Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 6, No. 2, April 2023 (135-146) **DOI: 10.32493/jtsi.v6i2.31535**

Analisa Forensik Memori pada Aplikasi E-Commerce Berbasis Web Menggunakan Metode National Institute of Justice (NIJ)

Deanna Durbin Hutagalung[1], Cholis Hanifurohman[2], Debby Rahadian Baskhara[3]

Teknik Informatika, Universitas Pamulang, Jl. Raya Puspitek No. 46 Buaran, Serpong, Tangerang Selatan, Banten, Indonesia, 15417
e-mail: [1]deanna.upn91@gmail.com, [2]cholis.hanifurohman@gmail.com,
[3]debbyrahadianbaskhara@gmail.com

Submitted Date: April 03rd, 2023 Reviewed Date: April 20th, 2023
Revised Date: April 26th, 2023 Accepted Date: April 30th, 2023

Abstract

Security threats to e-commerce data continue to occur in line with the development and growth of e-commerce. This makes us realize how important data security is in the e-commerce business, therefore protective measures are needed to keep data safe. The purpose of this study is to perform a forensic analysis of browser data memory in Web-based E-Commerce applications to improve browser data security. The research methodology used is Forensic Analysis from the National Institute of Justice (NIJ) that consists of five stages, namely Identification, Collection, Examination, Analysis, and Reporting. The method used in conducting the analysis is to conduct a literature study and analysis of the results of memory forensics conducted on 5 (five) Web-based E-Commerce namely Tokopedia, Shopee, Lazada, Bukalapak and Orami. In this case Key Search is used to view Username, Password, Item Items and Nominal data. The results of the study stated that in the five E-Commerce items and nominal values were found, but passwords and usernames were not found, except for Lazada and Bukalapak found usernames.

Keywords : Forensic Analysis; E-Commerce; Data Security; Browser

Abstrak

Ancaman keamanan terhadap data *e-commerce* terus berlangsung sejalan dengan perkembangan dan pertumbuhan e-commerce. Hal ini menyadarkan kita betapa pentingnya keamanan data dalam bisnis e-commerce, oleh sebab itu dibutuhkan tindakan perlindungan agar data tetap aman. Tujuan penelitian ini adalah melakukan analisa forensik memori data browser pada aplikasi *E-Commerce* berbasis *Web* guna meningkatkan keamanan data browser. Metodologi penelitian yang digunakan adalah Analisa Forensik dari *National Institute of Justice (NIJ)* yang terdiri dari lima tahapan yaitu *Identification, Collection, Examination, Analysis, dan Reporting.* Metode yang digunakan dalam melakukan analisis adalah dengan melakukan studi literatur dan analisa terhadap hasil dari forensik memori yang dilakukan terhadap 5 (lima) *E-Commerce* berbasis *Web* yaitu Tokopedia, Shopee, Lazada, Bukalapak dan Orami. Dalam hal ini digunakan Key Search untuk melihat data-data Username, Password, Item Barang dan Nominal. Hasil penelitian menyatakan bahwa pada kelima *E-Commerce* tersebut ditemukan Item Barang dan Nominal, tetapi tidak ditemukan Password dan Username, kecuali pada Lazada dan Bukalapak ditemukan *Username*.

Kata Kunci: Analisa Forensik; E-Commmerce; Keamanan Data; Browser

1 Pendahuluan

Survey yang dilakukan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2022 menyatakan bahwa pengguna internet di Indonesia terus naik dari 175 juta menjadi 220 juta. Hal tersebut disebabkan kebutuhan komunikasi di masa Pandemi tahun 2020-2022. (Ginanjar et al., 2019) Aktifitas

belanja online semakin meningkat membuat e-commerce semakin popular dan menjadi pilihan belanja masyarakat.

Metode pembayaran yang dapat diakses secara cepat, aman, dan nyaman untuk berbelanja secara online, demikian juga dengan platform kredit digital yang semakin menjadi populer sebagai metode pembayaran di e-commerce. Hal tersebut didukung oleh tawaran pembayaran fleksibel secara berkala dibandingkan metode pembayaran lainnya sehingga mendorong tingkat kepercayaan konsumen pada industri e-commerce. Kementerian Koordinator (Kemenko) Bidang Perekonomian mencatat nilai transaksi e-commerce di Indonesia, baik domestik dan luar negeri, mencapai Rp 108,54 triliun sepanjang kuartal I-2022. Realisasi itu tumbuh 23% dibandingkan periode yang sama tahun lalu. (Uly, 2022)

Dalam layanan e-commerce berbasis web, pengguna melakukan transaksi keuangannya untuk melakukan jual beli secara online dengan cara membuka layanan e-commerce yang disediakan oleh masing-masing penyedia e-commerce berbasis web menggunakan browser. Sebelum melakukan transaksi keuangannya, pengguna diminta untuk melakukan otentikasi pengguna yang sudah diberikan oleh pihak penyedia. Setelah dilakukan otentikasi, pengguna dapat melakukan transaksi dengan menggunakan tambahan pengamanan seperti token. Semua data yang dimasukkan oleh penguna ke layanan e-commerce berbasis web secara otomatis juga akan tersimpan juga dalam memori volatil. Selama komputer tersebut belum dimatikan atau data yang ada di memori volatil belum tertimpa dengan data yang lainnya, maka data-data sensistif dari pengguna masih akan tersimpan dalam memori volatil. Seperti diketahui bahwa media penyimpanan komputer terdiri dari dua yaitu *volatile memory* dan *nonvolatile memory*. *Volatile memory* disebut juga sebagai memori sementara di mana ketika arus listrik terputus maka akan kehilangan memori atau data yang tersimpan, sedangkan *non-volatile memory* adalah memori yang tidak kehilangan data karena pemadaman listrik atau ketika daya terputus. Contoh volatile memori seperti RAM, DRAM, DDR, SDRAM, SRAM, dan nonvolatile memory seperti ROM, memori flash, hard disk drive, cakram optik, pita kertas dan banyak lagi.

