

IDENTIFIKASI BUKTI DIGITAL WHATSAPP PADA SISTEM OPERASI PROPRIETARY MENGGUNAKAN LIVE FORENSICS

Ahmad Saeful Rido*¹⁾, Fahmi Fachri²⁾

1. Universitas Ma'arif Nahdlatul Ulama Kebumen, Indonesia
2. Universitas Ma'arif Nahdlatul Ulama Kebumen, Indonesia

Article Info

Kata Kunci: WhatsApp; FTK Imager; WinHex; Live Forensics; Bukti Digital

Keywords: WhatsApp; FTK Imager; WinHex; Live Forensics; Digital Evidence

Article history:

Received 25 March 2024
Revised 8 April 2024
Accepted 22 April 2024
Available online 1 June 2024

DOI :

<https://doi.org/10.29100/jipi.v9i2.5238>

* Corresponding author.
Corresponding Author
E-mail address:
al.rido0413@gmail.com

ABSTRAK

Salah satu bentuk kejahatan digital adalah menghilangkan atau menghapus barang bukti digital. Kemajuan teknologi memberikan tantangan langsung dalam menangani kejahatan digital. Media penyimpanan barang bukti elektronik dalam Random Access Memory (RAM) tidak lain hanyalah sasaran para pelaku kejahatan untuk menghindari hukum dengan cara menghilangkan berkas barang bukti. Salah satu metode yang digunakan untuk mengidentifikasi bukti kejahatan digital adalah dengan kerangka (Institut Standar dan Teknologi Nasional). Metode ini terdiri dari beberapa langkah yaitu: pengumpulan, perolehan, analisis dan pelaporan. Dengan metode ini, Tujuan penelitian adalah untuk mengetahui bukti digital yang telah dihapus menggunakan alat FTK Imager dan WinHex dengan metode National Institute of Standards and Technology. Mengetahui persentase keberhasilan bukti digital menggunakan tools FTK Imager dan WinHex dengan metode National Institute of Standards and Technology. Proses pencarian bukti digital dalam kasus penipuan transaksi online menggunakan ftk imager dan winhex tools. Barang bukti yang diperoleh berupa teks percakapan WhatsApp yang terjadi antara tersangka dan korban yang dapat dijadikan sebagai barang bukti digital terkait kasus tindak pidana penipuan toko online. Pembuktian kasus penipuan ini dilakukan dengan membandingkan atau menyinkronkan bukti digital teks percakapan yang diperoleh dari laptop pelaku dengan percakapan WhatsApp di smartphone korban.

ABSTRACT

One form of digital crime is eliminating or deleting digital evidence. Technological advances provide direct challenges in dealing with digital crime. Electronic evidence storage media in Random Access Memory (RAM) is nothing but a target for criminals to evade the law by eliminating evidence files. One method used to identify evidence of digital crime is the (National Institute of Standards and Technology) framework. This method consists of several steps, namely: collection, acquisition, analysis and reporting. With this method, the aim of the research is to find out digital evidence that has been deleted using the FTK Imager and WinHex tools using the National Institute of Standards and Technology method. Find out the percentage of success of digital evidence using the FTK Imager and WinHex tools using the National Institute of Standards and Technology method. The process of searching for digital evidence in cases of online transaction fraud using ftk imager and winhex tools. The evidence obtained is in the form of text of WhatsApp conversations that occurred between the suspect and the victim which can be used as digital evidence related to criminal cases of online shop fraud. Proving this fraud case is carried out by comparing or synchronizing digital evidence of conversation texts obtained from the perpetrator's laptop with WhatsApp conversations on the victim's smartphone.

I. PENDAHULUAN

TEKNOLOGI jaringan komputer saat ini telah memasuki hampir keseluruhan segi kehidupan. Pesatnya perkembangan internet telah berdampak pada perubahan organisasi bisnis di pemerintahan, pendidikan, kesehatan dan sektor lainnya[1]. Teknologi komunikasi membuat perubahan besar terhadap pola interaksi antar manusia menjadikan komunikasi dengan komunitas lain dengan lebih mudah, dalam arti komunikasi dapat

dilakukan dimana saja tanpa meninggalkan, bisa dilakukan dimana saja dan kapan saja. Saat ini Teknologi Informasi tidak lagi hanya dilihat sebagai pendukung, tetapi telah menjadi bagian utama dari organisasi untuk lebih kompetitif. Perlu diakui bahwa Teknologi Informasi meningkatkan praktik tata kelola perusahaan di karenakan proses bisnis yang biasanya otomatis dan direktur akan bergantung pada informasi yang disediakan oleh sistem teknologi informasi[2]. Interaksi sosial tidak lagi terkungkung dalam sekat teritorial suatu negara. Pertumbuhan atau perkembangan dalam era digital semacam ini dibarengi dengan kemunculan perusahaan-perusahaan teknologi yang menunjang peningkatan perubahan secara massif. Peningkatan ini berorientasi pada inovasi serta efisiensi yang semakin mempermudah masyarakat sebagai konsumen[3]. Teknologi komunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal partikular menjadi global universal. Hal ini pada akhirnya membawa dampak pergeseran nilai, norma, moral dan kesusilaan[4]. Di era teknologi industri 5.0 ini kita di tuntut untuk memanfaatkan dan menguasai teknologi. Penggunaan alat komunikasi seperti smartphone sudah menjadi hal tak terpisahkan bagi setiap orang untuk memudahkan dalam mencari informasi yang cepat dan akurat.[5] Pada prinsipnya manusia memiliki kebutuhan dan kemampuan serta kebiasaan untuk berkomunikasi dan berinteraksi dengan manusia satu sama lainnya, selanjutnya interaksi ini berbentuk kelompok. Sifat kelompok ini didasari rasa kepemilikan atau kemampuan dalam berkomunikasi, mengungkapkan rasa dan kemampuan untuk saling kerja sama dan bersosial. Globalisasi telah menjadi pendorong lahirnya era penggunaan teknologi informasi[6]. Globalisasi dan teknologi komunikasi mengubah struktur sosial, nilai dan interaksi manusia secara signifikan. Pengaruh perkembangan teknologi informasi dan komunikasi dalam era globalisasi bagi manusia adalah semakin terbukanya akses informasi dan komunikasi.

