RABIT : Jurnal Teknologi dan Sistem Informasi Univrab
Volume 10 No. 1 | Januari 2025 : Hal : 117-129

ISSN CETAK : 2477-2062
ISSN ONLINE : 2502-891X

IDENTIFIKASI BUKTI DIGITAL PINJAMAN ONLINE MENGGUNAKAN *LIVE FORENSIC* PADA SISTEM OPERASI *PROPRIETARY*

[1)] Islahiyatul Ilma Mubarokah, [2)] Fahmi Fachri
[1,2)]Teknik Informatika, Fakultas Teknik, Universitas Maarif Nahdlatul Ulama Kebumen
[1,2)] Jl. Kutoarjo KM 05 Jatisari – Jawa Tengah - Indonesia
E-mail : *ilislahiya@gmail.com, fahmifachriumnu@gmail.com*

ABSTRAK
Teknologi informasi dan komunikasi berkembang pesat seiring dengan peningkatan kualitas hidup manusia. Namun, kemajuan ini juga memunculkan berbagai tantangan, termasuk meningkatnya kejahatan dunia maya (*cybercrime*). Salah satu tantangan tersebut adalah upaya pelaku kejahatan untuk menghapus barang bukti elektronik yang tersimpan dalam *Random Access Memory* (RAM) guna menghindari jerat hukum. Penelitian ini bertujuan untuk melakukan analisis forensik digital dengan fokus pada pemulihan barang bukti yang telah dihapus. Metode yang digunakan dalam penelitian ini mengikuti pedoman dari *National Institute of Standards and Technology* (NIST), yang mencakup empat tahap utama: pengumpulan, perolehan, analisis, dan pelaporan. Untuk mendukung proses pemulihan bukti digital, alat forensik yang digunakan termasuk perangkat lunak yang umum digunakan dalam bidang ini, seperti *FTK Imager* dan *WinHex*. Alat-alat ini digunakan untuk mengevaluasi efektivitas dalam memulihkan data penting, seperti percakapan *WhatsApp* yang berkaitan dengan kasus penipuan pinjaman online. Hasil penelitian menunjukkan tingkat keberhasilan yang signifikan dalam memulihkan bukti digital yang relevan. Sebagai contoh, lebih dari 85% dari data yang dihapus berhasil dipulihkan menggunakan metode yang diterapkan. Temuan ini menunjukkan bahwa teknik forensik digital yang digunakan dapat memberikan kontribusi besar dalam mengatasi tantangan penghapusan barang bukti elektronik, khususnya dalam kasus *cybercrime*. Penelitian ini juga berkontribusi pada pengembangan teknik *live forensics* untuk meningkatkan efektivitas dalam investigasi kejahatan dunia maya

Kata Kunci: Digital Forensik, Live Forensik, Penipuan, Whatshapp web

ABSTRACT
Information and communication technology is rapidly evolving in line with the improvement in human quality of life. However, this advancement also presents various challenges, including the rise of cybercrime. One of these challenges is the efforts of perpetrators to delete electronic evidence stored in Random Access Memory (RAM) to avoid legal consequences. This study aims to conduct a digital forensic analysis with a focus on recovering deleted evidence. The method used in this research follows the guidelines of the National Institute of Standards and Technology (NIST), which includes four main stages: collection, acquisition, analysis, and reporting. To support the recovery process of digital evidence, forensic tools used include software commonly used in this field, such as FTK Imager and WinHex. These tools are employed to evaluate the effectiveness in recovering crucial data, such as WhatsApp conversation texts related to an online loan fraud case. The results of the study show a significant success rate in recovering relevant digital evidence. For instance, over 85% of deleted data was successfully recovered using the applied methods. These findings demonstrate that the digital forensic techniques used can provide a major contribution in addressing the challenges of electronic evidence deletion, particularly in cybercrime cases. This research also contributes to the development of live forensics techniques to enhance the effectiveness of investigations into cybercrimes.

Keyword*: Digital forensic, live forensic, fraud, whatsapp web*

PENDAHULUAN

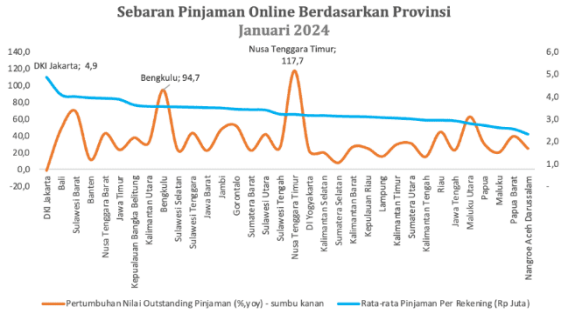
Kemajuan teknologi informasi dan komunikasi saat ini mengalami peningkatan yang signifikan, seiring dengan peningkatan kualitas hidup manusia [1]. Internet, selain digunakan sebagai alat komunikasi dan pertukaran informasi, juga menjadi salah satu perkembangan dalam berbagai aspek kehidupan modern, termasuk bisnis, pendidikan, dan hiburan [2]. Setiap inovasi diciptakan untuk memberikan manfaat positif bagi kehidupan manusia, seperti kemudahan dalam pencarian informasi, kemudahan dalam proses pembelajaran, pengolahan data, dan berbagai kemudahan lainnya [3].