Kemudahan yang diberikan oleh layanan e-commerce berbasis web tidak hanya berdampak posistif tetapi juga membawa dampak negatif, di antaranya adalah ancaman cyber crime. Tokopedia yang merupakan salah satu E-Commerce terkenal di Indonesia mengalami peretasan data pengguna. Jumlah total data pengguna yang dicuri mencapai 91 juta kemudian diperjualbelikan di *dark web*. Peretasan data tersebut menyadarkan kita betapa pentingnya keamanan dan perlindungan data dalam bisnis e-commerce. (Soedarso, 2020)

Untuk menangani kasus *cybercrime*, maka diperlukan alat bukti elektronik atau digital yang kuat sebagai bukti untuk melaporkan kepada pihak yang berwajib, dan dalam mendapatkan alat bukti elektronik tersebut diperlukan proses digital forensik. Cara kerja digital forensik adalah dengan cara mengembalikan, mengumpulkan, memeriksa dan menyimpan bukti informasi yang secara magnetis tersimpan pada komputer. Dalam melakukan analisa bukti digital yang baik diperlukan metode analisa forensik yang tepat, prosedur penanganan khusus dan mengkomparasi berbagai tool forensik sehingga diperoleh barang bukti berupa informasi yang valid (Fadillah et al., 2022).

Sudah banyak penelitian terkait analisis forensic. Beberapa penelitian terkait analisis forensic ditunjukkan pada Tabel 1.

Tabel 1. Literatur Riview

Nama Penulis	Judul Penelitian	Metode dan Tools	Hasil Penelitian
Muhammad Noor Fadillah, Rusydi Umar, Anton Yudhana, 2022	Analisis Forensik Aplikasi Dompet Digital Pada Smartphone Android Menggunakan	Metode: Digital Forensic Research Workshop (DFRWS). T*ools* forensik:	Dari perhitungan angka indeks data aktivitas simulasi, data berhasil ditemukan dengan *tools* forensik yaitu sebesar 100%

Nama Penulis	Judul Penelitian	Metode dan Tools	Hasil Penelitian
	Metode DFRWS	Belkasoft Evidence Center dan MOBILedit Forensic Express	
Rusydi Umar, Anton Yudhana, Muhammad Noor Fadillah, 2022	Perbandingan Tools Forensik Pada Aplikasi Dompet Digital	Metode: *Digital Forensic Research Workshop* (DFRWS) T*ools* forensik: Autopsy dan Belkasoft Evidence Center	Dari total 17 data aktivitas transaksi yang dilakukan, *tools* forensic Autopsy berhasil menemukan 8 aktivitas transaksi dan menemukan data sebesar 47,05%. Belkasoft Evidence Center mendapatkan 7 aktivitas transaksi sebesar 41,17%
Sang Putu Febri Wira Pratama**,** I Gusti Ngurah Anom Cahyadi Putra, Muhammad Akbar Hamid, Calvin Christian, I Ketut Kusuma Merdana, 2022	Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi Online	Metode: *National Institute of Justice (NIJ* *Tools Forensic: Mobiledit Forensic Express dan Systool SQLite Viewer*	Ditemukan percakapan terkait tindak prostitusi online pada tabel c*onversati on_entries* dalam *database* "1471436416148119552-61" yang akan dijadikan bukti adanya tindak Prostitusi Online
Nova Setiawan, Ahmad R Pratama, Erika Ramadhani, 2022	Metode *Live Forensics* untuk Investigasi Serangan *Formjacking* pada Website *E-Commerce*	Metode: *National Institute of Justice* (NIJ) dan metode investigasi Live Forensic. *Tools forensik:* Access Data FTK Imager 4.5.0	Formjacking dapat berjalan pada keempat browser yaitu Microsoft Edge, Opera, Mozila Firefox, Google Chrome dan dapat mengirimkan paket data berupa detail kartu kredit melalui perintah pada kode Javascript Hasil hash MD5 dan SHA1 didapat dari analisis data pada ram laptop menyakatan bahwa bukti digital asli dan valid
Aseh Ginanjar, Nur Widiyason, Rohmat Gunawan, 2018	Analisis Serangan *Web Phishing* pada Layanan *E-commerce* dengan Metode *Network Forensic Process*	Metode: *Network Forensic Process* *Tools Forensik:* Wireshark V.2.0.2 HashCalc V.2.0.2	terjadi pengiriman pesan melalui email dari freddynoer16@gmail.com kepada fanilla02@gmail.com pada tanggal 14 Oktober 2017. Isi pesan mengarahkan penerima email untuk mengakses web www.bukalapak.co.nf yang merupakan web palsu dari web *e-commerce* www.bukalapak.com. Ketika diakses pengguna akan diarahkan ke web *phishing* yang didaftarkan pada domain co.nf yang berlokasi di Bulgaria. Alamat host yang dibuat untuk phishing www.bukadiskusi.co.nf
Agil Nofiyan, Mushlihudin, 2020	Analisis Forensik pada *Web Phishing* Menggunakan Metode *National Institute Of Standards And Technology* (*NIST*)	Metode*:* *National Institute of Standards and Technology* (*NIST).* *Tools: Wireshark* dan *Hashcalc*	Diperoleh 7 paket data yang berhubungan dengan tindak kejahatan dilakukan *phiser*, *reporting* (pelaporan) melaporkan barang bukti berupa URL *phishing*, DNS yang digunakan pelaku, *IP address server*, *IP address destination*, identitas penyerang dan *email*, menghasilkan informasi tindak kejahatan dilakukan *phiser*

Penelitian yang berjudul Analisis Forensik Aplikasi Dompet Digital Pada *Smartphone* Android Menggunakan Metode *DFRWS* menyatakan bahwa dibalik kemudahan pada penggunaan aplikasi dompet digital, bisa saja terdapat pemanfaatan negatif yang berujung pada kasus *cybercrime*. Penelitian ini dilakukan dengan tujuan untuk memberikan gambaran proses forensik mencari informasi khususnya terkait transaksi yang dilakukan dengan menggunakan aplikasi dompet digital. Metode yang digunakan yaitu Digital Forensic Research Workshop (DFRWS) yang terdiri dari beberapa tahapan forensik meliputi *Identification, Preservation, Collection, Examination, Analysis* dan P*resentation.* Proses akusisi dan analisis menggunakan *tools* forensik Belkasoft Evidence Center dan MOBILedit Forensic Express. Informasi yang diperoleh berupa data pengguna dan aktivitas transaksi yang tersimpan pada perangkat *smartphone* dengan angka indeks sebesar 100% (Fadillah et al., 2022).