Teknologi informasi secara terus menerus dikembangkan agar dapat terus meningkatkan keefektifan dan kemanfaatannya. Dalam menjalankan perusahaan dibutuhkan teknologi yang mampu menangkap atau mengambil, menyimpan, mengelola, dan mengembalikan informasi dengan cepat, tepat, dan efisien. Perusahaan membutuhkan sistem informasi yang dapat menghasilkan informasi yang dibutuhkan agar dapat mencapai tujuan tertentu[7]. Perkembangan teknologi internet juga di dasari oleh perkembangan *smartphone*, saat ini memudahkan orang-orang dalam mengakses informasi dan diiringi juga dengan banyaknya pengguna media sosial[8]. Meski menghadirkan kemudahan dan kelebihan lainnya, internet juga menjadi masalah, yaitu kejahatan di dunia maya atau *cybercrime* yang semakin beragam. Selain itu dampak dari *cybercrime* sangat merugikan baik bagi individu maupun organisasi, termasuk kehilangan data pribadi, kehilangan uang, gangguan pada bisnis, ancaman keamanan nasional, dan kerugian reputasi. Pertumbuhan media sosial dan aplikasi pesan instan telah mempermudah pengembangan banyak kejahatan *cyber* dan aktivitas jahat yang serius[9]. Para penjahat dunia maya memanfaatkan teknologi komputer sebagai media melakukan kegiatan yang bertentangan dengan hukum. Salah satu tindak kejahatan yang sering terjadi adalah kasus penipuan *online shop*. Perdagangan di Indonesia telah memanfaatkan infrastruktur teknologi dalam menjalankan proses bisnis jual beli. [10]Hal ini dapat dilakukan dengan memanfaatkan aplikasi *instant messenger* (IM) berbasis desktop sebagai media komunikasi dengan korban. IM merupakan salah satu aplikasi yang sering digunakan untuk berkomunikasi menggantikan peran *Short Message Services* (SMS). Seiring berjalannya waktu, didapati bahwa aplikasi tersebut memiliki kekurangan seperti biaya pemeliharaan aplikasi yang tinggi, teknologi yang semakin terbelakang, dan hanya dapat beroperasi pada satu platform saja.[11]

Website merupakan sebuah sistem dimana informasi dalam bentuk teks, gambar, suara dan lain-lain dipresentasikan dalam bentuk *hypertext* dan dapat diakses oleh perangkat lunak yang disebut *browser*[12]. Dengan adanya *Website* ini memudahkan seseorang untuk menggunakan suatu sistem tanpa harus mengisntalnya salah satunya adalah WhatsApp Web. WhatsApp merupakan salah satu aplikasi yang mengalami peningkatan pengguna setiap tahunnya. Menurut data Statista, hingga bulan Desember 2022 jumlah pengguna WhatsApp di Indonesia sebanyak 112 juta pengguna aktif. Jumlah tersebut mengalami peningkatan dibandingkan jumlah pengguna WhatsApp pada bulan Desember 2021 sebanyak 84,8 juta pengguna. WhatsApp sendiri memiliki banyak fitur seperti pengiriman pesan, *group chat*, telpon, *video call*, Pengiriman dokumen, dan pesan suara. Selain itu WhatsApp memiliki fitur *to end encryption* atau E2EE, yaitu setiap pesan yang dikirim langsung dienkripsi secara aman dan hanya dapat dibuka oleh pengirim dan penerima saja. Artinya, pesan, foto, video, pesan suara, dokumen, pembaruan status dan panggilan telepon hanya dapat dilihat oleh pengirim dan penerima saja[13]. Gambar 1 menunjukkan data statistik pengguna WhatsApp dari bulan Desember 2017 sampai dengan Desember 2022.



.Statistik pengguna WhatsApp

Pengguna aplikasi pada komputer meninggalkan data informasi pada *Random Acces Memoy* (RAM). Pada saat menjalankan sesuatu pada komputer maka semua data yang kita RAM ini berfungsi sebagai tempat penyimpanan sementara dan hanya berkerja saat perangkat tersebut masih hidup atau beroperasi. Data yang terdapat pada RAM memberikan informasi yang berpotensi menjadikan data bukti digital terkait kasus kejahatan yang terjadi dikenal dengan sebagai forensik digital. Akan tetapi penggunaan data dan informasi yang terdapat pada RAM harus dilakukan dengan berhati-hati karena data dan informasi tersebut bisa hilang jika komputer mati.

