JUSTINDO
Jurnal Sistem dan Teknologi Informasi
http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO
E-ISSN: 25541-5735, P-ISSN: 2502-5724
Volume 7, No. 1, Februari 2022

Metode *Live Forensics* untuk Investigasi Serangan *Formjacking* pada Website *E-Commerce*

Nova Setiawan[1], Ahmad R Pratama[2], Erika Ramadhani[3]

Universitas Islam Indonesia
Email: [1] nova.setiawan@students.uii.ac.id, [2] ahmad.rafie@uii.ac.id, [3] erika@uii.ac.id

(Naskah masuk: 18 Juni 2021, diterima untuk diterbitkan: 31 Januari 2022, Terbit: 28 Februari 2022)

ABSTRAK

Pertumbuhan usaha *online* yang tinggi dan bergesernya sikap konsumen yang menginginkan transaksi serba cepat, fleksibel dan ekonomis menyebabkan pertumbuhan *e-commerce* yang kian meningkat. Hal ini mengindikasikan semakin ketatnya persaingan pada penjualan berbasis *e-commerce* dalam merebut pasar offline atau konfensional. Pertumbuhan *e-commerce* diikuti pula dengan munculnya ancaman keamanan bagi pengguna saat melakukan transaksi pembelian pada platform website *e-commerce*. Salah satunya adalah ancaman pencurian data digital berupa detail kartu kredit pengguna *e-commerce* yang dapat dilakukan dengan bantuan kode jahat yang mampu menduplikasi dan mengirimkan data pembayaran ke server yang dimiliki pelaku, atau biasa dikenal dengan serangan *formjacking*. Dengan mengacu pada metode forensik *National Institute of Justice* (NIJ) yang meliputi *identification*, *collection*, *examination*, *analysis*, serta *reporting*, penelitian ini bertujuan untuk menunjukkan bagaimana metode *live forensics* pada RAM di komputer milik korban dapat digunakan sebagai salah satu teknik investigasi atas serangan *formjacking*. Pengujian dilakukan sesuai skenario pada empat *browser* berbeda yaitu Opera Mini, Google Chrome, Microsoft Edge, dan Mozilla Firefox di perangkat komputer dengan sistem operasi Windows 10. Jejak digital yang ditinggalkan dianalisis dengan bantuan perangkat forensik AccessData FTK Imager 4.5.0. Hasil dari penelitian ini dapat dijadikan rujukan bagi penegak hukum untuk mengungkapkan kejahatan digital berupa *formjacking* pada website *e-commerce*.

Kata kunci: Formjacking, Live Forensics, Digital Forensic*, e-commerce*

ABSTRACT

The rapid expansion of online businesses, as well as changing consumer attitudes toward quick, flexible, and cost-effective transactions, have resulted in the rapid expansion of e-commerce. This reflects the increasingly fierce competition in e-commerce-based sales to capture the offline or traditional market. E-commerce growth is accompanied by the emergence of security threats for users when making purchases on e-commerce website platforms. One of them is the threat of digital data theft in the form of e-commerce users' credit card details, which can be accomplished with the help of malicious code capable of duplicating and sending payment data to a server owned by the perpetrator, also known as a formjacking attack. This study aims to demonstrate how the live forensics method on RAM on the victim's computer can be used as one of the investigative techniques for formjacking attacks by referring to the National Institute of Justice (NIJ) forensic methods, which include identification, collection, examination, analysis, and reporting. The experiments were carried out on four different browsers, namely Opera Mini, Google Chrome, Microsoft Edge, and Mozilla Firefox, on a computer device running Windows 10. The acquired digital traces were examined further using the

AccessData FTK Imager 4.5.0 forensic tool. The findings of this study can be used as a reference by law enforcement when investigating cyber crimes such as formjacking on e-commerce websites.