DOI : https://doi.org/10.36341/rabit.v10i1.5514

Meningkatnya penggunaan teknologi informasi tidak lepas dari peran *smartphone*, yang menyediakan berbagai aplikasi dan fungsi. Salah satu aplikasi yang banyak digunakan adalah aplikasi pesan instan (*Instant Messaging*/IM), seperti *WhatsApp* [4]. Meski memiliki banyak manfaat, *smartphone* juga berpotensi menjadi alat dalam tindak kejahatan siber. Pelaku kejahatan siber dapat memanfaatkan berbagai fungsi yang tersedia di *smartphone* untuk melakukan tindakan kriminal. Kejahatan siber merupakan bentuk akses ilegal terhadap suatu data menggunakan komputer, terutama untuk mengakses, mengirimkan, atau memanipulasi data [5]

Salah satu jenis kejahatan siber yang sering terjadi di Indonesia adalah penipuan. Pelaku penipuan sering menggunakan cara atau modus baru untuk mengelabui korbannya, sehingga perbuatannya tidak disadari [6]. Tindak pidana penipuan secara online diatur dalam Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Secara spesifik, Pasal 28 ayat (1) UU ITE mengatur tentang penipuan dengan memberikan informasi palsu melalui media elektronik, sehingga pelaku yang melanggar ketentuan tersebut dianggap telah melakukan tindak pidana penipuan. Ancaman pidananya diatur dalam Pasal 45A ayat (1) UU ITE, yaitu hukuman penjara paling lama enam tahun dan/atau denda maksimal Rp1.000.000.000,00 (satu miliar rupiah) [7].

Salah satu bentuk tindak kejahatan di dunia maya adalah penipuan pinjaman online, yang modusnya semakin canggih dan sulit terdeteksi oleh masyarakat awam. Entitas pinjaman online ilegal yang beroperasi di luar pengawasan lembaga keuangan resmi semakin memperumit situasi. Penipuan pinjaman online seringkali terjadi akibat kurangnya pemahaman masyarakat tentang literasi keuangan [8]. Pelaku biasanya mengirimkan tautan phishing atau situs online yang mengarahkan korban untuk segera mengajukan pinjaman, tanpa memastikan validitas situs tersebut [9].



Gambar 1. Sebaran Pinjaman Online

Tingginya angka kejahatan penipuan pinjaman online di platform *WhatsApp* menjadi masalah utama di Indonesia. Berdasarkan permasalahan tersebut, diperlukan upaya untuk menangani dan menindaklanjuti kejahatan yang dilakukan oleh pelaku. Salah satu pendekatan yang digunakan untuk mengumpulkan bukti digital terkait kasus kejahatan ini dikenal dengan istilah forensik digital. Forensik digital adalah ilmu yang mempelajari cara menangani berbagai kejahatan yang melibatkan teknologi komputer [10].

Ada beberapa teknik dalam forensik digital, salah satunya adalah *Live Forensics*, yang digunakan untuk menganalisis keamanan web. Teknik ini dilakukan secara langsung saat perangkat masih aktif dan dapat menghasilkan bukti ilmiah terkait keamanan situs web yang terhubung pada jaringan komputer [11]. Salah satu metode dalam mengungkap kejahatan melalui forensik digital adalah menggunakan standar *NIST (National Institute of Standards and Technology)*. Standar *NIST* membantu mempermudah pekerjaan penyidik dalam memahami alur penyelidikan secara sistematis dan lebih terstruktur, sehingga data yang telah dihapus atau disembunyikan dapat ditemukan [12].

Pengguna aplikasi pada komputer meninggalkan data dan informasi pada *Random Access Memory (RAM)*. *RAM* adalah memori tempat penyimpanan sementara saat komputer sedang dijalankan. Data dan informasi pada *RAM* harus ditangani dengan hati-hati karena data tersebut dapat hilang jika sistem mati. Meski demikian, data dan informasi pada *RAM* memiliki potensi menjadi

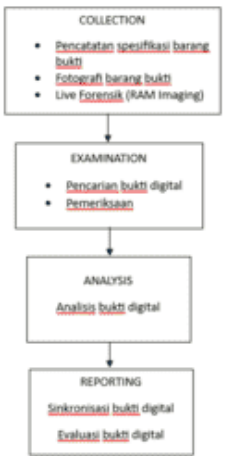
DOI : https://doi.org/10.36341/rabit.v10i1.5514 *Corresponding Author* : Fahmi Fachri

bukti digital yang dapat diolah untuk investigasi [13].

Dalam bidang forensik digital, terdapat berbagai alat yang digunakan untuk penyelidikan. Dalam penelitian ini, digunakan dua alat utama, yaitu *FTK Imager* dan *WinHex*. *FTK Imager* adalah perangkat lunak forensik yang digunakan untuk memperoleh gambar atau salinan forensik dari penyimpanan data, seperti *hard drive, USB drive*, dan kartu memori [14]. *FTK Imager* juga dapat menemukan bukti yang telah dihapus pada program *Google Chrome* di direktori laptop, sekaligus mendapatkan *data file* dan *log* [15]. Sementara itu, *WinHex* adalah perangkat lunak editor hexadesimal universal yang digunakan untuk pemulihan data yang sudah dihapus atau data yang hilang dari *hard drive* akibat sistem file yang rusak. Sistem Operasi *Proprietary* merujuk pada sistem operasi yang memiliki lisensi tertutup dan hak milik yang dikendalikan oleh satu entitas atau perusahaan. Artinya, hanya pemilik lisensi yang dapat mengakses, memodifikasi, atau mendistribusikan perangkat lunak tersebut. Pengguna sistem operasi *proprietary* biasanya tidak dapat melihat atau mengubah kode sumber (*source code*) dari sistem tersebut. Contoh dari sistem operasi proprietary adalah *Microsoft Windows* dan *macOS*, yang keduanya dimiliki dan dikembangkan oleh perusahaan tertentu, yaitu *Microsoft* dan *Apple* [16].

