan sebesar 87,5%. Hasil tersebut menunjukkan bahwa penggunaan kedua *tools* tersebut secara bersamaan cukup efektif dalam mendukung proses *investigasi* forensik digital, khususnya dalam pemulihan bukti digital pada *platform* WhatsApp Web.

Kata kunci : digital forensic, dfrws, whatsapp web, ftk imager, autopsy

ABSTRACT

The development of digital communication technology has had a positive impact in facilitating the exchange of information through instant messaging applications. One application widely used by the public is WhatsApp, including the WhatsApp Web service that allows access through a computer browser. However, this platform is also often exploited in cybercrimes such as online fraud. Perpetrators usually delete chat messages and supporting files to eliminate digital traces. This study aims to analyze the capabilities of the digital forensic tools FTK Imager and Autopsy in recovering digital evidence that has been deleted on WhatsApp Web using the Digital Forensic Research Workshop (DFRWS) method. This study was conducted through a simulation of an online fraud case on a Windows-based laptop device with a live forensic approach where the data acquisition process was carried out while the system was active (on). The research stages included identification, preservation, collection, examination, analysis, and presentation. FTK Imager was used in the data acquisition process as well as to recover text messages, while Autopsy was used to extract deleted image files. The results showed that all 11 text messages were successfully recovered with a success rate of 100%. Meanwhile, of the eight digital transaction evidence image files analyzed, seven were successfully recovered, with a success rate of 87.5%. These results demonstrate that the combined use of

these two tools is quite effective in supporting digital forensic investigations, particularly in recovering digital evidence on the WhatsApp Web platform.

***Keywords**: digital forensic, dfrws, whatsapp web, ftk imager, autopsy.*

1. PENDAHULUAN

Kemajuan digital sekarang ini, teknologi komunikasi digital telah membawa dampak positif yang besar, seperti kemudahan berinteraksi dan berbagi informasi antar pengguna di seluruh dunia. Salah satu aplikasi pesan instan paling populer adalah *WhatsApp*,yang digunakan oleh jutaan orang setiap harinya, tidak hanya itu *Whatsapp* juga sering kali digunakan oknum untuk melakukan tindak kejahatan seperti penipuan online. Meskipun data spesifik mengenai jumlah kasus penipuan yang dilakukan secara khusus melalui *WhatsApp* tidak tersedia, platform ini sering dimanfaatkan oleh pelaku kejahatan siber karena popularitas dan kemudahan penggunaanya. Modus penipuan yang umum dilakukan melalui *WhatsApp* meliputi pengiriman tautan malware, pesan berkedok hadiah, dan penipuanber kedok pinjaman online illegal [1]. Perusahaan induk platform pencarian kerja *Seek Limited* juga melaporkan tingginya kasus penipuan lowongan kerja di kawasan Asia Pasifik dalam International Fraud Awareness Week 2025. Indonesia tercatat sebagai negara dengan tingkat penipuan tertinggi, menyumbang sekitar 38% kasus di Asia Pasifik dan 62% di kawasan Asia selama periode Juli 2024 hingga Juni 2025[2]. Penipuan tersebut dilakukan melalui media sosial seperti *WhatsApp*, *Facebook*, dan *Telegram* dengan modus menawarkan pekerjaan paruh waktu yang mengatasnamakan perusahaan atau *e-commerce* [3].

Selain melalui perangkat mobile, aktivitas penipuan ini juga dapat dilakukan dengan memanfaatkan aplikasi instant *messenger* (IM) berbasis desktop sebagai media komunikasi dengan korban. Salah satu contohnya adalah WhastApp Web, yang memungkinkan pengguna mengakses layanan *WhatsApp* melalui *browser* tanpa perlu melakukan instalasi aplikasi [4]. Dalam konteks ini, forensic digital berperan penting dalam mengidentifikasi, mengumpulkan dan mengaalisis bukti digital terkait kasus kejadian yang penipuan yang banyak terjadi. Salah satu tantangan kejahatan di dunia digital juga tidak mudah untuk mengamatinya secara fisik, tetapi membutuhkan analisis digital, karena bukti-bukti yang ditinggalkan oleh pelaku kejahatan semakin berkembang ke arah bentuk kejahatan yang asimetris[5], Oleh karena itu, diperlukan metode forensik digital yang tepat untuk mengatasi tantangan tersebut salah satunya yaitu dengan menggunakan Metode *Digital Forensic Research Workshop* (DFRWS) terbukti efektif dalam menemukan artefak digital termasuk data yang terhapus, dengan tingkat akurasi yang tinggi[6]. Forensik digital bertujuan untuk membantu dalam penemuan dan analisis fakta serta bukti digital terkait suatu kejadian. Selain itu, teknik *live forensic* memungkinkan analisis data secara langsung pada sistem yang sedang berjalan, teknik yang melibatkan analisis data secara waktu nyata dalam suatu sistem yang biasanya disimpan di RAM atau ditransmisikan melalui jaringan [7].