***Keywords**: Formjacking, Live Forensics, Digital Forensics, e-commerce*

1. PENDAHULUAN

Kemunculan beberapa platform belanja online saat ini sangat membantu perkembangan dan perubahan di bidang perdagangan. Dimana biasanya dilakukan dengan cara konvensional menjadi transaksi online melalui website. Dalam hal ini yang dikembangkan adalah proses jual beli melalui situs *e-commerce*. E-commerce atau electronic commerce adalah transaksi elektronik yang melibatkan pembelian dan pertukaran informasi produk melalui internet (Tian dan Stewart, 2006)

Indonesia termasuk dalam dengan pertumbuhan *e-commerce* tercepat. Indonesia berada di atas negara lain dalam hal pertumbuhan hampir 78% di 2018, mengikuti angka ini dengan pengguna internet Indonesia, mesin pertumbuhan *e-commerce* lebih dari 100 juta orang Indonesia, rata-rata transaksi sekitar Rp.3,19 juta rupiah untuk masing-masing orang. Widowati (2019). Selain kemudahan yang dihasilkan terdapat hal yang mungkin tidak terfikirkan pada proses transaksi online pada website *e-commerce* yaitu ancaman serangan yang dilakukan orang yang tidak bertanggung jawab untuk dapat mencuri data akun pembayaran misalnya data kartu kredit (Kurniawan, 2014). Ditambah lagi, kesadaran keamanan di Indonesia masih belum merata dan cukup mengkhawatirkan di beberapa kalangan termasuk pelaku *e-commerce* (Alif dan Pratama, 2021; Rahmadi dan Pratama, 2020; Ramadhani dan Pratama, 2020).

Berdasarkan laporan tahunan tentang acaman dari perusahaan keamanan siber yaitu Symantec, yang bertajuk *Internet Security Threat Report* dikenal dengan istilah (ISTR). Mengungkapkan bahwa pada di tahun 2019 terdapat banyak serangan dari pegiat siber yang begitu agresif sehingga merusak, dan menjadi kian bahaya. Para penjahat di dunia maya menggandakan metode-metode alternatif, seperti *Formjacking*. Serangan ini memakai kode JavaScript berbahaya yang difungsikan untuk mencuri data dari kartu kredit seperti nomor, nama dan CVV yang diinput pada formulir pembayaran dalam laman form *check-out* pada situs *e-commerce*.

Nomor kartu kredit, nama, dan data CVV sangat penting dalam akun belanja online yang digunakan sebagai metode pembayaran. Karena data tersebut termasuk data volatil atau data sementara yang terekam dalam random access memory pada komputer yang menyala. Jika komputer dimatikan, maka data vilatil tersebut akan hilang (Bintang dkk, 2018). Menyadari pentingnya penindakan terhadap tindak pidana pencurian data pada website *e-commerce*, maka perlu dilakukan pembinaan pada tahapan penyidikan pada teknologi website *e-commerce* untuk memberikan bukti-bukti ilmiah. Penyelidikan forensik yang dilakukan oleh penyidik sesuai dengan prosedur forensik digital untuk menemukan barang bukti digital. Investigasi forensik memiliki metode yang digunakan untuk menemukan bukti, yaitu pengumpulan bukti di tempat secara *live forensics*. Metode *live forensic* untuk mengumpulan bukti digital dilakukan sesaat diketahui adanya tindak kejahatan terjadi, utamanya dengan menggunakan web browser untuk mencari jejak digital yang ditinggalkan untuk mengungkap suatu tindak kejahatan (Faiz

dkk, 2017; Rochmadi, 2019; Sidiq dan Faiz, 2019).

Berbagai penelitian terdahulu telah menunjukkan bagaimana bukti digital dapat ditemukan pada web browser dengan teknik *live forensic,* di mana kata kunci yang dicari dapat ditemukan dengan akusisisi RAM di komputer milik pengguna (Rochmadi, 2019; Sidiq dan Faiz, 2019; Umar dkk, 2018). Investigasi *live forensics* dapat dilakukan dengan bantuan *forensic tools* AccessData FTK Imager. FTK Imager sendiri adalah software forensik digital yang menggunakan teknologi *real-time* atau statis atau bahkan keduanya selama investigasi (Riskiyadi,2020).