METODE PENELITIAN

Penelitian ini menggunakan pendekatan *kualitatif* untuk menggali dan memahami secara mendalam kasus penipuan yang melibatkan aplikasi *WhatsApp* dengan metode *studi literatur*. Dalam penelitian ini, skenario yang dibuat berdasarkan kasus penipuan pinjaman online yang telah banyak terjadi, dengan melibatkan *pelaku* yang menawarkan pinjaman dan *korban* yang memberikan data pribadi mereka. Pelaku mengancam korban dengan menyebarkan data pribadi jika korban tidak mentransfer uang, kemudian pelaku mengirimkan *tautan phishing* yang menurut korban mencurigakan. Data yang digunakan dalam penelitian ini diperoleh melalui *simulasi* kasus penipuan dengan melibatkan data yang bersifat fiktif yang didesain untuk menciptakan skenario yang realistis. *Simulasi* ini dilakukan dengan hati-hati untuk memastikan bahwa data yang digunakan tidak melibatkan individu atau informasi pribadi yang sebenarnya, sehingga pengumpulan data dilakukan secara *etis*. Dalam tahap berikutnya, bukti dari percakapan dan ancaman yang dilakukan oleh pelaku akan dijadikan sebagai barang bukti. Barang bukti tersebut diperoleh dari sebuah *laptop* yang digunakan oleh pelaku dan akan dianalisis menggunakan alat *forensik digital*, yaitu *FTK Imager* dan *WinHex*. Untuk memastikan *validitas* dan *reliabilitas* hasil penelitian, alat forensik yang digunakan telah terbukti secara ilmiah dalam mengidentifikasi dan memulihkan data yang telah dihapus atau dihilangkan. Metode yang digunakan mengikuti pedoman dari *National Institute of Standards and Technology* (*NIST*), yang mencakup empat langkah utama: *pengumpulan*, *perolehan*, *analisis*, dan *pelaporan*. Dengan menggunakan metode ini, data yang telah hilang dapat dipulihkan dan dianalisis meskipun data tersebut telah dihapus atau dimodifikasi [17].



Gambar 2. Tahapan Penelitian

DOI : https://doi.org/10.36341/rabit.v10i1.5514 *Corresponding Author* : Fahmi Fachri

Langkah-langkah metode NIST sebagai berikut:

1. *Collection*

Langkah pertama adalah *Collection* atau pengumpulan barang bukti digital. Tahap ini mencakup persiapan, pengumpulan, dokumentasi, dan isolasi barang bukti. Persiapan melibatkan identifikasi awal perangkat yang relevan dengan kasus serta pemeriksaan kondisi perangkat keras dan lunak. Selanjutnya, data dari perangkat target, seperti *hard drive, USB*, kartu memori, atau *RAM*, diambil dengan hati-hati untuk menghindari kerusakan. Setiap barang bukti didokumentasikan secara rinci, termasuk spesifikasinya, melalui catatan, foto, atau video. Selain itu, perangkat diisolasi secara fisik dan logis untuk mencegah modifikasi lebih lanjut, misalnya dengan menggunakan perangkat *write-blocker*. Pada tahap ini, proses *Live Forensics,* seperti *RAM Imaging*, sering dilakukan untuk mendapatkan salinan data yang tersimpan sementara di memori.

2. Examination

Langkah kedua adalah *Examination* atau pemeriksaan barang bukti. Data yang telah dikumpulkan dimasukkan ke dalam perangkat lunak forensik, seperti *FTK Imager*, untuk memulai proses pemeriksaan. Perangkat lunak ini akan mencari, memfilter, dan mengelompokkan data berdasarkan kategori tertentu, seperti dokumen, gambar, atau log sistem. Tahapan ini bertujuan untuk menyaring data yang tidak relevan dan mengidentifikasi bukti awal yang berkaitan langsung dengan kasus. Pemeriksaan ini penting untuk memastikan bahwa hanya data yang relevan yang diteruskan ke tahap analisis lebih lanjut.

3. *Analysis*

Langkah berikutnya adalah *Analysis* atau analisis data. Pada tahap ini, data yang telah diperoleh dari pemeriksaan dianalisis lebih mendalam untuk mengidentifikasi informasi penting yang relevan dengan kasus. Proses ini melibatkan pemrosesan data menggunakan alat seperti *FTK Imager* untuk memverifikasi keabsahan dan keutuhan file, serta alat seperti *WinHex* untuk memulihkan data yang telah dihapus atau memeriksa metadata file. Analisis ini membantu menentukan keterkaitan antara bukti digital yang ditemukan dengan aktivitas atau kronologi kejadian yang sedang diselidiki. Hasil dari tahap ini berupa bukti digital yang siap diajukan sebagai bagian dari investigasi.

4. *Report*

Langkah terakhir adalah *Reporting* atau pelaporan. Tahap ini berfokus pada penyusunan laporan yang merangkum seluruh proses investigasi. Laporan ini mencakup langkah-langkah yang telah dilakukan, mulai dari pengumpulan barang bukti, pemeriksaan, hingga analisis. Selain itu, laporan menyertakan dokumentasi waktu, seperti kapan pengambilan gambar (*imaging*) dan analisis dilakukan, serta perbandingan file asli dengan hasil ekstraksi untuk memastikan integritas data. Hasil investigasi disajikan secara sistematis dalam laporan ini, termasuk bukti digital yang ditemukan, metode analisis yang digunakan, dan relevansinya dengan kasus. Laporan ini sangat penting karena menjadi dokumen resmi yang digunakan dalam proses hukum atau penyidikan lebih lanjut.