Terdapat beberapa penelitian mengenai *live forensic* yang telah dilakukan sebelumnya, Beberapa studi menunjukkan bahwa penerapan *live forensic* pada WhatsApp Web mampu mengungkap berbagai artefak penting, seperti percakapan, file media, timestamp, hingga riwayat aktivitas pengguna dengan bantuan tools seperti *FTK Imager* dan *Browser History Viewer*[8]. Sedangkan penelitian lain penggunaan *FTK Image* dan *Autopsy* juga terbukti mampu memulihkan data yang terhapus dengan tingkat keberhasilan yang tinggi. Hasil forensik menunjukkan bahwa *FTK Imager* dan *Autopsy* mampu memulihkan bukti yang dihapus secara permanen (Shift+Delete) dengan tingkat keberhasilan 100%. Namun demikian, data yang dihapus melalui pemformatan tidak dapat dipulihkan, dengan tingkat keberhasilan 0%[9].

Mengacu pada studi diatas, menunjukkan bahwa metode live forensic dapat digunakan

dalam pencarian bukti digital untuk mendukung penanganan kasus kejahatan. Penelitian ini bertujuan untuk menerapkan metode live forensic dalam menemukan bukti digital pada WhatsApp Web guna membuktikan kasus penipuan online dengan menggunakan tools *FTK Imager* dan *Autopsy* serta mengikuti tahapan sistematis DFRWS. Pada penelitian ini dilakukan pembaruan dalam penggunaan tools dengan memanfaatkan *FTK Imager* untuk proses akuisisi data serta *Autopsy* untuk proses analisis dan pemulihan bukti digital. Metode yang digunakan mengacu pada referensi yang relevan sebagai dasar dalam pelaksanaan penelitian. Tahapan penelitian ini adalah Akuisisi data dilakukan secara *live forensics* dengan pendekatan *logical acquisition* terhadap artefak WhatsApp Web yang tersimpan pada browser. *WhatsApp* Web dan *WhatsApp* Desktop memiliki karakteristik artefak digital yang kompleks, sehingga memerlukan pendekatan forensik yang tepat dalam proses investigasi [10].

Diharapkan dengan penelitian dengan menggunakan alat forensik yaitu FTK Imager dan Autopsy guna memastikan metode ini tetap relevan dan efektif seiring perkembangan teknologi juga versi perangkat Windows yang lebih canggih serta dapat memberikan kontribusi terhadap pengembangan metode investigasi digital yang semakin maju dan juga dapat menghadapi tantangan teknologi komusikasi yang semakin hari semakin berkembang serta modern.

2. METODE PENELITIAN DAN BAHAN

Penelitian ini menggunakan rancangan penelitian eksperimental dengan pendekatan simulasi kasus penipuan online melalui media *WhatsApp* Web. Simulasi dilakukan untuk menggambarkan kondisi nyata tindak kejahatan digital, Dimana pelaku mengirim pesan penawaran pekerjaan kerja palsu beserta file gambar pendukung kepada korban, kemudian menghapus seluruh pesan dan file setelah komunikasi selesai.

Penelitian dilakukan dengan menggunakan laptop berbasis *Windows* 10 Pro 64-bit yang digunakan untuk mengakses *WhatsApp Web* melalui *browser Google Chrome*. Perangkat yang digunakan memiliki prosesor Intel® Core™ i3-1005G1 @ 1.20 GHz, RAM 8 GB, dan media penyimpanan *Solid State Drive* (SSD) yang digunakan untuk mengakses *WhatsApp* Web melalui *browser Google Chrome*. Penggunaan SSD perlu dijelaskan karena media penyimpanan jenis ini memiliki mekanisme TRIM yang dapat memengaruhi proses pemulihan data yang telah dihapus sehingga menjadi salah satu tantangan dalam investigasi forensik digital. Oleh karena itu, proses akuisisi dilakukan sesegera mungkin setelah simulasi selesai untuk meminimalkan hilangnya artefak digital yang masih dapat diperoleh[11].

