Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce

Nova Setiawan
17917120

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2021

Lembar Pengesahan Pembimbing

Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce

Nova Setiawan
17917120

Yogyakarta, Juni, 2021

Pembimbing I

Ahmad M. Rafie Pratama, S.T., M.I.T.,PhD.

Lembar Pengesahan Penguji

Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce

Nova Setiawan

17917120

Yogyakarta, Februari, 2022

Tim Penguji,

Ahmad M. Raf'ie Pratama, S.T., M.I.T.,PhD.
Ketua

Dr. Imam Riadi, S.Pd., M.Kom.
Anggota I

Dr. Yudi Prayudi., S.Si., M.Kom.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce

Pertumbuhan bisnis *online* yang tinggi serta bergesernya perilaku konsumen yang menginginkan transaksi cepat, fleksibel dan hemat waktu menyebabkan pertumbuhan *e-commerce* kian meningkat pula. Hal ini menandakan semakin ketatnya persaingan di dunia *e-commerce* dalam merebut pasar. Pertumbukan *e-commerce* diikuti pula dengan pertubuhan kerentanan yang mengancam penggunan dalam bertransaksi menggunakan platform website *e-commerce*. Kerentanan tersebut ada pada pencurian data digital berupa detail kartu kredit pengguna layanan ecommerce. Terdapat kode yang mampu mencuri atau menduplikasi dan mengirimkan data pembayaran ke server pelaku. Kode jahat tersebut dikenal dengan formjacking atau pencurian data melalui form pembayaran dengan memanfaatkan kode javascript yang telah di sisipkan pada website. Dengan mengacu pada framework *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 scenario pada empat browser yang akan dianalisis yaitu Google Chrome, Mozilla Firefox, Opera Mini dan Microsoft Edge di perangkat computer windows 10. Jejak digital yang ditinggalkan diakuisisi dan di analisis dengan bantuan perangkat forensik FTK Imager 4.5.0. Barang bukti digital berupa log ip pada browser yang menunjukan data dikirmkan ke server pelaku. Hasil dari penelitian ini dapat dijadikan rujukan bagi penegak hukum untuk mengungkapkan kejahatan digital berupa formjacking pada website e-commerce

Kata kunci

Formjacking, Live Forensik, Digital Forensik.

Abstract

Live Forensics Method For Investigating Formjacking Attacks On Ecommerce Websites

The high growth of online business and the shifting behavior of consumers who want fast, flexible and time-saving transactions have caused the growth of e-commerce to increase as well. This indicates the increasingly fierce competition in the world of e-commerce in capturing the market. The growth of e-commerce is also followed by the growth of vulnerabilities that threaten users in transacting using e-commerce website platforms. The vulnerability is in the theft of digital data in the form of credit card details of e-commerce service users. There is code that is capable of stealing or duplicating and sending payment data to the perpetrator's server. This malicious code is known as formjacking or data theft through payment forms by utilizing javascript code that has been inserted on the website. By referring to the National Institute of Justice (NIJ) framework which includes identification, collection, examination, analysis, and reporting, this study aims to show how the live forensics method on RAM on the victim's computer can be used as an investigative technique for formjacking attacks. Tests were carried out according to scenarios on four browsers to be analyzed, namely Google Chrome, Mozilla Firefox, Opera Mini and Microsoft Edge on Windows 10 computer devices. The digital footprints left were acquired and analyzed with the help of the forensic tool FTK Imager 4.5.0. Digital evidence in the form of an IP log on a browser that shows the data sent to the perpetrator's server. The results of this study can be used as a reference for law enforcement to reveal digital crimes in the form of formjacking on e-commerce websites

Keywords

Formjacking, Live Forensics, Digital Forensics

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Juni 2021

Nova Setiawan, S.Kom.

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dari tesis ini

- Setiawan, N., Riadi, I., & Prayudi, Y. (2021). Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce; http://jurnal.unmuhjember.ac.id/JUSTINDO.vol7(2)

Kontributor	Jenis Kontribusi
Nova Setiawan	Mendesain eksperimen (70%) Menulis *paper* (100%)
Imam Riadi	Memberi saran pada *paper* (30%) Mereview Artikel
Yudi Prayudi	Memberi saran pada *paper* (30%) Mereview Artikel

Halaman Kontribusi

Penelitian ini merupakan hasil dari saran dan bimbingan dari berbagai pihak baik saat sedang seminar proposal, seminar kemajuan, hingga seminar pendadaran. Pihak-pihak tersebut antara lain adalah Dr. Imam Riadi, S.Pd., M.Kom., Dr. Yudi Prayudi, S.Si., M.Kom., Ahmad M. Raf'ie Pratama, S.T., M.I.T.,PhD., dan Erika Ramadhani, S.T., M.Eng.

Halaman Persembahan

Alhamdulillah, puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan banyak sekali rahmat dalam kehidupan. Selanjutnya penelitian ini penulis persembahkan kepada orang-orang yang telah mendukung dan memberikan semangat serta motivasi kepada penulis untuk dapat menyelesaikan pendidikan Pascasarjana di Universitas Islam Indonesia Yogyakarta. Persembahan secara khusus saya berikan kepada :

1. Kedua orang tua saya yang tak kenal lelah memberikan motivasi, doa dan harapan untuk terus menjadi lebih baik dalam kehidupan.
2. Istri saya yang tak kenal lelah memberikan dukungan, motivasi, doa dan harapan untuk terus menjadi lebih baik dalam kehidupan.
3. Saya ucapkan terima kasih kepada dosen pembimbing yang telah mengajar dan membimbing dengan sabar.
4. Saya mengucapkan terima kasih kepada rekan-rekan dan adik tingkat yang banyak memberikan masukan dan saran dalam menyusun laporan tesis ini dan yang terakhir saya ucapkan terima kasih.