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

No.	Kategori	Spesifikasi
1.	*Hardware*	Laptop HP 14s-fq1 Device name WINDOWS-LF8EC89 Processor AMD Ryzen 3 5300U with Radeon Graphics 2.60 GHz Installed RAM

DOI : https://doi.org/10.36341/rabit.v10i1.5514 *Corresponding Author* : Fahmi Fachri

		8,00 GB (7,33 GB usable) Device ID 579B4453-5B27-4E04-8EE8-A385FC6ED054 Product ID 00330-80000-00000-AA922 System type 64-bit operating system, x64-based processor Smartphone Iphone 11
2.	*Software*	Sistem operasi Windows 11
		FTK Imager versi 4.7.1.2 WinHex versi 20.6

Tabel 1. Alat dan Bahan Penelitian

Barang bukti laptop pelaku digunakan untuk mencaari bukti digital yang berkaitan dengan kasus pinjaman *online* yang terjadi. Barang bukti *smartphone* milik korban hanya dijadikan sebagai pembanding antara bukti digital yang telah diperoleh dari laptop pelaku dengan percakapan *whatshapp* pada *smartphone* korban.

A. RANCANGAN SIMULASI

Simulasi kasus penipuan pinjaman online melalui percakapan *Whatshapp* dilakukan karena didasari pada aturan berikut ini:

1) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 5 huruf a.

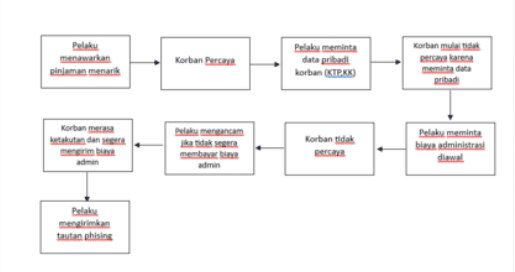
2) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 6 huruf a.

3) Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Pasal 7 ayat 1.[18]

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

Saat ini di Indonesia, tindak pidana *cybercrime* berupa phishing dapat dikenakan sanksi berdasarkan Pasal 35 dan Pasal 51 ayat (1) dari Undang-Undang ITE, karena phishing melibatkan pembuatan situs palsu yang menyerupai situs resmi untuk menipu korban. Selain itu, pelaku phishing juga dapat dikenakan Pasal 28 ayat (1) jo Pasal 45A ayat (1) yang mengatur tentang penipuan digital, di mana pelaku mengarahkan korban untuk mengakses tautan yang mengarah ke situs palsu, meminta informasi pribadi, dan mengakibatkan kerugian bagi korban.[9]

Rancangan sistem merupakan gambaran awal dari sistem yang akan dibuat. Pada rancangan sistem akan terlihat alur atau proses yang terjadi pada sistem.[19]Simulasi pada penelitian ini dilakukan untuk menggambarkan langkah-langkah penelitian yang dilakukan antara korban dan pelaku. Korban menggunakan aplikasi WhatsApp pada *smartphone* pribadi, sedangkan pelaku menggunakan aplikasi WhatsApp web pada komputer miliknya yang dijalankan pada *browser Google chrome* mode normal. Berikut ini merupakan gambaran simulasi kasus penipuan pinjaman online.



Gambar 3. Simulasi Penelitian

Penelitian ini dengan metode live *forensic*. Simulasi kasus penipuan pinjaman online melalui percakapan whatshapp web antara pelaku dan korban. Urutan hasil penelitian mengikuti tahapan framework digital forensic *NIST* yang digunakan.

HASIL

Penelitian ini dilakukan dengan menggunakan laptop bermerek HP dengan Windows 11 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. Maka dari itu penelitian ini menggunaakn metode *live forensic* dengan mengikuti tahapan framework digital forensic *NIST* yang digunakan.

A. Pengumpulan Barang Bukti

Langkah pertama penelitian ini yaitu 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. Pada tahapan ini menghasilkan beberapa catatan dan dokumentasi barang bukti yang terlibat dalam kasus ini meskipun *smartphone* korban hanya dijadikan sebagai penbanding dan tidak dianalisis lebih lanjut.

Tabel 2.Spesifikasi perangkat bukti

No.	Kategori	Spesifikasi
1.	*Laptop*	Laptop HP 14s-fq1 Processor AMD Ryzen 3 5300U with Radeon Graphics 2.60 GHz Installed RAM 8,00 GB (7,33 GB usable)
2.	*Smartphone*	Iphone 11 Versi Ios 17.4.1 RAM 64GB

Gambar 4. Dokumentasi Barang Bukti Laptop Pelaku

Gambar 5. Barang Bukti Smartphone Korban

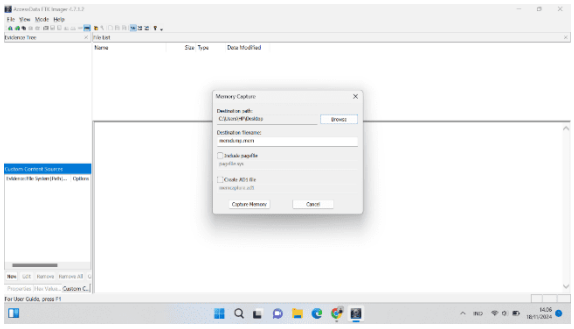
B. Pemrosesan Bukti Digital *FTK Imager*

Setelah pencatatan dan dokumentasi barang bukti, selanjutnya dilakukan proses *live forensic* pengumpulan barang bukti digital yang terdapat pada RAM dengan perangkat yang masih dijalankan.