Proses akuisisi dilakukan segera setelah skenario simulasi selesai untuk menjaga kemungkinan ditemukannya artefak digital yang masih tersimpan pada sistem. Selain itu, pendekatan live forensic diterapkan ketika perangkat masih berada dalam kondisi aktif dan terhubung ke internet. Hal ini dilakukan karena *WhatsApp Web* bekerja dengan mekanisme sinkronisasi data secara langsung melalui *browser*[8]. Selama sistem masih aktif, artefak digital seperti *cache, cookie, session storage,* dan data yang tersimpan pada memori volatil masih dapat diidentifikasi dan dikumpulkan untuk kepentingan *investigasi*[12].Akuisisi pada kondisi tersebut memungkinkan investigator memperoleh bukti digital yang relevan secara lebih optimal dibandingkan apabila perangkat telah berada dalam kondisi tidak aktif[4]

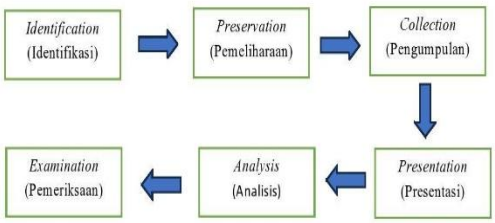
Penerapan metode *live forensic* juga dilakukan untuk mengidentifikasi informasi serta mengumpulkan barang bukti pada jaringan lokal, khususnya ketika perangkat di lokasi kejadian masih terhubung ke jaringan komputer dalam kondisi aktif (on)[12]. Pemanfaatan jaringan lokal bertujuan agar proses pengambilan data dapat dilakukan langsung pada perangkat tanpa risiko perubahan akibat sinkronisasi dengan server luar. Pada penggunaan *WhatsApp Web*, data aktivitas pengguna tidak selalu langsung hilang meskipun telah dihapus. Sebagian data masih tersimpan dalam sistem lokal, seperti *cache, cookie, dan session storage* yang digunakan oleh *browser*. Selama data tersebut belum tertimpa oleh aktivitas baru, artefak

digitalnya masih berpotensi untuk ditemukan kembali dan dianalisis[13].

Kondisi tersebut menjadikan pemeriksaan pada sistem jaringan lokal penting dilakukan untuk mengidentifikasi sisa artefak digital, termasuk data yang telah dihapus. Skenario kemudian diproses dengan metode *Digital Forensic Research Workshop* (DFRWS).

2.1 Digital Forensic Research Workshop (DFRWS)

DFRWS adalah metode atau model konseptual yang dikembangkan oleh komunitas akademik forensik digital dalam konferensi DFRWS (Palmer, 2001). Framework ini menjadi dasar bagi metodologi investigasi forensik digital yang banyak digunakan dalam berbagai standar dan pedoman investigasi kejahatan siber. DFRWS Framework juga merupakan model yang sangat penting dalam forensik digital karena memberikan panduan metodologis dalam investigasi kejahatan siber. Dengan enam tahapan yang jelas, framework ini membantu penyelidik dalam menangani bukti digital dengan cara yang dapat dipertanggungjawabkan secara hukum[13]. Adapun tahapan proses investigasi forensik dengan metode DFRWS ditunjukan pada Gambar 1.



Gambar 1. Tahapan Metode DFRWS

Penelitian ini menggunakan metode *Digital Forensics Research Workshop* (DFRWS) yang terdiri dari enam tahapan, yaitu identification, preservation, collection, examination, analysis, dan presentation. Tahap identification dilakukan untuk menentukan objek dan jenis data yang dianalisis, yaitu perangkat laptop, *browser*, serta *WhatsApp* Web dengan fokus pada pesan teks dan gambar. Tahap *preservation* bertujuan menjaga keutuhan data dengan mengamankan perangkat dan mendokumentasikan kondisi awal. Tahap *collection* dilakukan menggunakan teknik *logical acquisition* dengan *FTK Imager* untuk mengambil data dari direktori browser *Google Chrome*. Selanjutnya, tahap *examination* dilakukan untuk memverifikasi integritas data melalui pengecekan nilai hash. Tahap *analysis* menggunakan *FTK Imager* dan *Autopsy* untuk mengekstraksi artefak teks serta memulihkan file gambar. Tahap terakhir, *presentation*, dilakukan dengan menyajikan hasil analisis dalam bentuk tabel dan laporan forensik secara sistematis.