Berbeda dengan penelitian yang dilakukan oleh Rusydi Umar dengan judul Perbandingan Tool Forensik Pada Aplikasi Dompet Digital, di mana dilakukan perbandingan kemampuan *tools* forensik untuk menemukan bukti digital terkait dengan informasi dan aktivitas transaksi yang dilakukan pada empat aplikasi dompet digital. Dengan menggunakan metode *Digital Forensic Research Workshop* (DFRWS) dan *tools* forensik Autopsy dan Belkasoft Evidence Center, berhasil menemukan bukti digital dengan total 17 data aktivitas transaksi yang dilakukan. T*ools* forensic Autopsy berhasil menemukan 8 aktivitas transaksi dengan presentase kemampuan *tools* forensic sebesar 47,05%, sedangkan pada tool forensic Belkasoft Evidence Center mendapatkan 7 aktivitas transaksi sebesar 41,17%. (Umar et al., 2022)

Penelitian dengan judul Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi Online, di mana media sosial Twitter digunakan orang menjadi sarana menyebarkan konten pornografi dan prostitusi online. Oleh sebab itu perlu dilakukan tindakan forensik digital untuk mengatasi kejahatan tersebut. Dengan menggunakan metode *National Institute of Justice* (NIJ) dan tools *Mobiledit Forensic Express* dan *Systools SQLite Viewer*. Hasil penelitian ini yaitu penyidik menemukan percakapan terkait tindak prostitusi online pada table *conversation_entries* dalam d*atabase* "1471436416148119552-61" (Putu et al., 2022). Penelitian ini tidak mencantumkan berapa besar indeks hasil kinerja penggunaan *tools forensic* yang digunakan pada aplikasi media sosial Twitter.

Berbeda dengan penelitian yang dilakukan oleh Ikhwan Anshori yang berjudul Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ, di mana kinerja tool forensic sangat jelas diuraikan. Penelitian ini menggunakan 3 Tools Forensic yaitu MOBILedit Forensic Express, Magnet AXIOM dan Oxygen Forensic Suite 2014. Hasil kinerja *MOBILedit Forensic Express* mendapatkan bukti digital dengan persentase berupa 100% akun, 55% dalam mendapatkan chat dan 86% gambar. *Magnet AXIOM* mendapatkan bukti digital dengan persentase berupa 100% akun, 55 chat dan 86% gambar. *Oxygen Forensic Suite 2014* mendapatkan bukti digital dengan presentase breupa 100% akun, 5% chat dan 86% gambar. Dari hasil analisis digital pada Facebook Messenger dengan penggunaan 3 tools digital tersebut diperoleh kesimpulan bahwa *MOBILedit Forensic Express* dan *Magnet* AXIOM memiliki kinerja yang baik sedangkan Oxygen Forensic Suite 2014 kurang baik (Anshori et al., 2020).

Salah satu ancaman keamanan transaksi pengguna platform e-commerce adalah pencurian data digital seperti kartu kredit yang dilakukan dengan bantuan kode jahat dengan menduplikasi dan mengirimkan data pembayaran ke server milik pelaku yang dikenal dengan serangan formjaking (Setiawan et al., 2022). Penelitian dengan judul Metode *Live Forensics* untuk Investigasi Serangan *Formjacking* pada Website *E-Commerce* menyatakan bahwa *Live forensics* pada RAM di komputer milik korban dapat digunakan sebagai salah satu teknik investigasi atas serangan *formjacking*. Dengan menggunakan perangkat forensik AccessData FTK Imager 4.5.0. dan mengacu pada metode forensik *National Institute of Justice* (NIJ), pengujian dilakukan pada empat *browser* berbeda yaitu Opera Mini,

Google Chrome, Microsoft Edge, dan Mozilla Firefox di perangkat komputer dengan sistem operasi Windows 10. Penelitian ini mengungkapkan bahwa keempat browser mencatat artefak digital berupa kiriman paket data kartu kredit ke server pelaku berupa Nama, Nomor dan CVV pemilik kartu kredit. (Setiawan et al., 2022)

Paket data kartu kredit tersebut hanya memiliki 3 paket data sementara dalam penelitian yang berjudul Implementasi Teknik Forensik Dalam Cybercrime (Carding) menyatakan bahwa dalam pengungkapan pencarian barang bukti Carding, penyidik harus memahami konsep bukti, sistem operasi yang akan dicek, konsep jaringan dan serangan serta barang bukti Carding berupa phising email, invoice transaksi kartu kredit, percakapan IRC, log history, bookmark, aplikasi terkait dan sebagainya (Sallu & Fathoni, 2023).