Penelitian ini disusun dengan memperhatikan penelitian sebelumnya (Faiz dkk, 2017; Rochmadi, 2019; Sidiq dan Faiz, 2019; Umar dkk, 2018). Fokus dari penelitian ini yaitu pada tindak kejahatan siber berupa serangan *formjacking* di situs web *e-commerce* yang akan dilakukan proses investigasi dengan metode *live forensics* untuk mengumpulkan jejak digital yang tersimpan sementara dalam RAM (Random Access Memory) di komputer milik korban. Investigasi dilakukan dengan menggunakan FTK Imager sebagai alat forensik dalam mengakuisis ram pada lepto *user*. Alasan penelitian ini adalah untuk mengungkap alur pencurian data berupa pencurian data pembayaran dan untuk menemukan bukti digital berupa data kartu kredit yang dicuri oleh pelaku dengan cara mengirimkan ke server miliknya. Tujuan penelitian ini yaitu menunjukkan bagaimana penerapan metode *live forensics* pada beberapa web browser berbeda untuk mengakses *checkout form* di website *e-commerce* serta menemukan jejak digital yang dibutuhkan untuk membuktikan terjadinya serangan *formjacking* dan membantu proses investigasi lebih lanjut.

2. METODE

Metode ini secara sistematis memberikan rincian urutan langkah-langkah, termasuk penjelasan tentang bagaimana penelitian dilakukan, dan dapat digunakan sebagai panduan yang jelas untuk pemecahan masalah, analisis temuan dan kesulitan yang dihadapi. Adapun tahapan dan prosedur penelitian ini dapat dilihat pada Gambar 1

Gambar 1. Alur Tahapan Penelitian

A. Studi Literatur Dan Identifikasi Masalah

Penelitian ini dilakukan studi literatur oleh penulis yang mengumpulkan referensi terkait penelitian termasuk buku, artikel, jurnal ilmiah, dan berbagai situs web yang menampilkan penelitian ilmiah secara online. Langkah selanjutnya melihat referensik terkait dengan forensik digital, *live forensics*, tools FTK Imager, dan data digital pada ram laptop. Langkah selanjutnya adalah mengidentifikasi masalah untuk melakukan skenario penelitian. Masalah dalam penelitian ini adalah pencurian kartu kredit, juga dikenal sebagai formjacking yang terdapat pada form pembayaran atau formulir di situs *e-commerce*. Identifikasi masalah ini berdasarkan jumlah informasi kartu kredit yang dicuri yang dimuat dalam laporan ancaman yang dikeluarkan ISRT.

B. Skenario

Skenario di dalam penelitian ini menjelaskan tahapan dalam melakukan investigasi untuk mendapatkan hasil penelitan yang valid seperti tampak pada Gambar 2. User mengakses laman website *e-commerce* dengan keempat web browser, yakni Opera Mini, Google Chrome, Microsoft Edge, dan Mozilla Firefox dengan menggunakan detail kartu yang berbeda untuk melakukan *checkout*. Setelah melakukan pemilihan barang *user* akan dibawa dil aman *checkout* di mana *user* diminta memasukkan informasi alamat pengiriman dan metode pembayaran berupa kartu kredit. Setelah berhasil melakukan pengisian dan klik tombol *checkout,* akan muncul pesan notifikasi konfirmasi bahwa transaksi telah berhasil dilakukan. Selanjutnya, peneliti akan melakukan proses akuisisi data di *web browser* yang digunakan untuk melakukan transaksi dengan tool FTK Imager. Setelah selesai melakukan proses akuisisi dengan FTK Imager, peneliti akan melanjutkan tahapan analisis hasil dari data akuisis random access memory tersebut.