Digital forensik merupakan ilmu baru yang berkembang terus-menerus sehingga perlu mendalam belajar tentang ilmu ini. Ilmu digital forensik berubah karena perkembangan system operasi, smartphone, dan tablet. Langkah-langkah digital forensik yang banyak dan rumit ini membutuhkan kemampuan dan software khusus untuk memecahkan suatu permasalahan yang terjadi[14]. Digital forensik merupakan bagian ilmu forensik yang digunakan untuk penyelidikan dan penyidikan dalam investigasi materi (data) yang dan penemuan konten perangkat digital. Para Ahli mengatakan digital forensik adalah suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mencari dan mengumpulkan bukti-bukti berbasis entitas maupun piranti digital sebagai alat bukti yang sah di pengadilan. Analisis digital forensik umumnya ada dua, yakni *dead forensic* dan *Live Forensic*. *Live forensic* digunakan untuk mendapatkan bukti kejahatan yang terdapat pada komputer sedang berjalan dan terhubung jaringan internet. *Live Forensic* yaitu suatu teknik analisis dimana menyangkut data yang sedang berjalan pada sistem atau data volatile yang umumnya tersimpan pada *Random Acces Memory* (RAM) atau transit pada jaringan[15]. Analisis forensik digital adalah alat penting untuk penegakan hukum yang dapat membantu mengidentifikasi kejahatan yang mungkin dilakukan dengan informasi digital[16]

Komputer dijalankan membutuhkan sistem operasi. Sistem operasi dibagi menjadi dua yaitu sistem operasi *Open Source* dan sistem operasi *Proprietary*. Penelitian ini menggunakan sistem operasi *Proprietary windows 10*. Windows 10 ini diperkenalkan pada tanggal 30 September 2014, dirilis pada 29 Juli 2015.

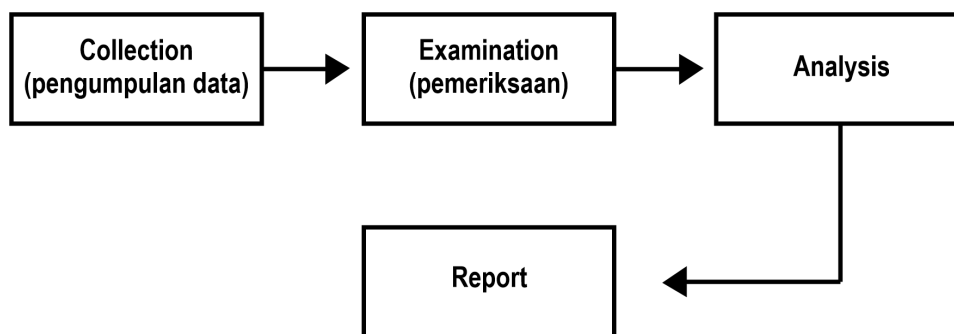
Berdasarkan latar belakang yang telah dijelaskan, Penelitian ini bertujuan untuk menemukan bukti tindak kejahatan pada kasus penipuan transaksi elektronik pada aplikasi WhatsApp menggunakan teknik *Live Forensic*. Dengan melakukan penelitian ini, diharapkan dapat memperoleh pemahaman yang lebih baik mengenai kasus-kasus penipuan khususnya pada transaksi online[17]. Salah satu metode untuk mengungkapkan kejahatan dengan digital forensik adalah dengan NIST (*National Institut of Standard and Technology*).

II. METODOLOGI

A. Metode

Penelitian ini menggunakan salah satu metode di dalam mengungkap kejahatan dengan digital forensik adalah dengan NIST (*National Institut of Standard and Technology*). Metode NIST dapat menjadi pilihan tepat untuk live forensik karena memberikan pedoman yang komprehensif dalam mengumpulkan, menganalisis, dan menyajikan bukti digital secara langsung dari sistem yang beroperasi. Metode ini terdapat beberapa keunggulan diantaranya memberikan pedoman yang rinci untuk dokumentasi, memudahkan penyajian bukti digital dalam proses penyelidikan atau di pengadilan. Namun ada juga kelemahan metode NIST diantaranya keterbatasan dalam teknologi dan memerlukan proses waktu yang lama. Metode tersebut terdiri dari beberapa langkah yaitu: *Collection, Acquisition, Analysis* dan *Reporting*. Dengan metode ini dapat mencari data dan analisis data yang

hilang, sehingga data dapat ditemukan dalam sistem meskipun data tersebut dihapus atau disembunyikan[18].



Gambar 2. Tahapan Penelitian

1) *Collection*

Tahapan *Collection* atau pengumpulan yaitu tahap yang terdiri dari persiapan, pengumpulan, dokumentasi, dan isolasi barang bukti. Hal yang dilakukan pada penelitian ini diantaranya mencatat layar dan spesifikasi barang bukti, mendokumentasikan barang bukti, serta melakukan proses *live forensics*. Pencatatan layar barang bukti dilakukan pada laptop pelaku untuk mengetahui waktu dan program yang sedang berjalan ketika perangkat bukti tersebut ditemukan. Pencatatan spesifikasi barang bukti dilakukan pada semua barang bukti yang terlibat, yaitu laptop pelaku dan *smartphone* korban.

2) *Examination*

Tahapan *Examination* dilakukan setelah data diperoleh, kemudian dikumpulkan sehingga ditemukan bukti-bukti yang terkait tindak kejahatan pelaku.