1. Pengambilan Bukti Digital

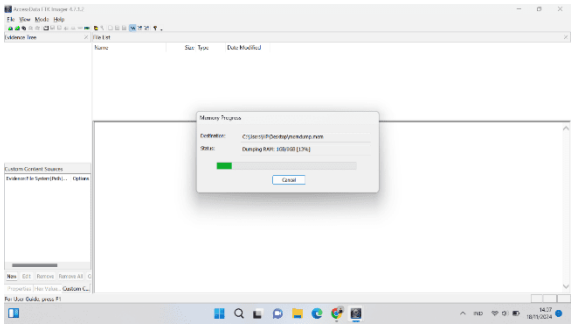
Untuk mendapatkan bukti percapakan *WhatsApp* yang terdapat pada RAM dilakukan dengan menggunkan teknik *Live Forensics*. Sedangkan Tools yang digunakan pada penelitian ini adalan *FTK Imager* karena memiliki kegunaan seperti *Capture Memory* yang sangat mendukung *Live Forensics*. Fitur ini dapat mengambil data dan informasi yang

terdapat pada RAM, termasuk percakapan. Gambar 6 menunjukkan sebuah proses pengambilan data pada RAM.



Gambar 6.Proses Meng capture Memory

FTK Imager mengambil semua data dan informasi dari aplikasi yang sedang berjalan pada laptop termasuk data percakapan WhatsApp yang telah dihapus. Gambar 7 menunjukan sebuah proses pengambilan data pada RAM.

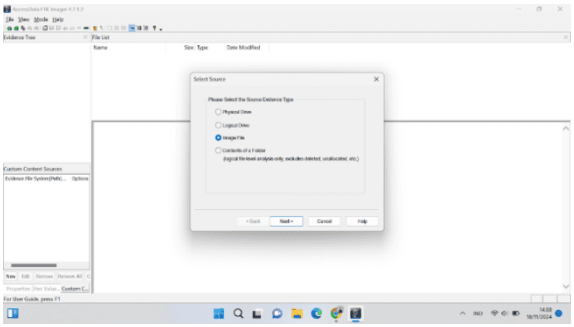


Gambar 7. Proses Pengambilan Data

Proses RAM imaging untuk mendapatkan bukti digital RAM imaging yang dilakukan menggunakan tools *FTK Imager*.Lamanya proses pengambilan data tergantung besar kecilnya kapasitas RAM jika semakin besar kapasitas maka semakin lama proses pengambilan bukti digitalnya. Hasil dari proses pengambilan bukti digital berupa file berekstensi .mem. Jenis file ini dapat dibuka dan dianalisis menggunakan tools yang mendukung ekstensi file tersebut, salah satunya adalah *FTK Imager*

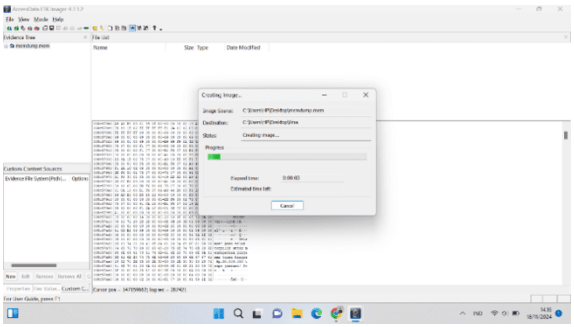
2. Proses Imaging

   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 asli.



Gambar 8. Select image file pada select source

Pada bagian *select sorce*, pilih *image file* karena prenelitian ini menggunakan memory capture. Pada bagian select file, pilih lokasi dimana hasil capture image disimpan.



Gambar 9. Proses Imaging

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

C. Pemrosesan Bukti Digital Winhex

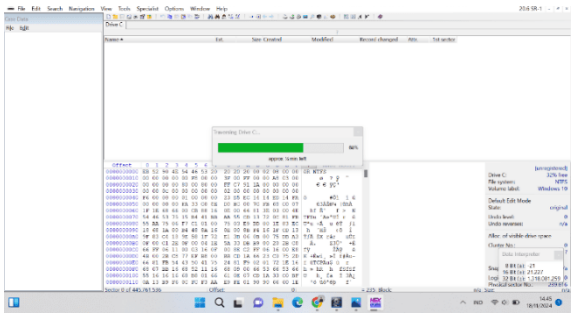
   Tahapan selanjutnya memanfaatkan tools winhex untuk menemukan bukti-bukti digital yang maksimum dari penipuan pinjaman online yang terjadi, yang mana dapat diketahui bentuk file dari bukti digital seperti text, gambar, atau video. Bukti digital dapat menjadi kunci dalam menyelidik kejahatan dan membantu memperkuat kasus. Namun,

DOI : https://doi.org/10.36341/rabit.v10i1.5514
Corresponding Author : Fahmi Fachri

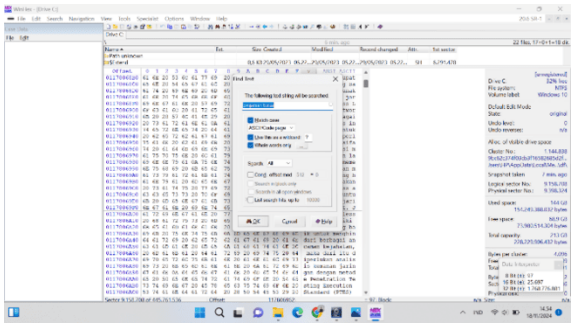
keberhasilan penggunaan bukti digital juga tergantung pada validasi, integritas, dan keandalan proses pengumpulan dan analisanya.