Kata Pengantar

Alhamdulillah puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan banyak sekali rahmat dalam kehidupan penulis sehingga dapat menyelesaikan laporan tesis dengan judul " Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce". Penulis sampaikan ucapan terimakasih kepada pihak-pihak yang telah membantu dalam terselesainya penyusunan laporan tesis ini yaitu :

1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D., selaku Rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk berkembang bersama di Universitas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D., selaku Ketua Program Studi Informatika Program Magister Fakultas Teknologi Industri Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Ahmad M. Raf'ie Pratama, S.T., M.I.T.,PhD., selaku dosen pembimbing I yang selalu memberikan masukan dan saran selama proses pembuatan tesis ini.
5. Ibu Erika Ramadhani, S.T., M.Eng., selaku dosen pembimbing II yang selalu memberikan movitasi dan saran dalam penelitian tesis ini.
6. Bapak Dr. Imam Riadi, S.Pd., M.Kom., selaku Dosen Penguji Ujian Tesis yang telah memberikan berbagai saran perbaikan untuk penelitian ini.
7. Bapak Dr. Yudi Prayudi., S.Si., M.Kom., selaku Dosen Penguji Ujian Tesis yang telah memberikan berbagai saran perbaikan untuk penelitian ini.
8. Seluruh dosen, staff administrasi dan civitas Magister Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama studi.
9. Semua pihak yang telah membantu dalam penyusunan tesis ini.

Dalam penulisan tesis ini penulis menyadari bahwa penelitian ini masih perlu banyak masukan dan saran yang membangun dari pembaca untuk pengembangannya. Akhir kata penulis sampaikan terimakasih, semoga laporan tesis ini dapat bermanfaat bagi pembaca.

Yogyakarta Februari 2022

Penulis

UNIVERSITAS ISLAM INDONESIA

Daftar Isi

Daftar Tabel

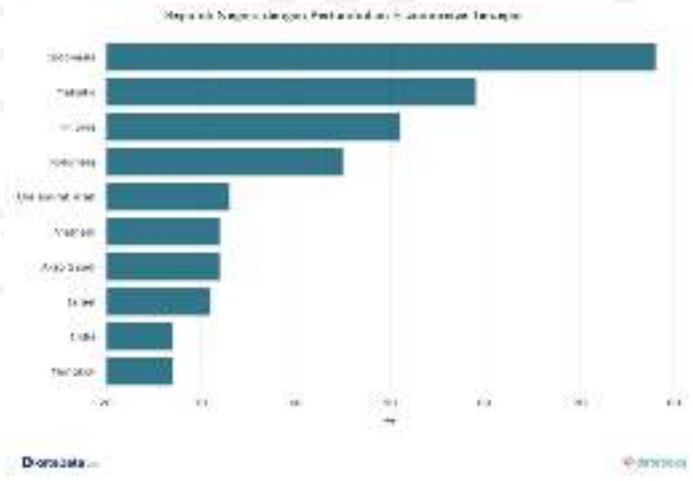
Daftar Gambar

UNIVERSITAS ISLAM INDONESIA

BAB 1
Pendahuluan

1.1 Latar Belakang

Munculnya beberapa *platform* belanja *online* saat ini sangat membantu proses perkembangan dan perubahan pada sektor transaksi jual beli. Dimana biasanya dilakukan dengan cara konvensional berubah menjadi transaksi *online* yang dilakukan melalui *website*. Dalam hal ini yang mengalami perkembangan adalah proses transaksi jual beli melalui *website e-commerce* (Gambar 1.1). *E-commerce* merupakan kegiatan perdagangan secara elektronik yang mencangkup transaksi jual, beli, pertukaran informasi tentang produk yang dilakukan melalalui jaringan internet (Puspitaningrum, 2017). Indonesia merupakan negara yang mengalami pertumbuhan *e-commerce* tercepat didunia. Indonesia mempimpin dengan pertumbunhan 78% pada 2018, jumlah ini diikuti dengan pengguna internet di Indonesia yang lebih dari 100 juta pengguna yang menjadi kekuatan mendorong pertumbuhan *e-commerce*. Rata-rata transaksi yang dilakukan orang Indonesia adalah sekitar Rp. 3,19 Juta per orang. Sekitar 17,7% responden membelanjakan uangnya untuk membeli tiket pesawat dan memesan hotel secara daring. Sebanyak 11,9% responden membelanjakan uangnya untuk produk pakaian dan alas kaki. Adapun kategori terpopuler ketiga adalah produk kesehatan dan kecantikan yang dipilih oleh 10% responden[1].