3) *Analysis*

Tahap *analysis* yaitu menganalisis hasil dari proses *Examination* yang telah dilakukan sehingga dapat mengidentifikasi konten atau file yang dapat dijadikan barang bukti. Bukti digital pada penelitian ini dianalisis dengan menggunakan *tools* FTK Imager dan WinHex. Bukti digital dianalisis hanya untuk mengetahui isi percakapan antara korban dan pelaku.

4) *Report*

Tahapan *Reporting* ini peneliti merangkum langkah yang sudah diuji mulai rentan waktu dan pada proses imaging sampai menganalisis membandingkan dan menghitung file hasil ekstraksi dengan file aslinya.

FTK Imager merupakan salah satu tools forensik yang digunakan untuk menganalisis bukti digital. Tools ini memungkinkan penyelidik untuk membuat salinan forensik dari media penyimpanan tanpa mengubah data asli. FTK Imager adalah sebuah tools yang digunakan untuk mengakuisisi atau melakukan imaging suatu file, direktori, partisi atau physical disk untuk keperluan forensik. Salah satu keunggulan dari FTK Imager dalam pengembalian file-file yang terhapus, tersembunyi dan terformat sehingga file-file tersebut dapat digunakan. Sama halnya dengan WinHex adalah sebuah editor hex dan alat pemulihan data yang umum digunakan dalam bidang komputer forensik, data recovery, proses data dalam tingkat yang rendah dan keamanan dalam IT. WinHex mendukung RAM editor dan menyediakan akses pada physical RAM.

Alat dan bahan yang digunakan pada penelitian ini yaitu berupa *Software* atau *Tools Forensic* serta *Hardware* yang merupakan barang bukti milik pelaku dan korban. Berikut ini adalah spesifikasi dari setiap alat dan bahan yang digunakan.

TABLE I.
ALAT DAN BAHAN PENELITIAN

No.	Kategori	Spesifikasi
1	Hardware	Laptop ASUS X441B Smartphone Android Realme 5
2	Software	Windows 10 Home single language Sistem Operasi 64-bit AMD A4-9125 Radeon R3 4GB FTK Imager versi 4.7.1.2 WinHex versi 20.9

Perangkat keras dan perangkat lunak yang akan digunakan dan tindakan yang akan diambil selama investigasi direncanakan. Perencanaan diperlukan agar proses penelitian dapat berjalan dengan lancar, termasuk menentukan

alat-alat yang akan digunakan dalam proses penelitian sehingga dapat diperoleh hasil penelitian yang valid. Spesifikasi *Software* yang digunakan juga sangat mempengaruhi sebuah penelitian ataupun hasil dari penelitian. Proses pengambilan barang bukti juga dipengaruhi oleh RAM yang tertera pada laptop karena semakin besar RAM maka akan semakin lama prosesnya. *Tools* yang digunakan pada suatu penelitian beserta kegunaannya masing-masing.

Tabel 1 menunjukkan alat yang digunakan dan spesifikasi tools yang digunakan. Barang bukti laptop pelaku digunakan untuk mencari barang bukti digital yang berkaitan dengan kasus penipuan bukti digital yang berkaitan dengan penipuan yang terjadi. Barang bukti *smartphone* milik korban hanya dijadikan sebagai pembandingan antara bukti digital yang telah diperoleh dari laptop pelaku dengan percakapan WhatsApp pada *smartphone* korban.

B. Rancangan simulasi

Simulasi kasus penipuan transaksi elektronik melalui percakapan WhatsApp dilakukan karena didasari pada aturan berikut ini:

- 1) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 5 huruf a.
- 2) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 6 huruf a.
- 3) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 7 ayat 1

Aturan tersebut menyatakan bahwa terdapat kriteria informasi publik yang salah satunya yaitu informasi yang diecualikan untuk dipublikasikan. Informasi yang dimaksud ialah informasi yang menghambat proses penyelidikan dan penyidik suatu tindak pidana seperti identitas saksi atau tersangka, barang bukti yang berkaitan, isi berkas perkara, dan modus operasi pada kasus tersebut.

Rancangan sistem merupakan gambaran awal dari sistem yang akan dibuat. Pada rancangan sistem akan terlihat alur atau proses yang terjadi pada sistem[19]. Penelitian ini membutuhkan simulasi untuk mendapatkan bukti digital. Simulasi yang dibuat lengkap dari aktivitas yang dijalankan pada aplikasi WhatsApp. Tujuan simulasi ini adalah agar menjadi pedoman untuk informasi yang akan diidentifikasi sebagai sebuah penipuan. Simulasinya sebagai berikut:

- 1) Membuat akun WhatsApp tersangka dan korban
- 2) Korban tertarik pada produk dan menghubungi pelaku
- 3) Pelaku mengirimkan foto dan video produk
- 4) Korban bertransaksi dan mengirim bukti transfer
- 5) Pelaku mengonfirmasi pesanan
- 6) Korban menanyakan resi pengiriman
- 7) Tersangka melakukan penipuan kepada korban
- 8) Menghapus semua percakapan dari akun tersangka

III. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan dengan menggunakan sebuah laptop Windows 10 sistem operasi 64 Bit. Pada kasus ini penyidikan menemukan barang bukti berupa sebuah laptop dalam kondisi hidup yang digunakan oleh tersangka. Laptop dibiarkan terus menyala dan tidak dimatikan untuk menghindari kehilangan barang bukti.