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 10 menunjukkan proses mencari bukti digital.



Gambar 10. Proses pada Winhex



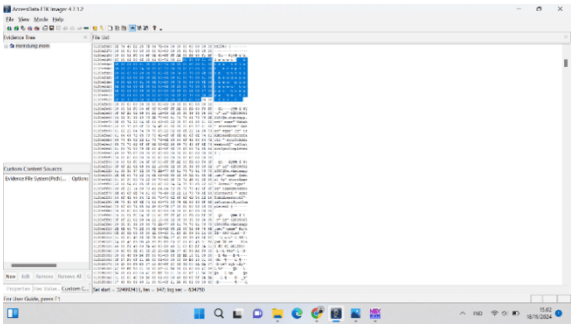
Gambar 11. Proses Pengambilan Bukti Digital pada Winhex

D. Analisis

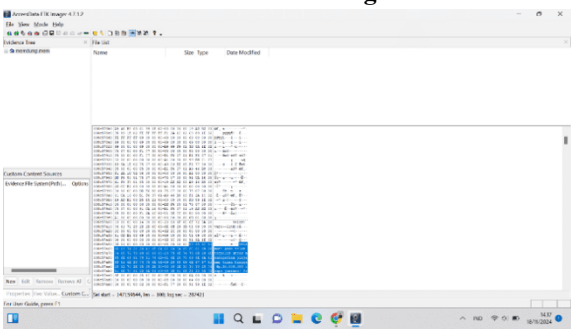
Pada tahapan ini, selanjutnya akan dilakukan analisis dari hasil pengambilan data menggunakan *tools FTK Imager* dan *Winhex.*

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 ditunjukan pada Gambar 12 dan gambar 13 .Pada gambar tersebut menunjukkan salah satu data percakapan yang terjadi pada WhatsApp.



Gambar 12. Bukti Data Digital



Gambar 13. 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. Analisis 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 perandingan percakapan WhatsApp yang dilakukan di laptop tersangka dengan smartphone korban. Dari perbandingan tesebut disimpulkan bahwa teks percakapan sama, sehingga penyidik menjadikan data percakapan tersebut sebagai

DOI : https://doi.org/10.36341/rabit.v10i1.5514
Corresponding Author : Fahmi Fachri

bukti digital kasus penipuan.

Tabel 3 Perbandingan Percakapan

Offsets	Isi Percakapan	Kesimpulan
0135efd90	Selamat! Anda telah terpilih untuk mendapatkan pinjaman tunai hingga Rp50.000.000 tanpa jaminan! Proses cepat, bunga rendah. Minat?	Sama dan Terbukti
054e27640	Terima kasih atas penawarannya. Namun, saya ingin memastikan apakah ini penawaran resmi dari perusahaan Anda? Bisakah Anda memberikan informasi lebih lanjut mengenai perusahaan dan syarat-syarat pinjamannya?	Sama dan Terbukti
0815d8000	Untuk proses verifikasi, mohon kirimkan foto KTP dan KK Anda beserta selfie dengan kedua dokumen tersebut.	Sama dan Terbukti
08d75d7e0	Mohon maaf, saya tidak nyaman memberikan data pribadi saya secara sembarangan. Apakah tidak ada cara lain untuk melakukan verifikasi selain mengirimkan foto dokumen asli?	Sama dan Terbukti
08ea03e10	Sebelum dana cair, Anda perlu membayar biaya administrasi sebesar Rp100.000. Silakan transfer ke nomor rekening ini 00345xxxxx	Sama dan Terbukti
08f09dla0	Mohon maaf, saya tidak pernah mendengar tentang biaya administrasi yang harus dibayar di awal untuk proses pinjaman. Saya akan mencari informasi lebih lanjut mengenai hal ini.	Sama dan Terbukti
08f297a80	Jika Anda tidak segera membayar, kami akan melaporkan Anda ke pihak berwajib dan menyebarkan data pribadi Anda!	Sama dan Terbukti
0995bf800	09Saya akan melaporkan tindakan ancaman dan intimidasi Anda ke pihak berwajib. Jangan coba-coba mengganggu saya lagi.	Sama dan Terbukti
09a8b0020	Silahkan klik tautan ini untuk mengisi formulir pengajuan pinjaman https://pendaftaran.pinajaman.com	Sama dan Terbukti
09cd3	: Saya tidak akan	Sam

cf60	mengklik tautan yang tidak jelas sumbernya. Saya akan mencari informasi mengenai perusahaan Anda melalui website resmi.	a dan Terbukti

Percakapan yang dimana peneliti berhasil mendapatkan bukti digital terkait kasus tindakan kejahatan penipuan pinjaman online .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 pinjaman online.

Pembuktian kasus penipuan pinjaman online yang terjadi memerlukan tinjauan dari segi hukum agar pelaku dapat mempertanggung jawabkan perbuatanya sesuai dengan hukum yang berlaku. Pengaturan perlindungan hukum terhadap korban tindak pidana penipuan melalui aplikasi digital dapat berpedoman pada Pasal 378 KUHP, Pasal 263 KUHP terbaru dan Pasal 28 ayat (1) UU ITE dengan cara menjatuhkan pidana terhadap pelaku sebagai bentuk pertanggungjawaban pelaku terhadap korban, serta Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dengan cara meminta pertanggungjawaban bank sebagai penyedia jasa terhadap kerugian yang dialami oleh korban. Ancaman untuk pelanggaran pada Pasal 28 ayat (1) UU ITE dapat dipidana penjara paling lama enam tahun dan /atau denda paling banyak Rp 1.000.000.000,- (satu miliar rupiah) sesuai dengan ketentuan yang terdapat dalam pasal 45 A ayat (1) UU ITE.[21]

Selain itu setelah menipu korbanya pelaku menghapus semua riwayat percakapan pada *WhatsApp* yang berati 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 lainya 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 forensic*s yang mendukung untuk mendapatkan bukti digital yang berkualitas.