Gambar 2. Skenario Kasus

C. Persiapan Tools

Persiapan tools atau alat yang digunakan yaitu berupa perangkat hardware dan software yang digunakan untuk mengalisa formjacking. Hardware dan software yang digunakan dalam penelitian ini sebagaimana disajikan dalam Tabel 1 dan Tabel 2 berikut:

Table 1. Perangkat Keras untuk Pengujian

No	Hardware	Keterangan
1	Laptop Asus GL503GE,	Merk
2	Core i7 8th	Prosesor
3	SSD 512GB	SSD M.2
4	SSHD 1TB	Hardisk
5	8 GB Ram DDR4	RAM
6	1TB	Hardisk External

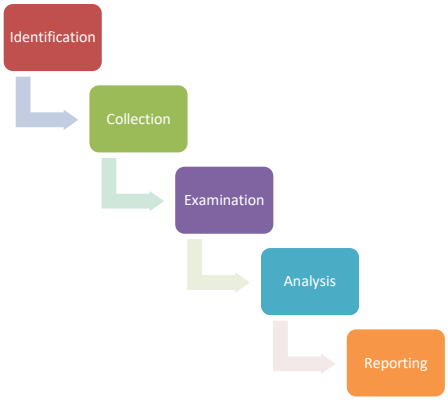
Table 2. Perangkat Lunak untuk Pengujian

No	Software	Keterangan
1	Sistem Operasi Windows 10 Pro 64Bit	Sistem Operasi
2	AccessData FTK Imager Versi 4.5.0.3	Tools Forensik
3	Opera Browser Versi 74.0.3911.160	Web Browser
4	Microsoft Edge Versi 91.0.864.48	Web Browser
5	Mozilla Firefox Versi 89.0	Web Browser
6	Google Chrome Versi 91.0.4472.101	Web Browser

D. Analisis Live Forensik

Syarat utama yang harus dipenuhi untuk live forensic adalah sistem sedang berjalan atau running, karena beberapa data dan informasi dalam random access memory bersifat volatile, yang artinya jika komputer dimatikan atau di-restart, data tersebut akan hilang. Untuk alasan ini, pemrosesan khusus diperlukan untuk akuisisi data yang mudah hilang saat laptop mati. Metode yang diterapkan untuk analisis *live forensics* adalah metode National Institute of Justice (NIJ). Proses tahapan dalam metode NIJ dapat dilihat pada Gambar 3.

p-ISSN : 2502-5724; e-ISSN : 2541-5735



Gambar 3. Metode Tahapan Digital Forensik

Terdapat lima tahapan utama dalam metode NIJ yang dapat dijelaskan sebagai berikut (Ahmadi dan Yudhana, 2018):

1. *Identification*, yaitu mengidentifikasi dan persiapan skenario penelitian dan persiapan alat forensik yang akan digunakan dalam proses penelitian ini.
2. *Collection* yaitu menggunakan tool FTK Imager untuk mengumpulkan data dari proses akuisisi yang dapat digunakan sebagai barang bukti digital pada browser yang digunakan dalam penelitian ini.
3. *Examination*, menggunakan FTK Imager untuk melihat dan melakukan validasi nilai hash dari setiap file memori yang ditemukan selama proses sebelumnya.
4. *Analysis* adalah tahapan menganalisis data dari ram yang dapat digunakan sebagai bukti digital sesuai dengan skenario penelitian.
5. *Report*, yang membandingkan hasil analisis keempat browser untuk menarik kesimpulan apakah history pencurian data kartu kredit dapat dicatat.

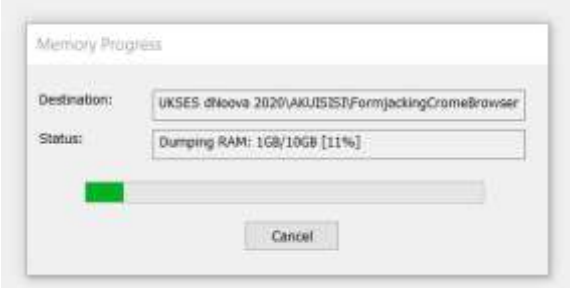
3. HASIL DAN PEMBAHASAN

A. Identification

Proses ini telah dilakukan sesuai dengan skenario pada Gambar 2 dan kebutuhan perangkat keras dan perangkat lunak pada Tabel 1 dan Tabel 2.