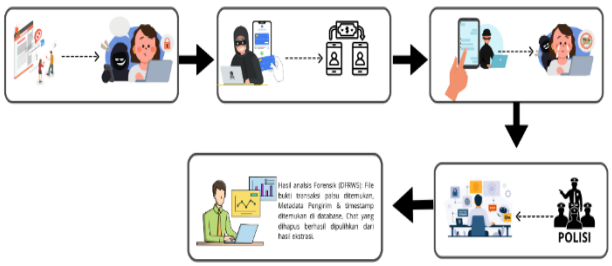
2.2 FTK Imager

FTK Imager merupakan perangkat lunak forensik digital yang digunakan untuk menganalisis serta memperoleh bukti digital. Aplikasi ini memungkinkan penyidik membuat salinan forensik (forensic image) dari media penyimpanan tanpa mengubah keaslian data. Selain itu, FTK Imager dapat digunakan untuk melakukan proses akuisisi terhadap file, direktori, partisi, maupun physical disk dalam rangka kebutuhan investigasi forensik. Salah satu keunggulannya adalah kemampuannya dalam memulihkan file yang telah terhapus, tersembunyi, maupun terformat, sehingga data tersebut masih dapat dimanfaatkan sebagai barang bukti. [4]. *FTK Imager* juga merupakan salah satu alat yang digunakan untuk membuat salinan bit-by-bit dari perangkat seluler. Meskipun lebih sering digunakan dalam forensik computer. FTK Imager juga dapat digunakan untuk mengekstrak data dari perangka seluler dan membuat salinan data yang dapat digunakan dalam analisis forensic lebih lanjut. FTK Imager memberikan kemampuan untuk melakukan pemindaian dan menganalisis file yang sudah terhapus (Garfinkel & Rosenberg, 2020)[14]. Pada penelitian ini *FTK Imager* menggunakan 1 dataset berupa *file memory dump* (.mem) yang diperoleh melalui proses *capture memory* pada sistem *Windows* saat menjalankan WhatsApp Web. Dataset tersebut diproses menggunakan *FTK Imager*, dengan ukuran data yang tergolong besar yang ditunjukkan oleh *unallocated space* sekitar 10 GB, sehingga proses pemindaian membutuhkan waktu lebih lama dan dapat

mempengaruhi tingkat keberhasilan pemulihan data.

2.3 Autopsy

Autopsy adalah platform forensik digital *open-source* yang berfungsi sebagai antarmuka pengguna grafis untuk *The Sleuth Kit* dan berbagai alat forensik digital lainnya. *Autopsy* memberikan kemampuan bagi penyidik atau analis forensik untuk mengekstraksi, menganalisis, dan memvisualisasikan data dari media penyimpanan seperti hard drive, SSD, dan perangkat penyimpanan lainnya. *Autopsy* menyederhanakan proses analisis forensik dengan menyediakan antarmuka yang mudah digunakan untuk menerapkan berbagai alat forensik digital dalam satu platform. Dengan antarmuka yang intuitif, aplikasi ini menampilkan informasi penting dari perangkat, seperti file yang dihapus, riwayat internet, log aktivitas, dan metadata, yang sangat berguna untuk keperluan investigasi [14].



Gambar 2. Simulasi Serangan

Sumber data dalam penelitian ini berasal dari simulasi penipuan online dengan menganalisis artefak digital yang tersimpan pada perangkat laptop yang digunakan pelaku dalam simulasi, khususnya data browser yang berkaitan dengan aktivitas *WhatsApp* Web. Barang bukti smartphone milik korban berupa data percakapan simulasi pesan teks dan *file* gambar hanya dijadikan sebagai pembanding antara bukti digital yang telah diperoleh dari laptop pelaku dengan percakapan *WhatsApp* pada smartphone korban. Teknik pengumpulan data dilakukan melalui proses akuisisi digital menggunakan aplikasi *FTK Imager*. Akuisisi difokuskan pada hasil *Capture Memory*. Proses ini dilakukan untuk memperoleh data digital sebagai objek peneriksaan lanjutan. Analisis data dilakukan menggunakan dua *tools* digital forensic, yaitu *FTK Imager* dan *Autopsy*. *FTK Imager* digunakan untuk menelusuri artefak teks, pencarian string data, serta pemulihan pesan percakapan yang telah dihapus. Sementara itu, *Autopsy* digunakan untuk memeriksa struktur file system dan melakukan pemulihan terhadap file gambar bukti transaksi palsu yang telah dihapus.