Penelitian ini memberikan kontribusi signifikan dengan menerapkan metode *live forensics* menggunakan *framework digital forensics NIST* pada kasus penipuan melalui aplikasi digital. Penelitian sebelumnya seperti yang dilakukan oleh Agustiono (2024) telah mengeksplorasi metode forensik digital,

DOI : https://doi.org/10.36341/rabit.v10i1.5514 *Corresponding Author* : Fahmi Fachri

namun kebanyakan fokus pada analisis data statis pada perangkat yang telah dimatikan. Kontribusi penelitian ini terletak pada penggunaan metode *live forensic*s untuk mengakses data yang masih aktif, termasuk percakapan *WhatsApp* yang telah dihapus, dengan memanfaatkan perangkat lunak seperti *FTK Imager* dan *WinHex*.

Penelitian ini menemukan bahwa metode live forensics memungkinkan pengambilan data digital dari memori aktif (RAM) tanpa mematikan perangkat, yang relevan untuk menjaga integritas bukti digital. Sebagai perbandingan, penelitian sebelumnya hanya mendokumentasikan bukti digital dari memori penyimpanan permanen seperti hard drive, yang memiliki risiko kehilangan data akibat perubahan status perangkat.

KESIMPULAN

Penerapan teknik *live forensics* dalam pencarian bukti digital dari aplikasi *WhatsApp* berbasis desktop pada sistem operasi *Windows 11* telah menunjukkan hasil yang signifikan. Bukti digital berupa teks percakapan yang diperoleh dapat menjadi dasar yang kuat untuk mengungkap kasus penipuan pinjaman online dengan membandingkan atau menyinkronkan percakapan antara perangkat tersangka dan korban. Proses investigasi ini dilakukan dengan menggunakan alat forensik digital yang memfasilitasi pengumpulan data tanpa merusak perangkat asli, sehingga memastikan integritas bukti. Penggunaan alat seperti *FTK Imager* dan *WinHex* memungkinkan pengumpulan bukti secara langsung dari perangkat tanpa merusak data yang ada, yang pada gilirannya memperkuat validitas bukti di pengadilan.

Selain teks percakapan, dalam proses investigasi ini juga dapat ditemukan jenis bukti lain yang relevan, seperti metadata file, informasi login, jejak aktivitas aplikasi, dan file sementara yang ada pada perangkat korban atau tersangka. Bukti-bukti ini dapat memberikan perspektif yang lebih luas mengenai dinamika komunikasi antara pelaku dan korban, serta dapat membantu dalam rekonstruksi kronologi kejadian.

Hasil penelitian ini memiliki implikasi penting bagi praktisi dan penegak hukum. Metode *live forensics* dapat memperkuat validitas bukti digital di pengadilan karena data diperoleh tanpa merusak perangkat asli, sehingga integritasnya terjaga. Selain itu, penggunaan alat forensik seperti *FTK Imager* dan *WinHex* meningkatkan efisiensi proses investigasi dengan mempermudah pengumpulan bukti langsung dari perangkat desktop.

Oleh karena itu, peningkatan kapasitas teknologi dan keahlian di kalangan penegak hukum sangat diperlukan, termasuk pelatihan dalam penggunaan alat-alat *digital forensics* untuk mengikuti perkembangan teknologi aplikasi berbasis desktop. Penegakan hukum yang lebih efektif dapat dicapai dengan pemahaman yang mendalam tentang proses investigasi forensik dan teknik-teknik yang digunakan untuk validasi bukti.

Untuk penelitian lebih lanjut, ada beberapa saran yang dapat dikembangkan. Pertama, metode *live forensics* ini perlu diuji pada sistem operasi lain seperti *macOS* atau *Linux* untuk mengevaluasi efisiensinya pada platform yang berbeda. Kedua, teknik serupa dapat diterapkan pada aplikasi lain seperti *Telegram* atau *Signal*, serta pada jenis kasus *cybercrime* yang berbeda, misalnya pembobolan data atau perdagangan ilegal. Selain itu, kombinasi metode *live forensics* dengan teknik lain, seperti *analisis memori* atau *forensik disk*, dapat menghasilkan bukti digital yang lebih lengkap dan akurat.

DOI : https://doi.org/10.36341/rabit.v10i1.5514 *Corresponding Author* : Fahmi Fachri

Penelitian yang mengevaluasi bagaimana bukti digital diterima dalam sistem hukum di berbagai negara juga penting, terutama terkait perbedaan regulasi dan standar pengadilan. Dengan penelitian lebih lanjut, diharapkan teknik *live forensics* dapat menjadi metode yang lebih andal dalam mendukung pengungkapan berbagai kasus kejahatan digital.

DAFTAR PUSTAKA

[1] M. S. I. Lubis, "Teknologi Informasi Dan Komunikasi Dalam Perspektif Islam," *Jurnal Prosiding Ilmu Sosial Dan Ilmu Politik Ilmu Sosial Dan Ilmu Politik*, pp. 79–88, 2021.