Gambar 1.1 Sepuluh Negara dengan Pertumbuhan E-commerce Tercepat

[1] https://databoks.katadata.co.id/datapublish/2019/04/25/indonesia-jadi-negara-dengan-pertumbuhan-e-commerce-tercepat-di-dunia

Gambar 1.2 Penggunan e-commerce di Indonesia (www.wearesocial.com)

Hootsuite[2] September 2019 mencatat Indonesia memiliki tingkat pengguna *e-commerce* tertinggi di dunia. Laporan yang dirilis ini menyebutkan 96% pengguna internet pernah mencari produk atau layanan untuk dibeli secara *online*. Adapun kunjungan pada toko retail *online* atau situs terkait dilakukan 91% dari total pengguna internet. Para pengguna internet juga melakukan pembayaran produk atau layanan *online* sebesar 90%. Secara berurutan, mereka melakukan pembayaran *online* melalui ponsel serta laptop atau komputer sebesar 79% dan 29%[3]. Kemudahan yang didapatkan dalam proses *transaksi e-commerce* dan dengan pertumbuhan yang sangat cepat ini memang sangat memudahkan dalam melakukan transaksi jual beli (Purbasari, 2017). Selain kemudahan yang didapatkan ada hal yang mungkin tidak terfikirkan dalam proses transaksi online di *website e-commerce* yaitu serangan yang dilakukan oleh orang yang tidak bertanggung jawab untuk mendapatkan data pribadi dan mencuri akun pembayaran contohnya seperti kartu kredit (Novryan Alfin Kurniawan, 2014). Berdasarkan laporan ancaman tahunan perusahaan keamanan siber Symantec yang bertajuk *Internet Security Threat Report (ISTR),* mengungkapkan bahwa pada tahun 2019 serangan oleh penjahat siber kian agresif, merusak, dan menjadi ancaman serius. Kini, para penjahat di dunia maya menggandakan metode-metode alternatif, seperti *Formjacking*. Serangan ini menggunakan kode *JavaScript* berbahaya untuk mencuri detail

[2] Hoosuite merupakan sistem manajemen berbasis sosial media berbasis web yang menyediakan layanan media daring
[3] https://datareportal.com/reports/digital-2019-ecommerce-in-indonesia

kartu kredit dan informasi lainnya dari formulir pembayaran pada halaman *form check-out* di situs *e-commerce.*

Selain kemudahan yang didapatkan ada hal yang mungkin tidak terfikirkan dalam proses transaksi online di website e-commerce yaitu serangan yang dilakukan oleh orang yang tidak bertanggung jawab untuk mendapatkan data pribadi dan mencuri akun pembayaran contohnya seperti kartu kredit (N A Kurniawan, 2014). Berdasarkan laporan ancaman tahunan perusahaan keamanan siber Symantec yang bertajuk Internet Security Threat Report (ISTR), mengungkapkan bahwa pada tahun 2019 serangan oleh penjahat siber kian agresif, merusak, dan menjadi ancaman serius. Kini, para penjahat di dunia maya menggandakan metode-metode alternatif, salah satunya adalah Formjacking. Serangan ini menggunakan kode JavaScript berbahaya yang disisipkan pada script website untuk mencuri detail kartu kredit dan informasi lainnya dari formulir pembayaran pada halaman form check-out di situs e-commerce.

Browser yaitu aplikasi yang digunakan untuk mengakses webisite ecommerce. Browser selalu mengembangkan fitur keamanannya karena informasi pada internet sangat rentan. Semua pertukaran informasi terjadi di internet termasuk pada saat proses pembelian berlangsung. Oleh karena itu, informasi dan internet saling berkaitan.(Faiz et al., 2017). Browser harus meningkatan keamanan disisi pengguna agar informasi yang diakses oleh pengguna tidak dapat diketahui oleh pengguna lain atau pelaku kejahatan (Rochmadi, 2019).

Data nomer kartu kredit, nama dan CVV merupakan hal yang sangat penting dalam akun belanja sebagai metode pembayaran dan termasuk data volatile atau data sementara yang ada pada saat komputer dalam keadaan menyala dan jika komputer mati maka data akan hilang (Bintang et al., 2018). Menyadari pentingnya untuk mengatasi kejahatan pencurian data di website, maka perlu adanya sebuah panduan tentang tahapan-tahapan dan teknik investigasi pada website e-commerce untuk menghasilkan pembuktian secara ilmiah. Investigasi forensik yang dilakukan investigator dilakukan sesuai dengan prosedur forensik digital dalam mencari barang bukti. Investigasi forensik terdapat metode yang digunakan dalam mencari barang bukti yaitu live forensic. Live forensic yaitu metode investigasi yang dilakukan saat tindak kejahatan berlangsung (Pii & Horsman, 2017). Dalam penelitian ini, investigator menggunakan metode live forensic.

Forensic Toolkit Imager (FTK Imager) adalah aplikasi forensik digital yang menggunakan teknologi real-time(live) atau statis atau bahkan keduanya selama investigasi (Sidiq & Faiz, 2019). FTK Imager digunakan untuk melakukan akuisisi data, dimana sistem

akuisisi tersebut merupakan sistem yang berfungsi untuk mengambil, mengumpulkan dan menyiapkan data, serta mengolahnya untuk menghasilkan data yang dibutuhkan. Jenis dan metode yang dipilih dirancang untuk menyederhanakan setiap langkah yang diambil dalam keseluruhan proses (Nur Faiz et al., 2018).