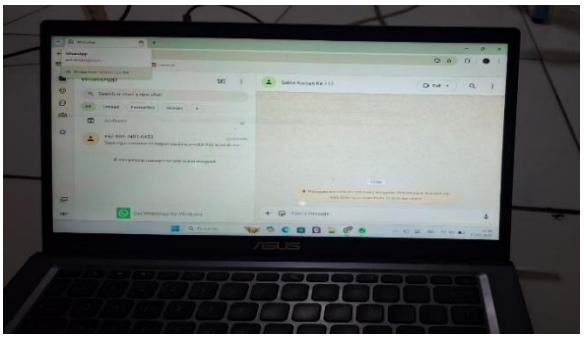
3. HASIL DAN DISKUSI

Penelitian ini dilakukan untuk menganalisis kemampuan tools *digital forensic* dalam memulihkan bukti digital yang telah dihapus pada platform WhatsApp Web. Skenario penelitian dibuat dengan mensimulasikan tindak penipuan online melalui percakapan WhatsApp Web menggunakan browser Google Chrome pada system operasi Windows. Dalam skenario tersebut, pelaku mengirimkan pesan penawaran kerja palsu beserta file gambar berupa bukti transfer digital Palsu. Setelah komunikasi selesai, seluruh pesan dan file gambar dihapus dengan tujuan menghilangkan jejak digital. Berdasarkan skenario insiden tersebut dilakukan proses digital forensic dengan teknik *live forensic*, hal ini dikarenakan kondisi Tempat Kejadian Perkara Digital yang berupa personal computer masih dalam keadaan menyala (on)[7]. Metode *investigasi* yang digunakan adalah *Digital Forensic Research Workshop* (DFRWS)[7] yang terdiri dari tahapan *identification, preservation, collection, examination, analysis*, dan *presentation*. *Tools* yang digunakan adalah *FTK Imager* untuk proses akuisisi dan pemulihan pesan teks, sedangkan *Autopsy* digunakan untuk analisis file system serta pemulihan file gambar yang telah dihapus.

3.1. Tahap *Identificaton*

Pada tahap *identification*, investigator menentukan objek penelitian berupa perangkat laptop *Windows* yang digunakan untuk mengakses *WhatsApp* Web melalui *browser Google* Chrome dalam keadaan menyala. Jenis data yang menjadi target pencarian meliputi teks

percakapan dan file gambar bukti transaksi palsu yang didikirim pada perangkat pelaku.



Gambar 3. Bukti Chat pada perangkat Pelaku

Gambar 4. Bukti Chat Pada Smartphone Korban

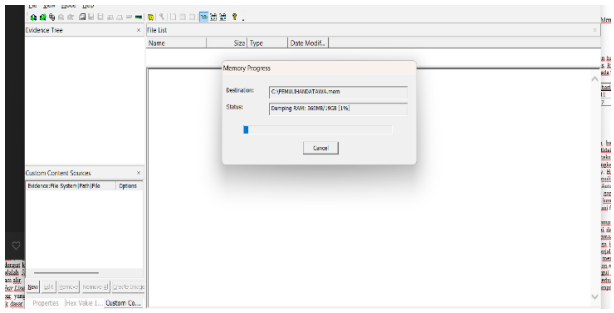
3.2. Tahap *Preservation*

Tahap *preservation* dilakukan untuk menjaga integritas barang bukti digital agar tidak mengalami perubahan selama proses investigasi. Langkah yang dilakukan yaitu mengamankan isi browser tanpa membersihkan *cache*,dan mendokumentasikan kondisi awal perangkat serta mengamankan bukti chat yang belum di hapus pada SmartPhone korban sebagai pembanding hasil pemulihan.

Gambar 5. Laptop Pelaku dan SmartPhone Korban

3.3 Tahap *Collection*

Tahap *collection* merupakan proses pengumpulan bukti digital dari perangkat yang digunakan untuk mengakses WhatsApp Web. Pada penelitian ini proses akuisisi dilakukan menggunakan *FTK Imager* dengan fitur *capture memory*.

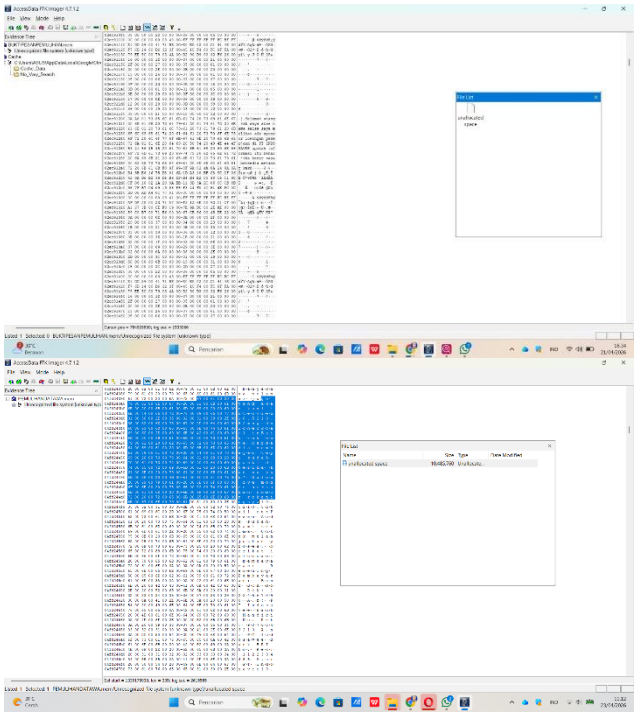


Gambar 6. Screenshot layar proses capture memory

3.4. Tahap *Examination*

Tahap *examination* dilakukan dengan menyaring dan menganalisis hasil akuisisi data untuk menemukan artefak digital yang relevan. Pada tahap ini, data hasil ekstraksi dari WhatsApp Web dianalisis secara lebih mendalam untuk merekonstruksi riwayat percakapan yang terdapat pada dua bukti gambar. Berdasarkan hasil analisis tersebut, bukti pertama menunjukkan awal interaksi antara korban dan pelaku, di mana korban mulai menghubungi pelaku melalui percakapan WhatsApp. Selanjutnya, pada bukti kedua terlihat perkembangan komunikasi yang lebih intens, di mana pelaku mulai melakukan pendekatan dan mempengaruhi korban hingga akhirnya korban mengikuti arahan pelaku.