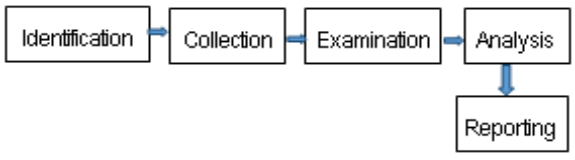
Penelitian dengan judul Analisis Serangan *Web Phishing* pada Layanan *E-commerce* dengan Metode *Network Forensic Process*, bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengamatan untuk menemukan identitas penyerang dan merekonstruksi tindakan serangan melalui analisis bukti penyusupan. Hasil investigasi diketahui telah terjadi pengiriman pesan melalui email dari freddynoer16@gmail.com kepada fanilla02@gmail.com pada tanggal 14 Oktober 2017. Isi pesan mengarahkan penerima email untuk mengakses web www.bukalapak.co.nf yang merupakan web palsu dari web *e-commerce* www.bukalapak.com. Saat pengguna mengakses web tersebut maka akan diarahkan ke web *phishing* yang didaftarkan pada domain co.nf berlokasi di Bulgaria dan alamat host yang digunakan adalah www.bukadiskusi.co.nf. Oleh sebab itu penelitian selanjutnya ketika ditemukan *fake domain* perlu dilakukan penelusuran lebih detail terhadap identitas personal yang terlibat dalam aktifitas *phishing* (Aseh Ginanjar, 2018).

Terkait penemuan fake domain maka penelitian yang dilakukan oleh Agil Nofiyan dan Mushlihudin (Mushlihudin & Nofiyan, 2021) dengan judul Analisis Forensik pada *Web Phishing* Menggunakan Metode *National Institute Of Standards And Technology* (*NIST*) menyatakan bahwa *Protocols* HTTPS pada website mempunyai keamanan yang tinggi dan hal ini yang dimanfaatkan phiser dengan cara mengenkripsi data menggunakan *algortihma*, di mana *phiser* memanfaatkan keamanan HTTPS untuk membuat web *phishing* dan juga meyakinkan korban bahwa web tersebut aman digunakan. Menggunakan *Tools Wireshark* untuk mencari barang bukti dan *tools Hashcalc* untuk mengakuisisi barang bukti yang didapatkan, maka penelitian ini bertujuan menganalisis serangan web phising oleh phiser menggunakan fitur fake login. Penelitian ini menghasilkan tujuh paket data yang berhubungan dengan tindak kejahatan berupa barang bukti URL *phishing*, DNS yang digunakan oleh pelaku, *IP address server*, *IP address destination*, identitas penyerang dan *email* yang menghasilkan informasi. Saat proses investigasi ditemukan celah untuk mendekripsi *protocols* HTTPS yang digunakan web *phishing* (Mushlihudin & Nofiyan, 2021).

Karena analisis forensik digital pada Web E-Commerce masih dilakukan satu per satu seperti Bukalapak, Tokopedia dan yang lainnya maka penelitian ini hadir untuk melakukan analisa forensik memori data browser pada 5 aplikasi E-Commerce sehingga dapat meningkatkan keamanan data pengguna.

2 Metodologi Penelitian

Pada penelitian ini mengadaptasi dan mengimplementasikan metode analisa forensic dar National Institute of Justice (NIJ). Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga diketahui alur dan langkah-langkah penelitian secara sistematis untuk dijadikan pedoman dalam menyelesaikan permasalahan. Tahapan penelitian ini digambarkan sebagai berikut



Gambar 1. Metode National Institute of Justice (NIJ)

Tahapan metode dari National Institute of Justice (NIJ) ini terbagi menjadi lima

tahapan yakni identification, collection, examination, analysis, dan reporting.

Tahap identification atau tahap identifikasi merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Tahap ini terdapat proses identifikasi, pelabelan, perekaman untuk menjaga keutuhan barang bukti.

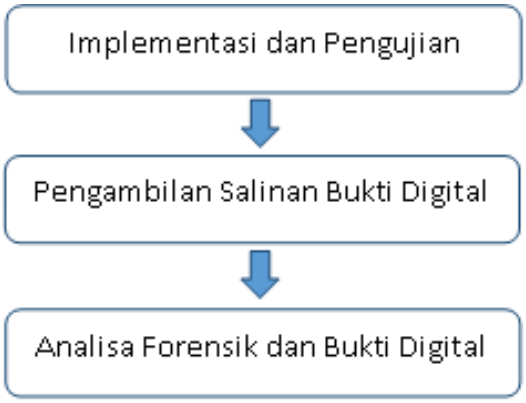
Tahap collection atau tahap pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan.

Tahap examination atau tahap pemeriksaan merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis maupun manual, serta memastikan bahwa data yang didapat berupa file tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada file digital perlu dilakukan identifikasi dan validasi file dengan teknik hashing.

Tahap analysis atau tahap meneliti ini dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan.

Tahap reporting atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tool, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, tool, atau aspek pendukung lainnya pada proses tindakan digital forensik.

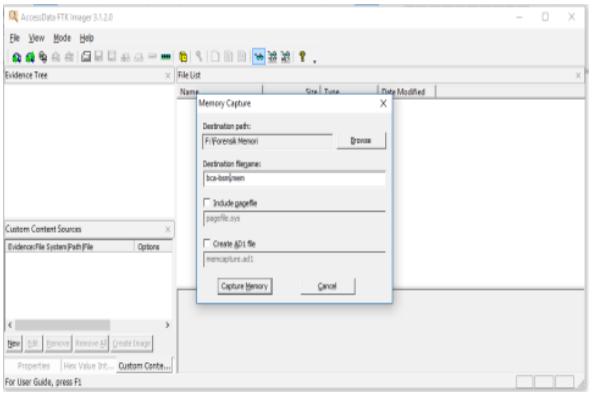
Untuk mendapatkan bukti digital tidak diperoleh dalam lingkungan yang sebenarnya atau barang bukti tidak didapatkan dari hasil tindak kejahatan komputer yang sebenarnya, melainkan bukti dari hasil skenario. Oleh sebab itu langkah yang dilakukan adalah Implementasi dan Pengujian, Pengambilan Salinan Bukti Digital dan Analisa Forensik Bukti Digital seperti gambar di bawah ini:



Gambar 2. Langkah Penelitian

Implementasi dan pengujian dilakukan dengan desain skenario, dengan tujuan untuk mendapatkan bukti digital seperti pada kasus kejahatan komputer yang sebenarnya pada saat pengguna melakukan aktivitas belanja online menggunakan e-commerce berbasis web. Metode yang digunakan dalam melakukan analis adalah dengan melakukan studi literatur dan analisa terhadap hasil dari forensik memori.