A. Pengumpulan Barang Bukti

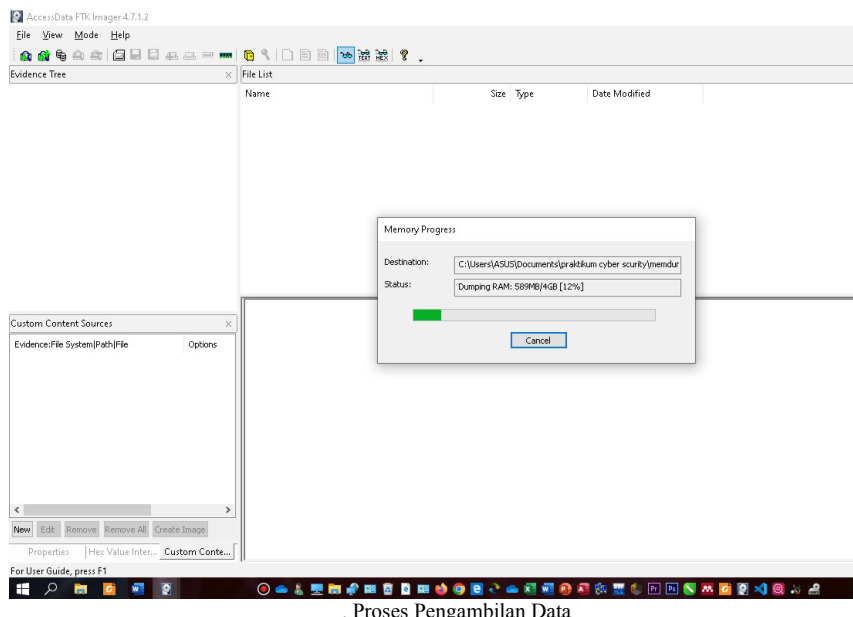
Langkah pertama yang penulis ambil adalah menganalisis masalah yang ada, mengidentifikasi masalah utama yang ada[20]. Pada tahapan ini, penyidik mengumpulkan barang bukti yang digunakan oleh tersangka guna melakukan tindakan kejahatan. Barang bukti tersebut yang akan digunakan untuk menemukan bukti digital terkait kejahatan penipuan. Tahapan ini untuk membantu proses investigasi yang akan dilakukan pada tahap selanjutnya. Pada tahapan ini menghasilkan beberapa catatan dan dokumentasi barang bukti yang terlibat dalam kasus ini. Catatan tersebut mengenai barang bukti yang ditemukan berupa sebuah laptop ASUS tipe X441B Windows 10.

B. Pemrosesan Bukti Digital FTK Imager

Setelah pencatatan dan dokumentasi barang bukti, selanjutnya dilakukan proses *live forensics* pengumpulan barang bukti digital yang terdapat pada RAM dengan perangkat masih dalam kondisi dijalankan. Untuk mendapatkan barang bukti digital dilakukan menggunakan *live forensics*.

1) Pengambilan Bukti Digital

Untuk mendapatkan bukti percakapan WhatsApp yang terdapat pada RAM dilakukan dengan menggunakan teknik *Live Forensics*. Sedangkan *Tools* yang digunakan pada penelitian ini adalah FTK Imager karena memiliki kegunaan seperti *Capture Memory* yang sangat mendukung *Live Forensics*. Fitur ini dapat mengambil data dan informasi yang terdapat pada RAM, termasuk percakapan. Gambar 3 menunjukkan sebuah proses pengambilan data pada RAM.

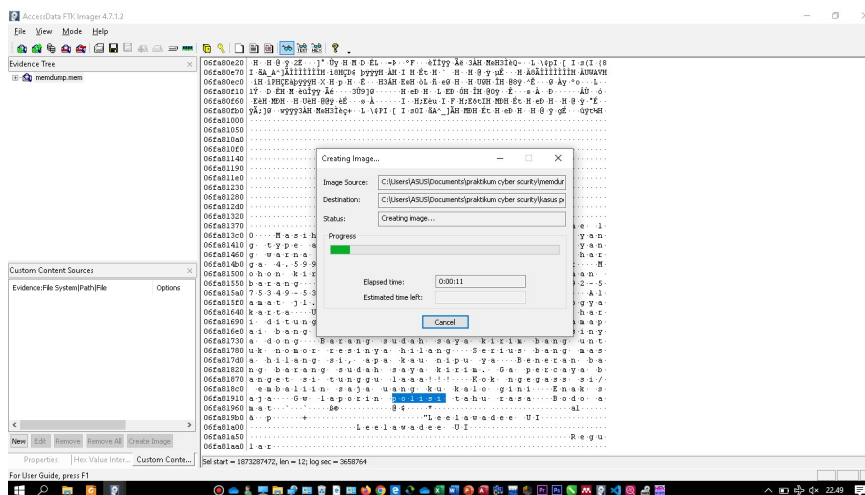


. Proses Pengambilan Data

Lamanya proses pengambil data tergantung besar kecilnya kapasitas RAM jika semakin besar maka akan semakin lama proses pengambilan bukti digitalnya, begitu juga sebaliknya. Hasil dari proses pengambilan bukti digital berupa file .mem yang dapat dibuka dan dianalisis menggunakan *tools* yang mendukung ekstensi file tersebut, salah satunya adalah FTK Imager.

2) *Penggandaan Bukti Digital*

Pengambilan bukti digital atau *Imaging* ini bertujuan untuk menghindari kerusakan pada barang bukti digital asli pada saat diproses analisis dilakukan. Bukti digital dari proses *Imaging* harus sama dengan bukti digital asli. Gambar 4 menunjukan sebuah proses *Imaging* bukti digital.