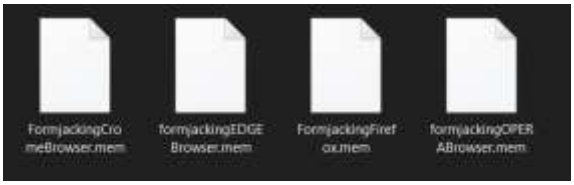
B. Collection

Proses *collection* menggunakan FTK Imager untuk mengumpulkan data dari aktivitas yang dilakukan di pada laman *checkout* website *e-commerce*. Pada RAM di komputer korban dilakukan proses akuisisi dengan melakukan *capture* ketika membukan browser dan mengakses laman *checkout*, dan akan dianalisis untuk mendapatkan proses yang berjalan di sistem seperti tampak pada Gambar 4.



Gambar 4. Proses akuisisi RAM

Hasil dari akuisisi RAM adalah sebuah file dengan ekstensi.mem yang dapat dilihat pada Gambar 5.

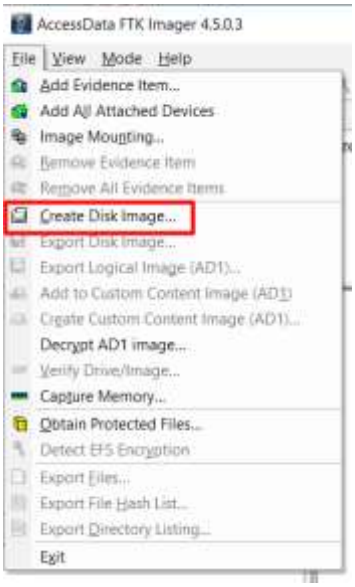


Gambar 5. Hasil Capture Memory

C. Examination

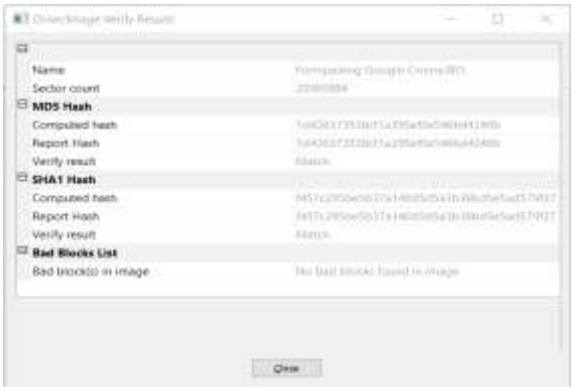
Setelah dilakukan capture memory atau proses akuisisi data pada RAM yang menghasilkan file dengan ektensi .mem, kemudian akan dilakukan pengecekan nilai Hash pada hasil capture memory. Untuk pengecekan nilai hash maka pada FTK

Imager dipilih menu File-pilih Create disk image seperti pada Gambar 6.



Gambar 6. Create Disk Image

Dari hasil proses *disk image* juga akan didapatkan informasi MD5 Hash dan SHA1 Hash seperti tampak pada Gambar 7. Nilai pada hash ini menunjukan keaslian file dan memastikan bahwa pada saat pengujian tidak ada perubahan.



Gambar 7. Hash File Fromjacking Google Chrome

Hasil dari create disk image nilai hash yang menujukan keaslian file bukti digital, sehingga file masih sama dan tidak termodifikasi. Pada hasil verifikasi data nilai hash untuk Google Chrome di atas adalah `1d2463758cf1a395ef0e5466d420b` untuk hash Md5, dan untuk hash SHA1 adalah `f457c295be5b37a140d5d5a3b38bd5e5ad579f27` sebagaimana tampak pada Tabel 3.