Setelah melakukan dump memori menggunakan DumpIt, software yang kedua yang dapat digunakan untuk melakukan akuisisi memori adalah FTK Imager dari Acces Data.



Gambar 3. FTK Imager

Dengan melakukan klik pada pilihan capture memory maka akan diminta untuk menentukan di mana hasil file akuisisi akan

disimpan. Berbeda dengan DumpIt, file akusisi yang dihasilkan oleh FTK Imager mempunyai ekstensi *.mem. Setelah melakukan akuisisi memori secara langsung, langkah selanjutnya adalah analisa file hasil akuisis memori tersebut. Dengan menganalisis memori kita bisa mendapatkan proses yang berjalan, daftar library dan lain-lain yang berjalan pada satu waktu, port terbuka, koneksi jaringan. Informasi ini biasanya menjadi fokus dari petugas inverstigasi forensik.

WinHex dan HxD dapat digunakan sebagai software untuk menganalisis hasil akuisisi memori. WinHex dan HxD adalah editor heksadesimal mampu melihat konten memori volatil. Pengujian akan dilakukan pada layanan internet banking yang dijalankan menggunakan browser Google Chrome. Hasil setiap fungsi implementasi diuji secara manual menggunakan editor heksadesimal tersebut.

"Keyword search", yang juga dikenal sebagai "string search" telah banyak digunakan oleh penyelidik forensik untuk mengidentifikasi bukti berdasarkan kata kunci yang diketahui. Metode ini yang digunakan penulis untuk melakukan analisa dengan cara data-data yang dimasukkan ke dalam layanan internet banking untuk keperluan transaksi transfer akan dicari ke dalam memori yang telah diakuisisi. Jika string yang dicari ditemukan akan dicatat pola penulisannya. Pola yang dicari adalah pola string sebelum atau sesudah data-data sensitif nasabah yang tersimpan di dalam memori.

Berikut adalah kebutuhan yang diperlukan untuk melakukan Analisa Forensik Memori Pada Aplikasi E-Commerce Berbasis Web.

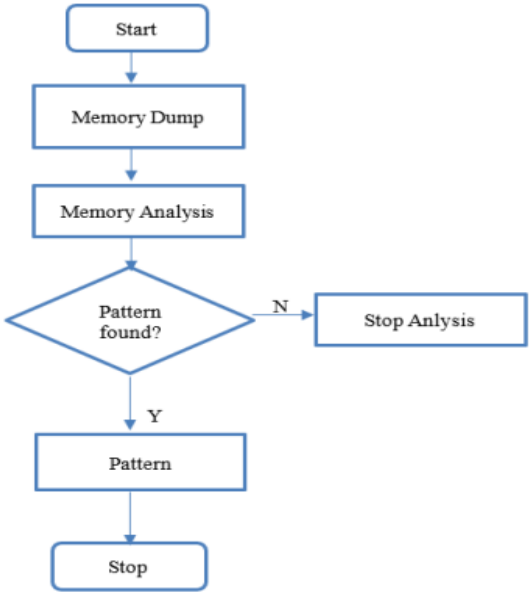
Kebutuhan software yang diperlukan yaitu :
1. Sistem Operasi : Windows 10 Pro 32 Bit
2. Browser : Google Chrome versi 55.0.2.8883.87
3. Sofware Akuisisi memori : DumpIt v1.3.2.20110401 dan FTK Imager 3.2.0
4. HxD Hex Editor 1.7.7. 0

Untuk kebutuhan hardware yaitu:
1. Komputer
2. Smartphone

Penelitian ini memanfaatkan aplikasi instan messenger telegram yang menyediakan API untuk membuat Bot di dalamnya secara bebas. Oleh karena itu dilakukan perancangan aplikasi Sinami Bot Unpam.

Gambar 4. Grup Pengelola Sinami Bot Unpam

Implementasi dan pengujian dilakukan skenario dengan tujuan untuk mendapatkan bukti digital seperti kasus kejahatan digital pada proses transaksi di e-commerce yang sebenarnya seperti pada flowchart berikut :



Gambar 5. Flowchart Analisa Forensik Memori

Pengambilan salinan bukti digital berupa data-data yang tersimpan dalam memori dari hasil transaksi online menggunakan e-commerce berbasis web menggunakan aplikasi untuk melakukan akuisisi memori.

Setelah dilakukan pengambilan salinan bukti digital berupa file.raw, selanjutnya dilakukan analisa menggunakan metode *key search* untuk menemukan pola-pola penyimpanan *credential* dari *e-commerce* yang digunakan untuk transaksi pembelian barang secara online.

3 Hasil dan Pembahasan

Penelitian yang dilakukan dengan sebuah simulasi transaksi pembelian online pada aplikasi e-commerce berbasis web. Pada simulasi ini peneliti akan melakukan proses akuisisi memori (RAM) menggunakan aplikasi DumpIt. File akuisisi dalam format *.raw selanjutnya diproses.

3.1 Tahap Identification

Tahap Identification dilakukan untuk mempersiapkan barang bukti digital mendukung proses identifikasi dalam sebuah kasus kejahatan digital. Berikut identifikasi alat yang digunakan.