. proses Imaging

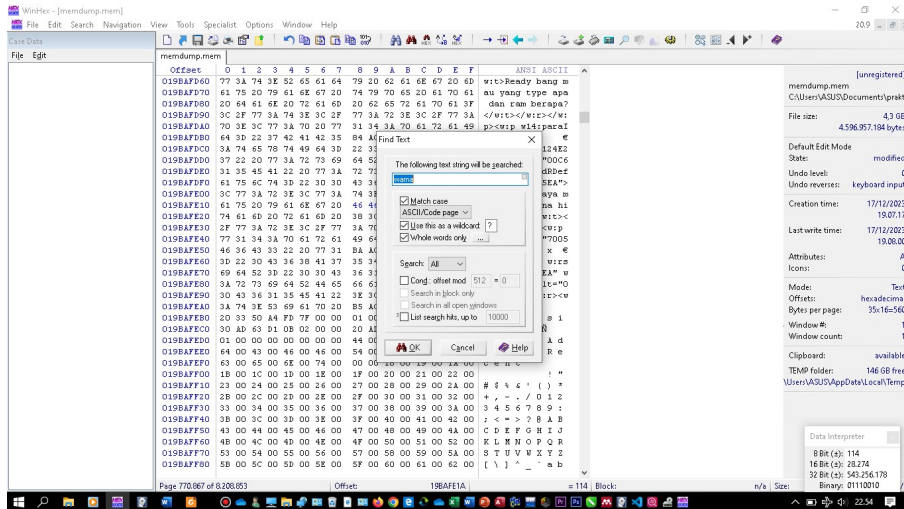
Proses yang dilakukan pada tahap analisis selanjutnya menggunakan bukti digital hasil dari *Imaging*. Dari proses pengambilan bukti yang asli atau bukti digital akan disimpan untuk mengantisipasi kesalahan pada saat proses analisis dilakukan.

C. *Pemrosesan Bukti Digital WinHex*

Untuk mendukung proses identifikasi dan untuk mendapatkan bukti digital maksimum dan dapat digunakan sebagai bukti digital yang sah dan meningkatkan kepercayaan dalam proses pengadilan, analisis tambahan dilakukan dengan menggunakan *tools* forensik WinHex[1]. Penggunaan bukti digital dapat memengaruhi proses pengadilan dengan memberikan bukti elektronik yang kuat untuk mendukung atau menentang klaim hukum. Penggunaan bukti digital dapat memiliki dampak signifikan pada proses pengadilan. Bukti digital dapat menjadi kunci dalam menyelidiki kejahatan dan membantu memperkuat kasus. Namun, keberhasilan penggunaan buktidigital juga tergantung pada validasi, integritas, dan keandalan proses pengumpulan dan analisisnya.

1) Pengambilan Bukti Digital

Untuk mendapatkan bukti percakapan WhatsApp yang terdapat pada RAM dilakukan menggunakan teknik *Live Forensik*. Sedangkan *tools* yang digunakan adalah FTK Imager akan tetapi hasil dari capture memory tersebut akan dibuka menggunakan *tools* WinHex untuk mencari bukti digital. Gambar 4 menunjukkan proses mencari bukti digital.



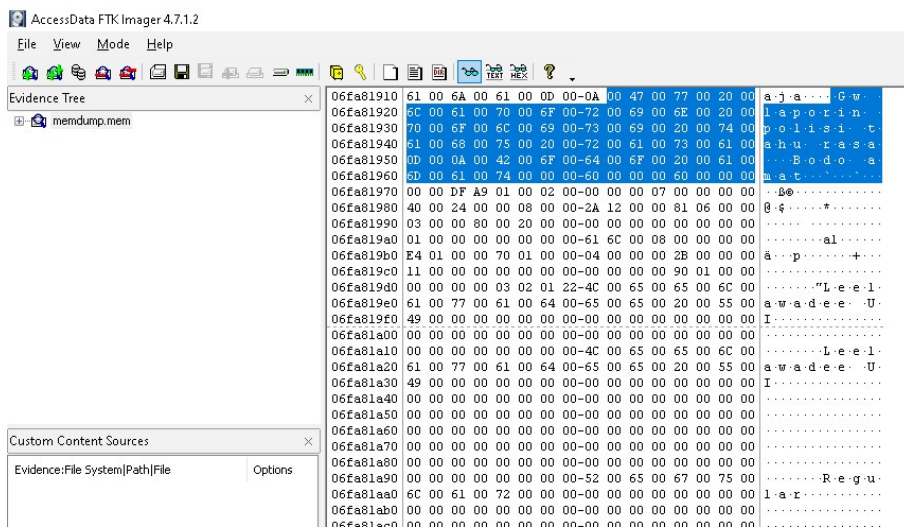
. Proses Pengambilan Bukti Digital

D. Analisis Bukti Digital

Pada tahapan ini, selanjutnya akan dilakukan analisis dari hasil pengambilan data menggunakan *tools* FTK Imager dan WinHex

1) Analisis Data Digital

Berdasarkan dari hasil proses pengambilan data pada RAM. Penyidik menemukan rekaman data percakapan yang dilakukan pelaku dan korban pada WhatsApp. Data yang dihasilkan adalah berupa teks percakapan WhatsApp, seperti yang ditunjukkan pada Gambar 4. Pada gambar tersebut menunjukkan salah satu data percakapan yang terjadi pada WhatsApp.