Pada penelitian Muhammad Nur Faiz, dkk yang berjudul "Experimental Analysis of Web Browser Sessions Using Live Forensics Method" (Umar et al., 2016). Studi ini menunjukkan bahwa kata kunci ganja dan metamfetamin digunakan dalam eksperimen yang dilakukan, dan semua kata kunci dicatat dalam RAM. Pada saat yang sama, akses jaringan dari bukti digital yang ditemukan didasarkan pada planetdrugsdirect.com dan ID Facebook dan ID email yang ditemukan dalam eksperimen yang dilakukan. ID Facebook menggunakan eksperimen, dan ID email menggunakan practicecoba1@gmail.com. Eksperimen simulasi dilakukan menggunakan browser web Google Chrome dan Mozilla Firefox dalam mode privat. Setelah menggunakan DumpIt untuk mendapatkan hasil pada media penyimpanan, kloning dan periksa nilai hash Pada file asli dan cocok dengan hasil kloning. Analisis lebih lanjut penggunaan web browser saat komputer dihidupkan. Proses analisis metode direct forensik dilakukan dengan mencari bukti seperti kata kunci pencarian, akses jaringan, ID email dan ID Facebook dari dua browser. Studi penelitian dari Tri Rochmadi yang berjudul "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar" (Rochmadi, 2019). Dengan berkembangnya internet cepat yang semakin mudah diakses dimana saja, cybercrime terus berkembang dan berinovasi. Browser juga disesuaikan untuk meningkatkan keamanan di sisi pengguna, sehingga informasi yang diakses oleh pengguna tidak dapat diketahui oleh pengguna lain.

Penelitian ini dibuat dengan memperhatikan penelitian-penelitian yang sudah ada sebelumnya. Perbedaan dari penelitian sebelumnya yaitu penelitian ini mengangkat tentang serangan formjacking pada website ecommerce sebagai study kasus, menggunakan live forensics untuk mendapatkan data yang terekam pada RAM (Random Access Memory), serta dengan menggunakan FTK Imager sebagai tools forensics. Alasan dilakukan penelitian ini untuk mengetahui alur pencurian data formjacking dan menemukan artefak bukti digital berupa data kartu kerdit yang dicuri pelaku. Tujuan penelitian ini yaitu menerapkan live forensic pada web browser untuk mengakses form checkout website ecommerce serta menemukan bukti digital dari analisis formjacking pada browser Microsoft Edge, OperaMini, Mozilla Firefox, dan Google Crome.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka yang menjadi rumusan masalah adalah sebagai berikut:

a. Bagaimana analisis karakteristik web browser terhadap *formjacking*.
b. Bagaimana analisis proses akuisisi dan investigasi secara live forensik adanya *formjacking* pada *website ecommerce*.
c. Bagaimana penerapan metode *live forensik* untuk mengumpulkan bukti digital pada website *ecommerce.*

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan penelitian ini adalah sebagai berikut:

a. Untuk mengetahui karakteristik bukti digital berupa *formjacking* pada web ecommerce.
b. Untuk menganalisa ancaman yang ada pada website *ecommerce*
c. Untuk menerapkan *Live Forensik* dalam proses pengumpulan bukti digital pada website *ecommerce.*

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini meliputi:

a. Penelitian ini dilakukan untuk mengetahui bukti digital pada *formjacking* website *ecommerce*
b. Penelitian ini akan menerapkan metode *live forensik* untuk mengumpulkan barang bukti di empat *web browser* untuk mengumpulkan barang bukti digital.

1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini antara lain :

a. Dengan adanya penelitian ini, diharapkan dapat melakukan analisa live forensik terhadap serangan website ecommerce.
b. Menghasilkan langkah yang tepat penanganan formjecking di website e-commerce, diharapkan dapat memberikan kontribusi dan kemudahan untuk penyidik dalam melakukan investigasi
c. Dengan adanya penelitian ini juga diharapkan dapat memberikan kontribusi bagi penelitian selanjutnya.

1.6 Literatur Review

Pada bagian ini akan di ulas tentang penelitian terkait yang telah dilakukan sebelumnya dengan topik *live forensics, e-commerce*, xss dalam penyelesain kasus-kasus yang berhubungan dengan digital forensik membutuhkan sebuah framework untuk membantu mempermudah pengumpulan barang bukti digital.

Penelitian ini membahas jika kejahatan email dapat dicegah dengan penggunaan username dan password yang rumit, selain itu teknik hacking yang mulai meningkat seiring dengan penggunaan tools yang freeware menyebabkan penyalahgunaan email menjadi lebih banyak. Maka, penelitian ini mengusulkan analisis forensics live di sistem operasi terbaru yaitu Windows 10. Studi kasus berfokus pada kemanan beberapa email seperti Gmail, Yahoo dan Outlook dan beberapa browser seperti Google Chrome, Mozilla Firefox, dan Microsoft Edge. Berdasarkan penelitian yang dilakukan oleh Ellick M. Chan maka peneliti akan menggunakan metodologi penelitian The U.S. National Institute of Justice (NIJ) (Faiz et al., 2016).

Telah banyak penelitian dalam digital forensik yang membahas tentang investigasi bukti digital pada platform web. Penelitian penerapan Framework NIST SP 800 -30 yang dilakukan oleh (Nugraha, 2016) tentang penerapan manajemen risiko pada sistem informasi menyimpulkan bahwa Framework NIST SP 800-30 membuktikan bahwa dengan melakukan menggunakan Framework NIST - 800-30 hasilnya dapat mengurangi risiko ancaman pencurian data dan informasi yang berpotensi disalah gunakan.

Investigasi kasus cybercrime yang terjadi di Line Messenger berbasis web. Metode yang digunakan untuk penelitian ini, yaitu menggunakan metode National Institute of Justice (NIJ). Penelitian ini dalam prosesnya berhasil diperoleh lokasi file log, cache, dan bukti digital dari simulasi tindak kejahatan yang didapatkan melalui proses penyadapan aplikasi Line Messenger berbasis android milik korban. Bukti digital yang didapat dari proses eksplorasi direktori laptop menggunakan tools FTK Imager tidak hilang walaupun chat pada aplikasi Line Messenger korban dan pelaku telah dihapus. Bukti digital forensik yang didapat diharapkan dapat memperkuat bukti kasus kejahatan di pengadilan dalam bentuk hasil analisis bukti digital.