Dari percakapan tersebut juga teridentifikasi adanya proses manipulasi yang mendorong korban untuk mengirimkan data rekening, yang kemudian berujung pada terjadinya transaksi atau transfer sejumlah uang. Hasil ini menunjukkan adanya pola komunikasi yang berurutan dan saling berkaitan, sehingga dapat menggambarkan kronologi kejadian secara jelas berdasarkan artefak digital yang ditemukan.



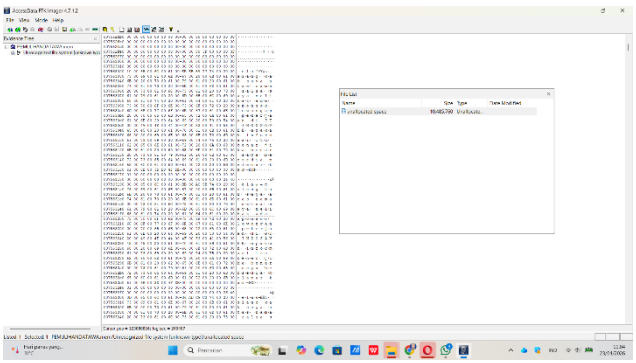
Gambar 7. Screenshot Gambar Folder Hasil ekstraksi Tools FTK Imager

3.5 Tahap Analisis

Tahap analisis merupakan proses utama dalam penelitian ini, yaitu melakukan pemulihan data yang telah dihapus berhasil dipulihkan menggunakan *FTK Imager* dan *Autopsy*. Hasil analisis menunjukkan bahwa proses pemulihan pesan dengan *FTK Imager* mampu mengembalikan seluruh bukti percakapan antara pelaku dan korban. Berdasarkan proses akuisisi data pada RAM, penyidik menemukan kembali aktivitas komunikasi yang terjadi melalui WhatsApp. Data yang diperoleh berupa 11 pesan teks percakapan, sebagaimana ditampilkan pada Gambar 7. Gambar tersebut memperlihatkan salah satu contoh percakapan yang terjadi pada aplikasi *WhatsApp*.

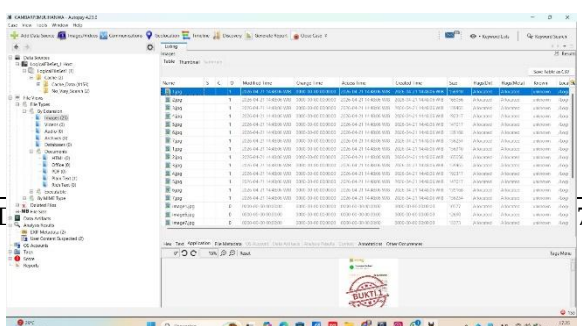
Pada tahap analisis, dilakukan proses pemulihan data yang telah dihapus dengan menggunakan *FTK Imager* dan *Autopsy*. Berdasarkan hasil yang diperoleh, seluruh percakapan antara pelaku dan korban berhasil dipulihkan melalui *FTK Imager*. Proses ini memanfaatkan data yang masih tersimpan pada RAM, sehingga aktivitas komunikasi pada *WhatsApp* masih dapat diidentifikasi kembali. Data yang diperoleh berupa 11 pesan teks percakapan, sebagaimana ditunjukkan pada Gambar 8. Berbeda dengan data teks, pemulihan file gambar menggunakan Autopsy tidak sepenuhnya berhasil. Dari total 8 file gambar, sebanyak 7 file dapat dipulihkan, sedangkan 1 file lainnya tidak berhasil dikembalikan.

Dengan demikian, dapat disimpulkan bahwa FTK Imager lebih efektif dalam pemulihan data berbasis teks, sementara Autopsy lebih optimal dalam analisis struktur *file system* dan pemulihan file gambar, meskipun masih memiliki keterbatasan pada kondisi tertentu.