. Bukti Data Digital

Dari gambar di atas menunjukkan sebuah data yang didapat pada percakapan WhatsApp. Pada data tersebut tidak ada nomor telepon pengirim, penerima dan waktu kapan percakapan tersebut dilakukan, hanya berupa teks percakapan.

2) Analisa Bukti Digital

Berdasarkan hasil analisis data digital teks percakapan yang telah ditemukan akan dibandingkan dengan teks percakapan WhatsApp yang ada pada *smartphone* milik korban. Hasil menunjukkan perbandingan percakapan WhatsApp yang dilakukan di laptop tersangka dengan *smartphone* korban. Dari perbandingan tersebut disimpulkan bahwa teks percakapan sama, sehingga penyidik menjadikan data percakapan tersebut sebagai bukti digital kasus penipuan.

TABLE II.
 PERBANDINGAN PERCAKAPAN

Offsets	Isi Percakapan	Kesimpulan
00a52b6b0	WhatsApp Image 2023-11-22 at 10.09.00.jpg	Sama dan Terbukti
06fa81370	Realme 10	Sama dan Terbukti
06fa813c0	Masih ready bang?	Sama dan Terbukti
06fa81410	Ready bang mau yang type apa dan ram berapa?	Sama dan Terbukti
06fa81460	Saya mau yang warna hitam dan ram 8	Sama dan Terbukti
06fa814b0	Siap bang untuk harga 4.599.00	Sama dan Terbukti
06fa81500	Siap bang langsung order	Sama dan Terbukti
06fa815a0	Mohon kirim alamat bang untuk pengiriman barang	Sama dan Terbukti
06fa815f0	Bukti transfer No.Rek 5224-92-575349-53-6 atas nama afrida hidayati	Sama dan Terbukti
06fa81640	Alamat jl. kusuma rt: 05/01 kedawung Yogyakarta	Sama dan Terbukti
06fa81690	Untuk extimasi pengiriman 3-4 hari ditunggu saja	Sama dan Terbukti
06fa816f0	Paketnya ko belum sampai bang sudah seminggu ini. Minta resinya dong	Sama dan Terbukti
06fa81730	Barang sudah saya kirim bang untuk nomor resinya hilang	Sama dan Terbukti
06fa81780	Serius bang masa hilang si, apa kau nipu ya	Sama dan Terbukti
06fa817d0	Beneran bang barang sudah saya kirim. Ga percaya banget si tunggu laaa!!!	Sama dan Terbukti
06fa81820	Kok ngegass si kembaliin saja uang ku kalo gini	Sama dan Terbukti
06fa81870	Enak saja	Sama dan Terbukti
06fa818c0	Gw laporin polisi tahu rasa	Sama dan Terbukti
06fa81910	Bodo amat	Sama dan Terbukti

Pada tabel 2 menunjukkan adanya perbandingan percakapan yang dimana peneliti berhasil mendapatkan bukti digital terkait kasus tindakan kejahatan penipuan. Bukti digital ini yang didapatkan berupa data percakapan WhatsApp antara pelaku dan korban. Data percakapan ini hanya berupa teks percakapan, tidak ada nomor telepon pengirim serta penerima, dan waktu percakapan. Selain bukti teks percakapan juga terdapat sebuah file gambar/ Kecocokan *tools live forensics* dengan aplikasi *instant messenger* sangat mempengaruhi kelengkapan bukti digital yang didapat. Semakin lengkap bukti digital maka semakin cepat penyidik mengungkap kasus tindak kejahatan penipuan.

Pembuktian kasus penipuan *online* yang terjadi memerlukan tinjauan dari segi hukum agar pelaku dapat mempertanggung jawabkan perbuatannya sesuai dengan hukum yang berlaku. Pertama, pelaku berusaha menipu dan merugikan korban dengan berpura-pura menjual sebuah barang. Tindakan kejahatan dapat dijerat dengan UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 28 Ayat 1 Juncto Pasal 45a Ayat 1 Serta UU Nomor 9 Tahun 1981 Pasal 378 Kitab Undang-Undang Hukum Acara Pidana Ayat 1 dan 2 yang mengatur tentang penipuan

Selain itu setelah menipu korbanya pelaku menghapus semua riwayat percakapan pada WhatsApp yang berarti pelaku berusaha menghilangkan barang bukti. Maka perbuatannya tersebut dapat dijerat dengan UU Nomor 11 Tahun 2008 Tentang ITE Pasal 32 Ayat 1 Juncto Pasal 48 Ayat 1. Adapun metode yang digunakan untuk memperoleh bukti digital pada penelitian ini, yaitu ilmu Digital Forensik, dapat digunakan sebagai alat bukti yang sah di pengadilan karena termasuk keterangan ahli yang disebutkan di dalam UU Nomor 8 Tahun 1981 Pasal 184 Kitab Undang-Undang Hukum Acara Pidana Ayat 1. Bukti digital yang diperoleh pun dinyatakan sebagai alat bukti yang sah karena termasuk informasi/dokumen elektronik berdasarkan UU Nomor 11 Tahun 2008 Tentang ITE Pasal 5 Ayat 1 dan Pasal 6.