Tabel 2. Hasil Identifikasi Alat

No.	Alat dan Bahan	Keterangan
1	Laptop	Hp Spectre
2	Chrome	Browser untuk membuka aplikasi e-commerce
3	DumpIt	Aplikasi untuk melakukan akuisisi memori di windows
4	HxD	Hexa editor untuk membuka file.raw hasil akuisisi memori

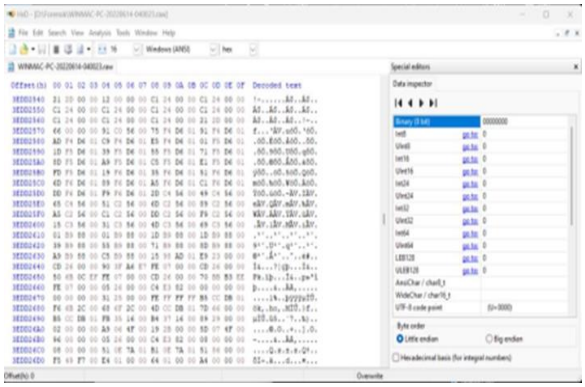
3.2 Tahap Collection

Tahap Collection dilakukan pengumpulan barang bukti digital yang berupa data-data/file-file pada sebuah objek yang diindikasi sebagai source yang valid untuk sebuah kasus kejahatan digital. Barang bukti berupa hasil akusisisi memori pada laptop yang digunakan untuk melakukan transaksi menggunakan aplikasi e-commerce dalam bentuk file.raw.

3.3 Tahap Examination

Tahap Examination atau tahap pemeriksaan pada barang bukti digital dilakukan secara manual ataupun otomatis yang didapatkan dari tahapan sebelumnya yaitu collection. Barang bukti yang dimaksud berupa file-file yang didapatkan dari objek pada sebuah kasus kejahatan digital. Proses akuisisi data pada data browser yang tersimpan di memori menggunakan aplikasi DumpIt.

Proses akuisisi merupakan merupakan tahapan pertama yang dilakukan sebelum melakukan tahapan analisis. Pada tahapan akuisisi data pada file-file yang akan menjadi barang bukti digital. Hasil dari tahap eksaminasi data yang telah didapatkan dari proses akuisisi yakni nama file.raw seperti pada gambar berikut:



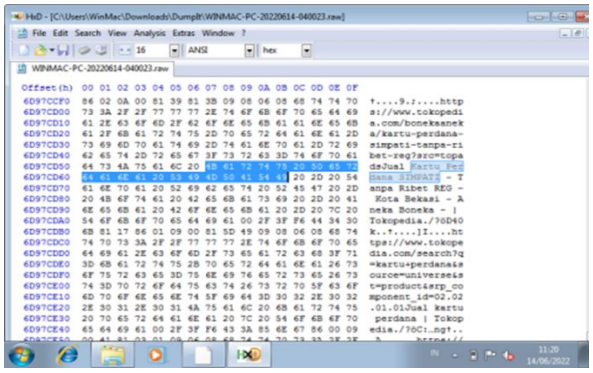
Gambar 6. Hasil file .raw dibuka dengan HxD

3.4 Tahap Analysis

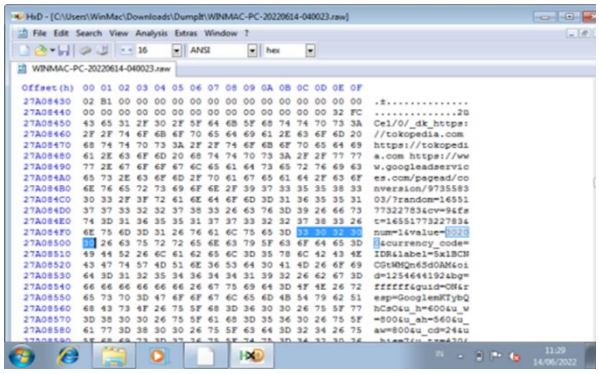
Tahap Analysis dilakukan pada hasil temuan barang bukti digital pada tahapan examination, selanjutnya data dianalisis menggunakan metode yang sah secara teknis dan hukum sebagai pembuktian data tersebut sehingga hasil analisis digital evidence dapat dibuktikan dan dipertanggungjawabkan secara ilmiah dan hukum. Analisis dilakukan menggunakan metode *Keyword search* di mana jika string yang dicari ditemukan akan dicatat pola penulisannya. Pola yang dicari adalah pola *string* sebelum atau sesudah data-data sensitif customer yang tersimpan di dalam memori.

3.4.1 Tokopedia

Hasil analisis forensik terhadap data browser yang diperoleh dari E-commerce Tokopedia yang beralamat di https://tokopedia.com ditemukan nama item barang, harga atau nilai transaksi dari sebuah transaksi pembelian online. Namun data akun dan password pengguna tidak ditemukan.



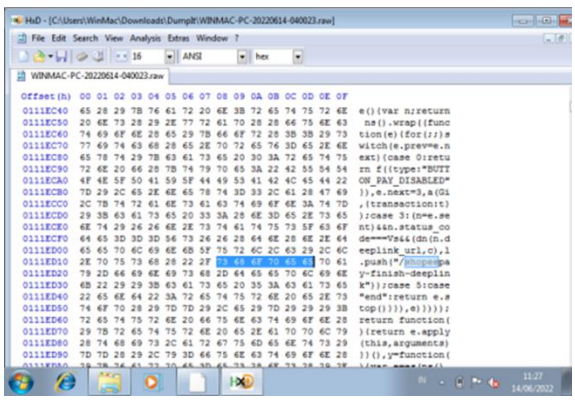
Gambar 7. Item Barang yang dibeli di Tokopedia



Gambar 8. Nilai Transaksi di Tokopedia

3.4.2 Shopee

Hasil analisis forensik terhadap data browser yang diperoleh dari E-commerce Shopee yang beralamat di https://shopee.co.id didapatkan hasil bahwa ditemukan nama item barang, harga atau nilai transaksi dari sebuah transaksi pembelian online. Namun data akun dan password pengguna tidak ditemukan.