Teknik digital forensik digunakan dengan melakukan analisis komputer atau perangat lunak digital. Analisis digital forensik terbagi menjadi 2 kategori yaitu Dead/Tradisional dan Live. Analisis Dead menyangkut data yang tersimpan permanen di dalam suatu perangkat, sedangkan Analisis Live analisis yang bersifat sementara atau data

yang disimpan dalam perangkat lunak. Paper ini mengusulkan analisis forensik live disistem menggunakan Operasi Sistem Windows10 yg terbaru saat ini. Metode yang akan digunakan yaitu National Institute of Justice (NIJ) dengan tahapan berikut Collection, Examination, Analysis dan Reporting. Teknik live forensics ini sangat bergantung pada keadaan komputer yang sedang menyala, karena membutuhkan data yang berjalan pada Random Access Memory (RAM). Data pada RAM disebut juga data volatile atau data sementara yaitu data yang hanya terdapat saat komputer menyala jika komputer mati maka data itu akan hilang. Data volatile ini berisi data penting seperti username, password, file akses, file modifikasi, aplikasi yang digunakan, kata kunci pencarian.(Bintang et al., 2018).

Solid State Drive (SSD) adalah solusi terbaru untuk mempercepat pemrosesan data di berbagai komputer desktop multiplatform. Fitur TRIM pada SSD berguna untuk menghilangkan data sampah yang dihapus secara permanen oleh pengguna, manfaat dari pendekatan ini adalah dapat memperpanjang umur perangkat SSD. Paradoks penggunaan metode ini adalah dengan bukti berupa komputer dengan penyimpanan SSD, sangat sulit bagi penyidik forensik untuk memulihkan data yang dihapus dalam konteks kejahatan dunia maya. Subjek eksperimen dalam penelitian ini didasarkan pada perspektif sistem operasi mainstream, yaitu Windows, Linux, dan Macintosh yang diinstal pada SSD, yang masing-masing mensimulasikan penghapusan data yang disimpan, dan membandingkan konfigurasi yang diaktifkan dengan TRIM dan yang dinonaktifkan. Metode forensik digital yang diterapkan dalam hal ini adalah National Institute of Justice (NIJ), yang digunakan dalam penelitian ini sebagai acuan praktik forensik digital. Perangkat lunak SLUTH KIT Autopsy adalah alat forensik digital yang digunakan untuk memperoleh dan menganalisis bukti SSD dari sudut pandang penyidik dalam simulasi kasus penelitian ini. (Ramadhan & Mualfah, 2020)

Media penyimpanan telah banyak berubah, tidak hanya lebih banyak Minimalisme, tetapi juga dalam kapasitas itu sendiri. Forensik digital hari ini adalah bidang penyimpanan data berbasis media yang berkembang untuk berbagai Akuisisi data, polusi data, kloning data, dan persyaratan lainnya. CD ROM seperti CD dan DVD, termasuk media enyimpanan yang digunakan untuk menyimpan data pada Format file audio dan video. Dalam studi drive optik khusus, CD-R/DVD dapat melalui proses pencitraan untuk mendapatkan ruang yang tidak terisi, Berisi data yang telah diformat atau dihapus sebelumnya. Kajian ini membahas tentang proses pemulihan file yang diformat dengan alat Forensik Otopsi selama inspeksi dan inspeksi menganalisa. Pengambilan bukti digital objek penelitian melalui metode

forensik statis, penilaian dan analisis adaptor menggunakan metode forensik National Institute of Justice (NIJ) ke bukti digital subjek penelitian (Riadi et al., 2019).

Gupta, Govil, & Singh, (Gupta et al., 2015) bahwa baru-baru ini menjelaskan prediksi kerentanan berdasarkan model machine-learning mendapatkan popularitas dalam keamanan Web, model ini memberikan cara efisien dan sederhana untuk menangani masalah keamanan aplikasi Web. Ada state-of-art Cross-Site Scripting (XSS) yaitu pendekatan prediksi kerentanan yang tidak mempertimbangkan masukan user konteks sebagai output-pernyataan yang sangat penting untuk mengidentifikasi kerentanan keamanan konteks-sensitif. Dalam tulisan ini, mereka mengusulkan algoritma ekstraksi fitur baru untuk mengekstrak fitur dasar dan konteks dari kode sumber aplikasi Web. Pendekatan menggunakan fitur ini untuk membangun memprediksi Cross Site Sripting (XSS) dari kerentanan keamanan konteks-sensitif berbasi model machine-learning. Hasil penelitian menunjukkan bahwa model prediksi fitur yang diusulkan berdasarkan dapat membedakan kode rentan dari kode non-rentan pada tingkat palsu yang sangat rendah. penelitianya menuturkan semakin banyak sensitif data yang tersedia maka hacker menjadi lebih tertarik untuk menambil data yang nantinya dapat menyebabkan kerusakan besar dilakukan oleh Sonewar & Mhetre, (2015)

Serangan ini dapat digunakan untuk menyusup ke aplikasi Web yang dapat menyebabkan perubahan pada script web atau mengungkapkan informasi penting. Fromjacking adalah salah satu serangan yang lebih bahaya dimana penyerang memberikan masukan pada aplikasi Web yang dapat menyebabkan perubahan dalam dari halaman Web. Model pemetaan mencegah jenis serangan di mana permintaan dipetakan pada permintaan dapat digunakan secara efektif untuk mendeteksi jenis seperti serangan dan logika pencegahan dapat diterapkan.