Table 3. Nilai Hash

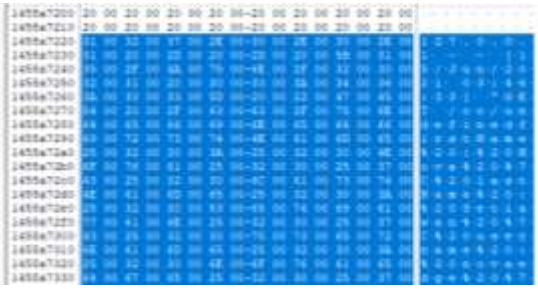
Nama File	MD5	SHA1
Edgebrowser	7b68457ed77ac3ccbbd7e6b0a0072201	59afafeec953903B5e7d77a1b7e80ca0065c99a2
OperaBrowser	15ce82d6d4a7aacea26c6ae428552f66	81fdcd0ff3403a36af5d8c2332f9e42ff03c6fa3
FirefoxBrowser	96ac1fe9df2edb546a1b72cee21a6280	fb25ea8e6f4795783349ebb1fb6ed9fade4be1c5
ChromeBrowser	1d426373538cf1a395ef0e5466d4240b	f457c295be5b37a140d5d5a3b38bd5e5ad579f27

D. Analysis

a) Analisis Microsoft Edge

Setelah dilakukan proses *capture* RAM pada laptop, maka didapatkan file FormjackingEdgeBrowser.mem. Analisis yang dilakukan untuk mendapatkan hasil sebagaimana tampak pada Gambar 8.

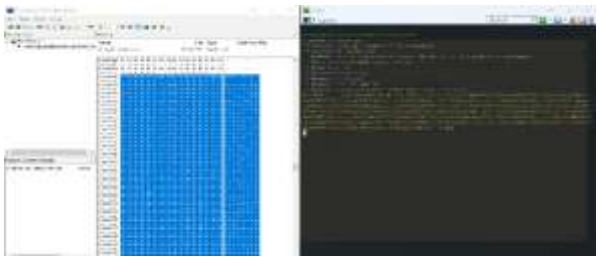
Gambar 8. Nomor Kartu Kredit di browser Microsoft Edge



Gambar 9. Artefak pengiriman data ke server pelaku di browser Microsoft Edge

Pada Gambar 8, di offset `008a64030` terlihat detail nomor kartu kredit yang digunakan oleh *user*. Pada Gambar 9, di offset `1455a7220` sampai dengan `145517330` tampak paket pengiriman detait *checkout* ke alamat server seperti pada Gambar 10.

p-ISSN : 2502-5724; e-ISSN : 2541-5735

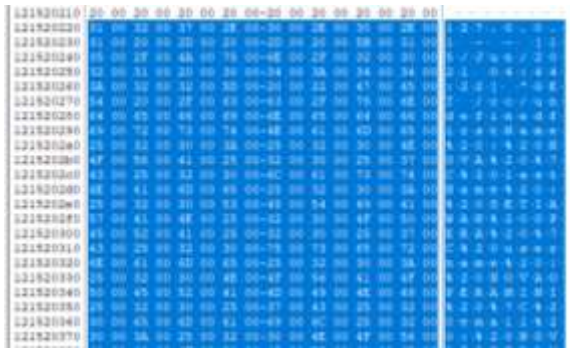


Gambar 10. Data kartu dikirim ke server melalui browser Microsoft Edge

b) Analisis Opera

Proses yang sama dilakukan pada web browser Opera yang hasilnya tampak pada Gambar 11 untuk data kartu kredit dan Gambar 12 untuk detail server yang digunakan oleh pelaku.

Gambar 11. Data Kartu Kredit di Browser Opera



Gambar 12. Detail Server Pelaku di Browser Opera

Pada opera browser menunjukan hal yang sama, yaitu ditemukannya jejak digital proses pencurian data kartu kredit yang digunakan *user* untuk melakukan pembelian.

c) Analisis Mozilla Firefox

Proses yang sama dilakukan pada web browser Mozilla Firefox yang hasilnya tampak pada Gambar 13.