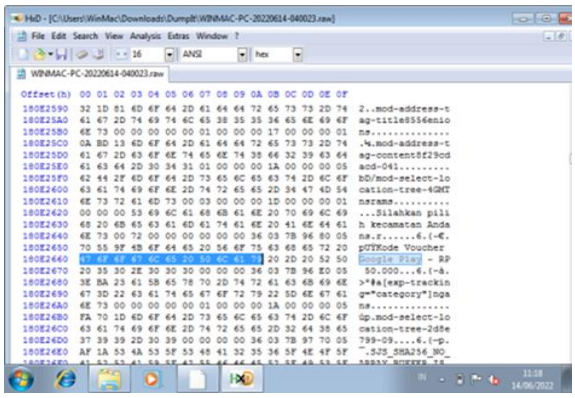


Gambar 9. Nilai Transaksi di Shopee

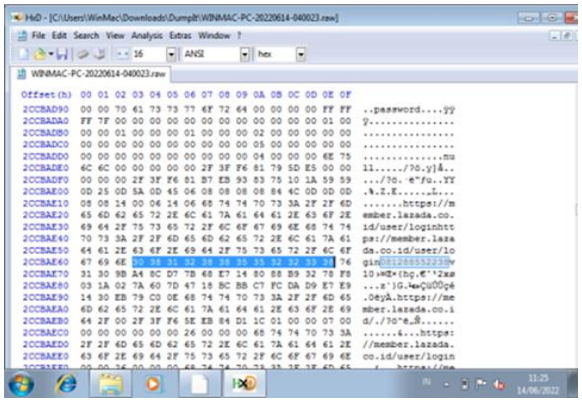
3.4.3 Lazada

Hasil analisis forensik terhadap data browser yang diperoleh dari e-commerce yang beralamat di https://lazada.co.id didapatkan hasil bahwa ditemukan nama item barang, harga atau nilai transaksi dari sebuah transaksi pembelian online. Data akun berupa nomor handphone ditemukan, namun data password pengguna tidak ditemukan.

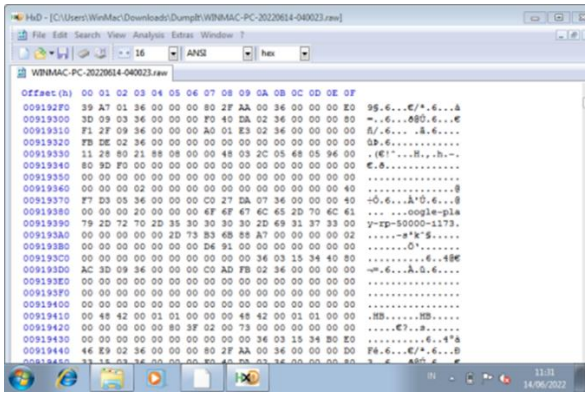
Berikut ini adalah gmabar item barnag yang dibeli di e-commerce Lazada.



Gambar 10. Item Barang yang dibeli di Lazada



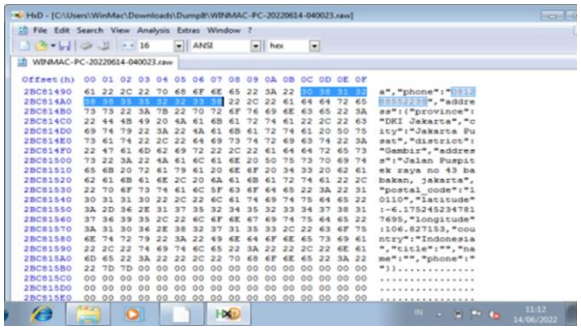
Gambar 11. User Login Lazada



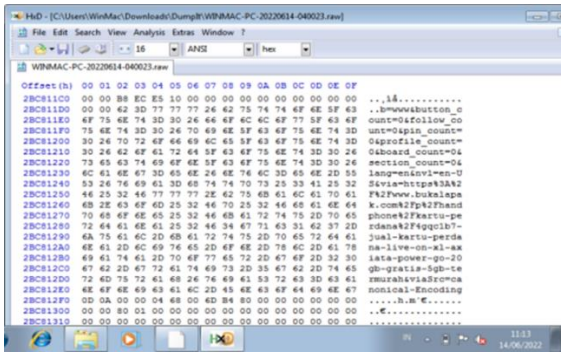
Gambar 12. Nilai Transaksi di Lazada

3.4.4 Bukalapak

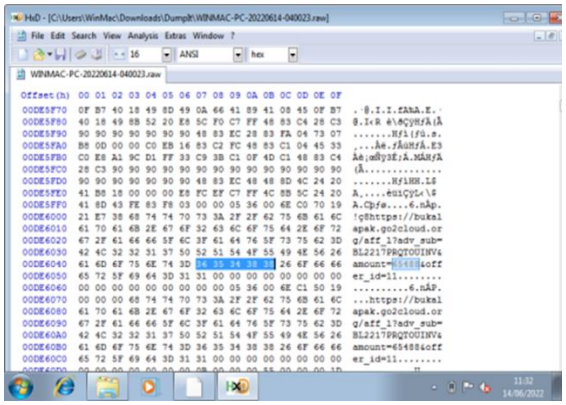
Hasil analisis forensik terhadap data browser yang diperoleh dari E-commerce Bukalapak yang beralamat di https://bukalapak.com didapatkan hasil bahwa ditemukan nama item barang, harga atau nilai transaksi dari sebuah transaksi pembelian online serta nomor handphone pengguna. Namun data akun dan password pengguna tidak ditemukan.