Table 1.1 Literatur Review

No	Literatur	Keyword	Metode	Latar Belakang	Hasil
1	(Faiz et al., 2016).	*Email, Forensik Sistem Operasi, Live Forensik*	Live Forensik	Kejahatan email dapat diminimalisir dengan penggunaan username dan password yang rumit, selain itu teknik hacking yang mulai meningkat seiring ngan penggunaan tools yang freeware Menyebabkan penyalahgunaan email menjadi lebih banyak. Digital forensics sabagai suatu ilmu untuk menemukan barang bukti dari kejahatan yang terjadi dan dapat dipertanggung jawabkan	Dari hasil penelitian menunjukan jika, type public dengan email Outlook, Yahoo dan Gmail username masih dapat terlihat sedangkan untuk penerima atau recipient, body dan subject email hanya Gmail yang hanya dapat dilihat sedangkan untuk password sebaliknya yaitu hanya Gmail yang hanya tidak terlihat. Untuk type private username hanya dapat terlihat pada Outlook dan Yahoo
2	(Nugraha, 2016)	Risk Management, information system, NIST	NIST SP 300-80	Penerapan manajemen risiko pada sistem informasi menyimpulkan bahwa Framework NIST SP 800-30 membuktikan bahwa dengan melakukan menggunakan	NIST memberikan 3 tahapan yaitu penilaian risiko, peringanan risiko, dan evaluasi risiko. Hasil dari penilaian risiko yang dilakukan,

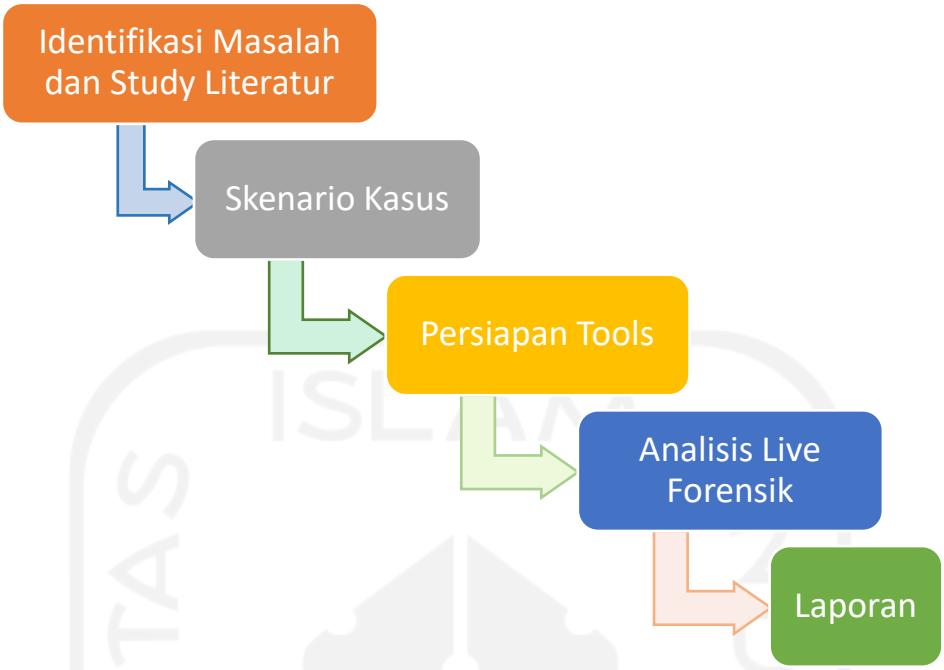
No	Literatur	Keyword	Metode	Latar Belakang	Hasil
				Framework NIST - 800-30 hasilnya dapat mengurangi risiko ancaman pencurian data dan informasi yang berpotensi disalah gunakan.	diketahui terdapat 3 risiko yang dapat mengganggu keberlangsungan sistem informasi Perguruan tinggi, dan masing- masing risiko memiliki tingkat risiko, diantaranya tinggi, dan sedang. Hasil akhir dari kegiatan ini berupa rekomendasi untuk mengurangi risiko yang akan terjadi pada sistem informasi
3	M. Abdul Aziz 2018	Forensik, LINE, Investigasi, cybercrime.	National Institute of Justice (NIJ)	Aplikasi LINE messenger yang berbasis web atau smartphone, sangat memungkinkan dimanfaatkan untuk melakukan tindak kejahatan digital dengan menggunakan layanan, informasi pribadi user, maupun dengan meretas aplikasi LINE messenger tersebut. Penelitian ini	Penelitian ini dalam prosesnya berhasil diperoleh lokasi file log, cache, dan bukti digital dari simulasi tindak kejahatan yang didapatkan melalui proses penyadapan aplikasi Line Messenger berbasis android milik korban . Bukti digital yang didapat dari proses eksplorasi direktori laptop menggunakan tools FTK Imager tidak