[2] I. Istikomah and I. Khoiril Mala, "Dampak Internet terhadap Pola Interaksi Masyarakat di Desa Tawangharjo," *Bisnis dan Digital (JIMaKeBiDi)*, vol. 1, no. 2, 2024, [Online]. Available: http://www.ut.ac.id

[3] Muh David Balya Al, "Kemajuan Teknologi Dan Pola Hidup Manusia Dalam Perspektif Sosial Budaya," *TUTURAN: Jurnal Ilmu Komunikasi, Sosial dan Humaniora*, vol. 1, no. 3, pp. 26–53, 2023, doi: 10.47861/tuturan.v1i3.272.

[4] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 7, no. 1, pp. 43–48, 2022, doi: 10.30591/jpit.v7i1.3639.

[5] S. Marcellino, H. B. Seta, and I. W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute of Justice (NIJ)," *Informatik : Jurnal Ilmu Komputer*, vol. 19, no. 2, pp. 141–156, 2023, doi: 10.52958/iftk.v19i2.4676.

[6] S. J. Ashady, "Jurisdische : Jurnal Penelitian Hukum Cybercrime sebagai Kejahatan Dunia Maya dalam Perspektif Hukum dan Masyarakat Jurisdische : Jurnal Penelitian Hukum," vol. 1, pp. 34–46, 2024.

[7] M. Mulyadi, A. A. Nurdin, A. A. Anjani, and ..., "Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi," *Media Hukum ...*, vol. 2, no. 2, pp. 74–82, 2024, [Online]. Available: https://ojs.daarulhuda.or.id/index.php/MHI/article/view/296%0Ahttps://ojs.daarulhuda.or.id/index.php/MHI/article/download/296/327

[8] E. Jusriadi, E. Caronge, and Y. Nginang, "Penipuan Pinjaman Online kehidupan , termasuk dalam hal keuangan . Financial technology (fintech) satunya yaitu melalui peer to peer lending (P2P), Dewi (2018), hasil ini," vol. 8, no. 2, pp. 1–4, 2024.

[9] S. Pokhrel, "No TitleΕΛΕΝΗ," *Αγαη*, vol. 15, no. 1, pp. 37–48, 2024.

[10] A. Q. I. Hidayat, E. I. Alwi, and A. W. M. Gaffar, "Studi Forensik Digital: Analisis Bukti Video TikTok dengan Metode DFRWS," *Jurnal Minfo Polgan*, vol. 13, no. 1, pp. 1138–1146, 2024, doi: 10.33395/jmp.v13i1.13966.

[11] N. D. Putri, "Analisis Keamanan Menggunakan Metode Live Forensic pada Web Abstrak Pendahuluan tuntutan terhadap kehidupan menjadi serba mudah dan instan . Perkembangan teknologi hidup di masyarakat . Teknologi informasi memudahkan seluruh kegiatan masyarakat digital se," vol. 10, no. 1, pp. 51–66, 2024.

[12] J. Teknologi, W. Agustiono, D. W. 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," vol. 14, no. September, pp. 174–185, 2024, doi:

10.34010/jati.v14i2.

[13] A. S. Rido and F. Fachri, "Identifikasi Bukti Digital Whatsapp Pada Sistem Operasi Proprietary Menggunakan Live Forensics," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 2, pp. 1043–1051, 2024, doi: 10.29100/jipi.v9i2.5238.

[14] Mega Rosita, "Analisis Komparatif Performa FTK IMAGER dan AUTOPSY dalam Forensik Digital pada Flashdisk," *Info Kripto*, vol. 17, no. 3, 2023, doi: 10.56706/ik.v17i3.83.

[15] F. Dwi, "Analisis Aktivitas Cyber Bullying Pengguna Facebook Melalui Browser Chrome Dengan Pendekatan Live Forensics," *Jurnal TIMES*, vol. 12, no. 1, pp. 21–27, 2023, doi: 10.51351/jtm.12.1.2023687.

[16] M. A. Kustian, "Analisis Forensik Penggunaan Fungsi Hash Dalam Menentukan Keaslian Video, Metadata Image Dan Magic Number File," *Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi*, vol. 2, no. 2, pp. 10–16, 2023, doi: 10.20885/snati.v2i2.21.

[17] C. Putra, I. W., Suharso, A., Rozikin, "Akuisisi bukti digital dan deteksi keaslian citra pada whatsapp menggunakan metode NIST dan ELA," *Jurnal Sains Komputer & Informatika (J-SAKTI)*, vol. 5, no. 2, pp. 1–15, 2021.

[18] Kepala Kepolisian Negara Republik Indonesia, "Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 16 Tahun 2010 Tentang Tata Cara Pelayanan Informasi Publik di Lingkungan Kepolisian Negara Republik Indonesia," 2010.

[19] N. I. Pamungkas, I. R. I. Astutik, and M. A. Rosid, "Sistem Informasi Penjualan Tas Berbasis Web Pada Toko Tas Ud. a&N Collection Tanggulangin Dengan Metode Waterfall," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 8, no. 4, pp. 1467–1478, 2023, doi: 10.29100/jipi.v8i4.4039.

[20] W. Purnama and E. Supratman, "Sistem Informasi Pusat Layanan Psikologi Universitas Bina Darma Berbasis Web," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 8, no. 3, pp. 1074–1081, 2023, doi: 10.29100/jipi.v8i3.4041.

[21] D. E. Putri, "Perlindungan Hukum Terhadap Korban Tindak PidanaPenipuan Melalui Aplikasi Digital," 2024.