Gambar 13. Nomor HP Penggguna Bukalapak



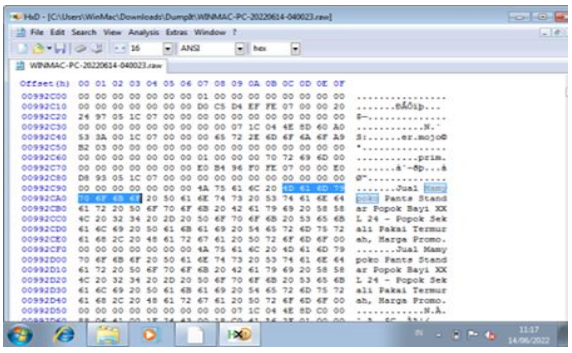
Gambar 14.Item Barang yang dibeli di Bukapalak



Gambar 15. Nilai Transaksi di Bukapalak

3.4.5 Orami

Hasil analisis forensik terhadap data browser yang diperoleh dari E-commerce Orami yang beralamat di https://orami.co.id didapatkan hasil bahwa ditemukan nama item barang, harga atau nilai transaksi dari sebuah transaksi pembelian online. Namun data akun dan password pengguna tidak ditemukan.



Gambar 16. Item Barang yang dibeli di Orami

3.5 Tahap Reporting

Tahap Reporting dilakukan setelah tahapan pemeriksaan dan analisis mencapai akhir. Setelah hasil analisis diperoleh maka dilakukan pelaporan dengan ilustrasi terhadap proses yang dilakukan mengenai tools yang digunakan, metode/framework, tindakan pendukung yang diambil, perbaikan kebijakan, serta tools ataupun komponen pendukung lainnya pada proses tindakan digital forensik.

Hasil eksaminasi pada 5 e-commerce berbasis web dengan metode *Key Search* ditemukan data-data sebagai berikut:

Tabel 3. Hasil Keyword "Search"

No	E-Commerce	User	Pass word	Item	No minal
1	Tokopedia	X	X	√	√
2	Shopee	X	X	√	√
3	Lazada	√	X	√	√
4	Bukalapak	√	X	√	√
5	Orami	X	X	√	√

Keterangan : √ = Ditemukan, X = Tidak Ditemukan

4 Kesimpulan

Menggunakan metode National Institute of Justice (NIJ) dengan tools forensik DumpIt v1.3.2.20110401 dan FTK Imager 3.2.0 dengan HxD Hex Editor 1.7.7. 0, forensik digital terhadap lima E-Commerce diperoleh hasil pada E-Commerce Tokopedia, Shopee, Lazada, Bukalapak dan Orami ditemukan Item Barang dan Nominal, tetapi tidak ditemukan Password. Sedangkan Username hanya ditemukan pada Lazada dan Bukalapak.

Dengan metode "*keyword search*" atau yang dikenal "string search" data yang dihasilkan browser untuk membuka layanan e-commerce ditemukan pola penyimpanan data-data sensitif pengguna ketika melakukan transaksi transfer menggunakan layanan e-commerce. Pola tersebut dapat digunakan oleh petugas digital forensik dalam melakukan investigasi kasus kejahatan yang menggunakan layanan e-commerce.

5 Saran

Dari hasil pembahasan, penulis memberikan saran untuk penelitian selanjutnya sebagai berikut:

1. Perlu dilakukan pengujian untuk seluruh layanan e-commerce berbasis web di Indonesia sehingga mendapatkan data dari seluruh layanan e-commerce berbasis web.
2. Perlu dilakukan penelitian lebih lanjut terkait aspek keamanan dari layanan e-commerce berbasis web baik untuk pengguna layanan maupun penyedia layanan.
3. Lakukan pengujian berkala pada sistem operasi lain dan platform aplikasi mobile.

Daftar Pustaka

Anshori, I., Setya Putri, K. E., & Ghoni, U. (2020). Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ. *IT Journal Research and Development*, *5*(2), 118–134. https://doi.org/10.25299/itjrd.2021.vol5(2).4664

Aseh Ginanjar. (2018). Analisis Serangan Web Phishing pada Layanan E-commerce dengan Metode Network Forensic Process. *JUTEI*, *2*, 147–157.

Fadillah, M. N., Umar, R., Yudhana, A., Studi, P., Informatika, M., Dahlan, U. A., Studi, P., Elektro, T., Dahlan, U. A., & Soepomo, J. P. (2022). *Analisis Forensik Aplikasi Dompet Digital Pada Smartphone Android Menggunakan Metode Dfrws*. *09*(02), 265–278.

Ginanjar, A., Widiyasono, N., & Gunawan, R. (2019). Web Phising Attack Analysis on E-Commerce Service Using Network Forensic Process Method. *Jurnal Terapan Teknologi Informasi*, *2*(2), 147–157. https://doi.org/10.21460/jutei.2018.22.111

Mushlihudin, M., & Nofiyan, A. (2021). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology. *Cybernetics*, *4*(02), 11–23. https://doi.org/10.29406/cbn.v4i02.2287

Putu, S., Wira, F., Ngurah, I. G., Cahyadi, A., & Akbar, M. (2022). *Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi Online*. *10*(3), 271–278.

Sallu, S., & Fathoni, A. (2023). *Implementasi Teknik Forensik dalam Cybercrime (Carding)*. *7*, 1–16.

Setiawan, N., Pratama, A. R., & Ramadhani, E. (2022). *Jurnal Sistem dan Teknologi Informasi Metode Live Forensics untuk Investigasi Serangan Formjacking pada Website E-Commerce*. *7*(1), 1–9.

Soedarso. (2020). *Perlindungan Keamanan E-Commerce*. Nasional.Sindonews.Com.

Uly, Y. A. (2022). *Nilai Transaksi E-Commerce Indonesia Capai Rp 108,54 Triliun di Kuartal I-2022 Halaman all - Kompas.com*. Kom[as.Com. https://money.kompas.com/read/2022/08/03/211200826/nilai-transaksi-e-commerce-indonesia-capai-rp-108-54-triliun-di-kuartal-i-2022?page=all

Umar, R., Yudhana, A., & Fadillah, M. N. (2022). Perbandingan Tools Forensik Pada Aplikasi Dompet Digital. *JIKO (Jurnal Informatika Dan Komputer)*, *6*(2), 242. https://doi.org/10.26798/jiko.v6i2.621