No	Literatur	Keyword	Metode	Latar Belakang	Hasil
				menjelaskan tahapan-tahapan investigasi kasus cybercrime yang terjadi di LINE messenger berbasis web.	hilang walaupun hat pada aplikasi Line Messenger pelaku telah dihapus.
4	Bintang 2018	Live Forensics, Media Sosial, Browser	National Institute of Justice (NIJ)	Teknik digital forensik digunakan dengan melakukan analisis komputer atau perangat lunak digital. Analisis digital forensik terbagi menjadi 2 kategori yaitu Dead/Tradisional dan Live. Analisis Dead menyangkut data yang tersimpan permanen di dalam suatu perangkat, sedangkan Analisis Live analisis yang bersifat sementara atau data yang disimpan dalam perangkat lunak. Paper ini mengusulkan analisis forensik live disistem Operasi Sistem Windows10	Dengan metode National Institute of Justice (NIJ) dengan tahapan berikut Collection, Examination, Analysis dan Reporting. Metode berikut diharapkan dapat menghasilan bukti digital forensik yang dapat mengetahui tingkat keamanan pada media sosial Facebook, Instagram dan Twitter

No	Literatur	Keyword	Metode	Latar Belakang	Hasil
5	(Ramadhan & Mualfah, 2020	Solid State Drive Digital Forensik Investigation Recovery Files Operating System	National Intitute of Justice (NIJ)	Solid State Drive (SSD) adalah solusi terbaru untuk mempercepat pemrosesan data di berbagai komputer desktop multiplatform. Fitur TRIM padax, dan Macintosh yang diinstal pada SSD, yang masing-masing mensimulasikan penghapusan data yang disimpan, dan membandingkan konfigurasi yang diaktifkan dengan TRIM dan yang dinonaktifkan. yang ada pada SSD berguna untuk menghilangkan garbage data yang dihapus permanen oleh user, dimana metode ini memiliki benefit untuk memperpanjang usia pakai dari perangkat SSD.	Metode forensik digital yang diterapkan dalam hal ini adalah National Institute of Justice (NIJ), yang digunakan dalam penelitian ini sebagai acuan praktik forensik digital. Perangkat lunak SLUTH KIT Autopsy adalah alat forensik digital yang digunakan untuk memperoleh dan menganalisis bukti SSD dari sudut pandang penyidik dalam simulasi kasus

No	Literatur	Keyword	Metode	Latar Belakang	Hasil
6		Bukti Digital, Forensik, National Institute of Justice, Optikal Drive	National Institute of Justice (NIJ)	Media penyimpanan telah banyak berubah, tidak hanya lebih banyak Minimalisme, tetapi juga dalam kapasitas itu sendiri. Forensik digital hari ini adalah bidang penyimpanan data berbasis media yang berkembang untuk berbagai Akuisisi data, polusi data, kloning data, dan persyaratan lainnya. CD ROM seperti CD dan DVD, termasuk media penyimpanan yang digunakan untuk menyimpan data pada Format file audio dan video. Dalam studi drive optik khusus, CD-R/DVD dapat melalui proses pencitraan untuk mendapatkan ruang yang tidak terisi, Berisi data yang telah diformat atau dihapus sebelumnya.	Kajian ini membahas tentang proses pemulihan file yang diformat dengan alat Forensik Otopsi selama inspeksi dan inspeksi menganalisa. Pengambilan bukti digital objek penelitian melalui metode forensik statis, penilaian dan analisis adaptor menggunakan metode forensik National Institute of Justice (NIJ) ke bukti digital subjek penelitian.

1.7 Metode Penelitian



Gambar 1.3 Alur desain Penelitian

Alur desain penelitian terbentuk, dilakukan pengumpulan dan pemetaan atas literatur dan penelitian terdahulu terkait dengan penelitian investigasi live forensik sehingga fokus untuk menetapkan metode yang tepat dan sesuai. Adapun metode yang dipilih dalam penelitian ini adalah *live forensic* dengan menerapkan *Framework National Institute of Justice (NIJ).*

1.8 Sistematika Penulisan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut :

BAB I Pendahuluan

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tuuan penelitan, manfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II Kajian Teori

Pada Bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang berkaitan dengan penelitian yang sedang diteliti.

BAB III Metodologi Penelitian

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta perancangan antar muka aplikasi yang akan dibuat.

BAB IV Pembahasan

Pada Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis dan evaluasi dari penelitian yang diangkat.