Gambar 8. Bukti Teks Chat Korban Dan Pelaku menggunakan FTK Imager

Data yang diperoleh menjukukan salah satu dari 11 pesan teks percakapan, sebagaimana ditunjukkan pada Gambar 8. Hasil tersebut menunjukkan bahwa data berbasis teks cenderung lebih mudah dipulihkan karena masih meninggalkan jejak pada memori sistem, meskipun telah dihapus oleh pengguna.



Gambar 9. Bukti Transaksi digital Menggunakan Autopsy

Berdasarkan Gambar 9. diatas menunjukan hasil pemulihan gambar menggunakan tools *Autopsy*. Bukti transaksi palsu yang dikirim oleh pelaku behsil memulihkan 7 gambar, serta 1 gambar bukti transaksi yang dikirim korban tidak dapat dipulihkan dapat dilihat dari hasil ekstraksi pada tools *Autopsy*. Hal ini diduga disebabkan oleh adanya proses penimpaan data (*overwrite*) atau kerusakan pada struktur file, sehingga sebagian data tidak dapat direkonstruksi secara utuh.

3.6 Tahap Presentasi

Tahap ini dilakukan dengan Menyusun hasil investigasi dalam bentuk laporan yang sistematis. Tahap ini bertujuan untuk menyusun dan menyajikan hasil investigasi ke dalam laporan yang terstruktur. Ringkasan hasil pemulihan bukti digital selama proses analisis ditampilkan dalam bentuk tabel. Tingkat keberhasilan pemulihan data dihitung berdasarkan perbandingan antara data yang berhasil dipulihkan dan total data, kemudian dinyatakan dalam persentase.

$$Recovery\ Rate = \frac{Jumlah\ data\ berhasil\ dipulihkan}{Jumlah\ Total\ data} x100\%$$

Tabel 2. Hasil Recovery Data Berdasarkan Tools Forensik

Tools	Jenis Bukti	Berhasil	Gagal
FTKImager	Pesan teks	11	0
Autopsy	File gambar	7	1

Berdasarkan Tabel 2. *FTK Imager* mampu memulihkan seluruh pesan teks yang dianalisis dengan jumlah 11 data tanpa adanya kegagalan. Sementara itu, pada penggunaan *Autopsy*, dari total 8 file gambar yang diperiksa, sebanyak 7 file berhasil dipulihkan dan 1 *file* tidak dapat dikembalikan. Perbedaan hasil tersebut menunjukkan bahwa tingkat keberhasilan pemulihan dipengaruhi oleh jenis data yang dianalisis. Secara keseluruhan, tingkat keberhasilan pemulihan mencapai 100% untuk pesan teks dan 87,5% untuk file gambar. Hasil ini menunjukkan bahwa pemulihan data berbasis teks cenderung lebih optimal, sedangkan pada file gambar masih terdapat keterbatasan dalam proses pemulihannya

Perbedaan tingkat keberhasilan pemulihan antara pesan teks dan file gambar dipengaruhi oleh karakteristik penyimpanan datanya. Artefak percakapan *WhatsApp Web* umumnya masih tersimpan pada *cache browser*, *session storage*, atau memori sistem saat akuisisi dilakukan sehingga pesan teks lebih mudah ditemukan kembali menggunakan *FTK Imager*[8]. Sebaliknya, file gambar tersimpan sebagai berkas digital yang lebih besar dan lebih rentan mengalami perubahan, penghapusan permanen, atau penimpaan data sehingga proses pemulihannya lebih sulit[12]. Kondisi ini menyebabkan seluruh pesan teks berhasil dipulihkan, sedangkan satu file gambar tidak dapat dipulihkan. Selain itu, penggunaan media penyimpanan SSD yang menerapkan mekanisme *TRIM* juga dapat mengurangi ketersediaan data yang telah dihapus sehingga turut memengaruhi hasil pemulihan artefak digital[11].

4. KESIMPULAN DAN SARAN

Hasil penelitian menunjukkan bahwa penghapusan data pada *WhatsApp* Web tidak sepenuhnya menghilangkan jejak digital. Pesan teks masih dapat ditemukan menggunakan *FTK Imager*, sedangkan file gambar masih dapat dipulihkan melalui *Autopsy*. Berdasarkan hasil pengujian, *FTK Imager* berhasil memulihkan seluruh 11 pesan teks yang telah dihapus dengan tingkat keberhasilan mencapai 100%. Sementara itu, *Autopsy* mampu memulihkan 7 dari total 8

file gambar dengan tingkat keberhasilan sebesar 87,5%, meskipun terdapat 1 file yang tidak berhasil dipulihkan.