Gambar 13. Artefak digital di browser Mozilla Firefox

Sama dengan kedua browser sebelumnya, tampak bahwa pada browser Mozilla Firefox juga berhasil ditemukan artefak digital pengiriman data kartu kredit korban ke server pelaku.

d) Analisis Google Chrome

Proses yang sama dilakukan untuk terakhir kalinya pada web browser Google Chrome yang hasilnya tampak pada Gambar 14.

Gambar 14. Artefak digital di browser Google Chrome

Tidak berbeda dengan ketiga browser sebelumnya, tampak bahwa pada browser Google Chrome juga berhasil ditemukan artefak digital pengiriman data kartu kredit korban ke server pelaku.

E. Reporting

Hasil dari penelitian ini adalah keempat browser yang digunakan dalam penelitian sama sama mencatat artefak digital berupa kiriman paket data kartu kerdit ke server pelaku. Berikut tabel hasil validasi hasil analisa Random Access Memory (RAM) pada keempat Browser.

Table 4. Hasil investigasi detaik kartu kredit

No	Browser	Nama	Nomor	CVV
1	Microsoft Edge	✓	✓	✓
2	Opera	✓	✓	✓
3	Mozilla Firefox	✓	✓	✓
4	Google Chrome	✓	✓	✓

4. KESIMPULAN

Berdasarkan hasil penelitian yang ada dapat disimpulkan bahwa formjacking dapat berjalan pada keempat browser dan dapat mengirimkan paket data berupa detail dari kartu kredit melalui perintah yang berada dalam kode Javascript. Penelitian ini menggunakan metode *National Institute of Justice* (NIJ) live forensic yang kemudian dijalankan menggunakan tools forensic FTK Imager 4.5.0 sebagai tool pendukung investigasi bukti digital pencurian data formjacking pada website *e-commerce*. Dalam menyakinkan bahwa barang bukti adalah asli yaitu dengan hasil hash MD5 dan SHA1 didapat dari analisi data pada ram laptop. Berdasarkan hasil dari tahapan-tahapan metode yang telah dilakukan, proses investigasi bukti digital formjacking pada website *e-commerce* dapat dikatakan bahwa bukti digital berupa data yang valid.

DAFTAR PUSTAKA

Ahmadi, A. dan Yudhana, A.U., 2018. Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ). J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf, 4(1), p.8.

Alif, M.S. dan Pratama, A.R., 2021. Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia. AUTOMATA, 2(1).

Bintang, R.A.K.N., Umar, R. and Yudhana, A., 2018. Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10. Prosiding SNST Fakultas Teknik, 1(1).

Faiz, M.N., Umar, R. dan Yudhana, A., 2017. Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. Jiska (jurnal informatika sunan kalijaga), 1(3), pp.108-114.

Kurniawan, N.A., 2014. Pencegahan Kejahatan Carding Sebagai Kejahatan Transnasional Menurut Hukum Internasional. Kumpulan Jurnal Mahasiswa Fakultas Hukum, 1(1).

Rahmadi, G. dan Pratama, A.R., 2020. Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia. AUTOMATA, 1(2).

Ramadhani, M.R. and Pratama, A.R., 2020. Analisis Kesadaran Cyber Security Pada Pengguna Media Sosial Di Indonesia. AUTOMATA, 1(2).

Riskiyadi, Moh. 2021. Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime. CyberSecurity dan Forensik Digital,

Vol. 3, No. 2, November 2020, hlm. 12-21. e-ISSN: 2615-8442.

Rochmadi, T., 2019. Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar. Indonesian Journal of Business Intelligence (IJUBI), 1(1), pp.32-38.

Sidiq, M.F. dan Faiz, M.N., 2019. Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital. Jurnal Edukasi dan Penelitian Informatika (JEPIN), 5(1), p.67.

Tian, Y. dan Stewart, C., 2006. History of *e-commerce*. In Encyclopedia of *e-commerce*, e-government, and mobile commerce (pp. 559-564). IGI Global.