Penelitian ini juga dapat dilakukan pada simulasi kejahatan lainnya yang mendukung dengan *live forensics*. Kerumitan dalam mencari, mendapatkan, dan menganalisis suatu bukti digital yang ada disaat aplikasi sedang berjalan pada laptop membutuhkan pengetahuan, kemampuan, pengalaman dan waktu yang lama. Hal tersebut juga sangat dibutuhkan *tools forensics* yang mendukung untuk mendapatkan bukti digital yang berkualitas.

IV. KESIMPULAN

Berdasarkan penelitian yang dilakukan pencarian bukti digital dari aplikasi IM WhatsApp berbasis *desktop* pada sistem operasi Windows 10 menggunakan metode *Tools Forensik FTK Imager* dan *WinHex*. Bukti yang diperoleh berupa teks percakapan WhatsApp yang terjadi antara tersangka dan korban yang dapat dijadikan bukti digital terkait kasus kejahatan penipuan *online shop*. Pembuktian kasus penipuan ini dilakukan dengan membandingkan atau sinkronisasi antara bukti digital teks percakapan yang telah diperoleh dari laptop pelaku dengan percakapan

WhatsApp pada *smartphone* korban. Beberapa saran untuk penelitian selanjutnya adalah terdapat beberapa macam metode forensik digital, aplikasi IM berbasis dekstop, dan sistem operasi komputer yang bisa dikombinasikan menjadi topik penelitian yang kemungkinan besar mendukung teknik *live forensics* dan mendapatkan hasil penelitian yang berbeda dan lebih akurat. Penggunaan *tools live forensics* dalam proses pengambilan dan analisis bukti digital dapat juga dikombinasikan dengan *tools* lainnya, agar memperoleh bukti digital yang berkualitas sehingga dapat membantu para penyidik dalam mengungkap sebuah tindak kejahatan yang terjadi

DAFTAR PUSTAKA

- [1] T. Rochmadi, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," *Indones. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.
- [2] A. H. Muhammad and A. Purwanto, "Identifikasi level tata kelola ti dan penilaian tingkat capability level menggunakan cobit 2019," vol. 8, no. 3, pp. 815–827, 2023.
- [3] A. K. A. I. Access, "Implementasi machine learning sebagai analisis kepuasan pelanggan terhadap penggunaan aplikasi kai access," vol. 8, no. 4, pp. 1248–1255, 2023.
- [4] S. Rachmie, "DIGITAL WEBSITE," vol. 21, no. 1, pp. 104–127, 2020.
- [5] S. Di, W. Jakarta, and S. Berbasis, "Metode haversine formula pada pencarian rumah sakit di wilayah jakarta selatan berbasis android," vol. 8, no. 4, pp. 1142–1153, 2023.
- [6] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics," *Semin. Nas. Inform. 2008 (semnasIF 2008)*, vol. 2018, no. November, pp. 86–91, 2018.
- [7] P. Xyz and M. Flask, "Pengembangan aplikasi," vol. 8, no. 4, pp. 1288–1299, 2023.
- [8] M. N. Faiz, R. Umar, and A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Keamanan Email Pada Sistem Operasi Proprietary," *Ilk. J. Ilm.*, vol. 8, no. 3, pp. 242–247, 2016, doi: 10.33096/ilkom.v8i3.79.242-247.
- [9] A. Yudhana, I. Riadi, and I. Zuhriyanto, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," *J. TECHNO*, vol. 20, no. 2, pp. 125–130, 2019.
- [10] I. Nizar, L. Handayani, and S. A. Sudiro, "Machine Translated by Google MENCIPTAKAN KUALIFIKASI PRODUK BERBASIS BLOCKCHAIN SISTEM E-MARKETPLACE MENGGUNAKAN PRAKTIS ALGORITMA TOLERANSI KESALAHAN BYZANTINE," pp. 1111–1120, 2023.
- [11] U. Kristen and S. Wacana, "Implementasi python framework flask pada modul transfer out toko di pt xyz," vol. 8, no. 4, pp. 1121–1131, 2023.
- [12] S. A. Ardana, F. Sukmana, and H. D. Bhakti, "Evaluasi kualitas," vol. 8, no. 4, pp. 1439–1450, 2023.
- [13] I. Saputra and M. Nauval Azhar, "Seminar Nasional dan Diskusi Panel Multidisiplin Hasil Penelitian & Pengabdian kepada Masyarakat, Jakarta, 2 Agustus 2018 ANALISIS DAN INVESTIGASI FORENSIK DIGITAL LIVE MEMORY UNTUK DETEKSI TINGKAH LAKU AGRESI PADA APLIKASI WHATSAPP," pp. 119–125, 2018.
- [14] T. D. Larasati and B. C. Hidayanto, "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10," *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.
- [15] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 1, no. 3, pp. 108–114, 2017, doi: 10.14421/jiska.2017.13-02.
- [16] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," vol. 7, no. 1, pp. 43–48, 2022.
- [17] N. Wahyuningsih, "Perbandingan metode klasifikasi dalam analisis sentimen masyarakat terhadap identitas kependudukan digital (ikd)," vol. 8, no. 4, pp. 1218–1227, 2023.
- [18] 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.
- [19] N. I. Pamungkas, "Sistem informasi penjualan tas berbasis web pada toko tas ud. a&n collection tanggulangin dengan metode waterfall," vol. 8, no. 4, pp. 1467–1478, 2023.
- [20] W. Purnama and E. Supratman, "Sistem informasi pusat layanan psikologi universitas bina darma berbasis website," vol. 8, no. 3, pp. 1074–1081, 2023.