Hasil tersebut menunjukkan bahwa kombinasi kedua tools cukup efektif dalam mendukung proses investigasi forensik digital pada *WhatsApp* Web. Penerapan *framework* DFRWS juga terbukti memberikan alur investigasi yang sistematis, mulai dari tahap identifikasi hingga penyajian bukti digital. Penggunaan metode ini membantu investigator dalam menjaga integritas data serta memastikan proses investigasi berjalan secara terstruktur. *FTK Imager* memiliki keunggulan dalam menemukan artefak berbasis teks melalui fitur pencarian yang detail, sedangkan *Autopsy* lebih optimal dalam menganalisis dan memulihkan file. Dengan demikian, penggunaan kedua *tools* secara bersamaan mampu memberikan hasil investigasi yang lebih lengkap dalam mengungkap bukti digital.

5. DAFTAR PUSTAKA

[1] M. Harapansyah, S. Rahman, and B. Badaru, "The Effectiveness of Law Enforcement for Criminal Fraud via WhatsApp in the Legal Area of the Pasangkayu Police." [Online]. Available: https://ojs.staialfurqan.ac.id/IJoASER/

[2] A. Hardiantoro, "Indonesia Jadi Pusat Penipuan Lowongan Kerja Nomor 1 di Asia Pasifik, Ini Modus dan Bidang yang Disasar.," Kompas.Com. [Online]. Available: https://www.kompas.com/tren/read/2025/11/24/200000865/indonesia-jadi-pusat-penipuan-lowongan-kerja-nomor-1-di-asia-pasifik-ini

[3] F. W. Utomo, D. Rorin, M. Insana, and E. C. Mayndarto, "Mekanisme penipuan digital pada masyarakat era 5 . 0 (studi kasus penipuan online berbasis lowongan kerja paruh waktu yang merebak di masyarakat)," vol. 6, no. 1, pp. 32–41, 2024.

[4] I. I. Mubarokah and F. Fachri, "Identifikasi Bukti Digital Pinjaman Online Menggunakan Live Forensic Pada Sistem Operasi Proprietary," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 10, no. 1, pp. 117–129, 2025, doi: 10.36341/rabit.v10i1.5514.

[5] A. Ajuj, R. M. G. S. Bintang, and D. Arya Bahytsani, "Analisis Bukti Digital Forensik pada Aplikasi Threads MenggunakanMetode Digital Forensic Research Workshop," *J. Inform. Komputer, Bisnis dan Manaj.*, vol. 22, no. 2, pp. 1–10, 2024, doi: 10.61805/fahma.v22i2.118.

[6] A. Yudhana, I. Riadi, R. Yudhi Prasongko, A. Dahlan, J. Ahmad Yani Tamanan, and J. Soepomo, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," vol. 7, no. 1, 2022.

[7] M. Wibowo, M. R. Firmansyah, and R. S. Efendi, "ANALISIS BUKTI DIGITAL PADA APLIKASI DISCORD DESKTOP DENGAN MENGGUNAKAN FRAMEWORK DFRWS," 2024, [Online]. Available: http://ejurnal.provisi.ac.id/index.php/JTIKP page98

[8] S. D. Utami, C. Carudin, and A. A. Ridha, "Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[9] W. Agustiono, D. Wulan Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," *J. Teknol. dan Inf.*, vol. 14, 2024, doi: 10.34010/jati.v14i2.

[10] P. Widiandana and I. Riadi, "Forensik Digital Cyberbullying pada Grup WhatsApp

Menggunakan National Institute of Standards and Technology," vol. 12, no. 01, 2026.

[11] R. A. Ramadhan and D. Mualfah, "Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 183–192, 2020, doi: 10.25299/itjrd.2021.vol5(2).5750.

[12] E. D. Ariyanti, D. Yusup, U. S. Karawang, I. Web, L. Forensic, and P. Online, "Identifikasi Bukti Digital Instagram Web Dengan Live Forensic Identification Of Digital Evidence Instagram Web With Live Forensic In Online Shop Fraund Cases," *CyberSecurity dan Forensik Digit.*, vol. 4, no. 2, pp. 58–62, 2021.

[13] N. Anwar, M. A. Hadi, A. M. Widodo, M. Rahamawan, and B. A. Sekti, "Paduan Praktis Forensik Digital," in *Paduan Praktis Forensik Digital*, Yogyakarta, Indonesia: PT. Star Digital Publishing, Yogyakarta-Indonesia, 2025. [Online]. Available: https://www.google.co.id/books/edition/Panduan_Praktis_Forensik_Digital/lgZeEQAAQBAJ?hl=id&gbpv=0

[14] M. Salim, S. Ahmad, and S. Syaifudin, "Pengantar Forensik Digital," in *Pengantar Forensik Digital*, Yayasan Tri Edukasi Ilmiah, 2025. [Online]. Available: https://www.google.co.id/books/edition/Pengantar_Forensik_Digital/ASQ-EQAAQBAJ?hl=id&gbpv=0