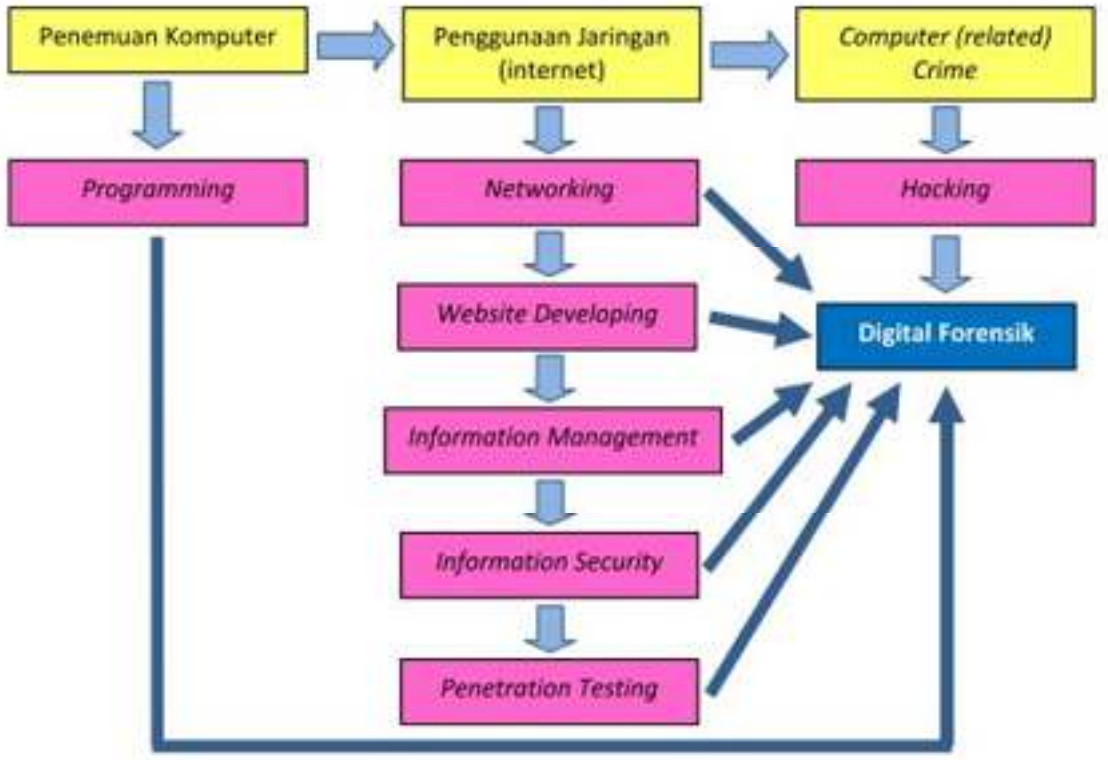
BAB V Penutup

Pada bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

BAB 2
Kajian Teori

2.1 Digital Forensik

Menurut (Nuh Al-Azhar, 2012) digital forensik merupakan *"aplikasi bidang ilmu pengetahuan dan teknologi komputer yang digunakan dalam kepentingan pembuktian hukum (pro justice), untuk melakukan pembuktian kejahatan dengan menggunakan teknologi atau komputer secara ilmiah hingga memdapatkan bukti digital yang digunakan untuk menjerat pelaku kejahatan".* Forensik digital mengacu pada proses akuisisi, pelestarian, analisis, dan penyajian bukti digital yang dihasilkan dari kejahatan terkait digital (Sant, 2014). Digital forensik juga merupakan salah satu bidang spesialis pemahaman komputer yang sangat luas. Digital forensik menjadi salah satu bentuk spesialisasi untuk melakukan investigasi yang berhubungan dengan kejahatan komputer (computer related crime). Digital forensik akan melakukan pemeriksaan setiap barang bukti elektronik dalam rangka mencari data-data digital yang berkaitan dengan kesus kejahatan dan pelakunya.



Gambar 2.1 Spesialisasi yang berkaitan dengan digital forensik.

2.2 Bukti Digital

Barang bukti sangat penting akan keberadaanya karena barang bukti mengarah pada proses bagaimana, siap, dan dimana pelaku melakukan dan tidak hanya halteknis saja tapi barang bukti mempengaruhi hasil dipengadilan nantinya. untuk itu sangat perlu memperhatikan perubahan disetiap tahap dalam proses analisa forensic yang kita kembangkan. Berikut ini beberapa definisi tentang barang buktidigital) :

a) Kelompok kerja yang bernama "The Scientific Working Group on Digital Evidence" (SWGDE), (US Federal Crime Laboratory) dan supervisi dari Internasional Organization on Computer Evidence (IOEC).

   Bukti Digital adalah "information of probative value stored or transmitted in digital form." Artinya bukti digital adalah segala informasiyang bersifat membuktikan terhadap nilai yang tersimpan atauditransmisikan dalam bentuk digital. berdasarkan definisi tersebut, buktidigital tidak hanya meliputi bukti yang dihasilkan atau ditransmisikanmelalui jaringan komputer saja, akan tetapi juga termasuk perangkat audio, Video bahkan telepon selular.

b) Menurut (Casey, 2011)

   Bukti digital adalah semua data yang dapat menampilkan atau menujukkan bahwa tindak kriminal terjadi atau dapat memberi atau menghubungkan antara kriminalitas dan korbannya, atau tindak kriminal dan pelakunya.

c) Menurut (Marshall, 2005)

   Bukti digital adalah setiap dan semua data digital yang dapat membuktikan bahwa itu adalah sebuah kejahatan yang telah dilakukan atau data digital yang menghubungkan antara kejahatan dengan korban ataukejahatan dengan pelakunya.

d) Menurut (Casey, 2011)

Bukti Digital umumnya merupakan abstraksi dari beberapa objek digital atau kejadian. ketika seseorang mengoperasikan komputer untuk melakukan berbagai hal seperti mengirim emmail, atau kegiatan lainnya maka kegiatan itu akan menghasilkan jejak-jjejak data yang dapat memberikan sebagian gambaran dari kejadian yang sudah terjadi sebelumnya.

2.3 Investigasi Forensik Digital

Komputer forensik adalah identifikasi, memelihara, menganalisis, dan menggunakan bukti digital secara sah berlaku. Ruang lingkup forensik komputer adalah suatu kegiatan berkaitan dengan pemeliharaan, identifikasi, pengambilan, menyaring dan merekam bukti komputer

dalam kejahatan komputer. Dari proses ini, analisis dan investigasi dapat dilakukan untuk kemungkinan untuk menentukan bukti hukum. Data yang tersedia dan diambil dari sumber daya komputer, termasuk yang ada di sistem, komputer, jaringan komputer, jalur komunikasi, media penyimpanan, aplikasi komputer dan lain-lain. data bisa terapkan prosedurnya agar dapat digunakan sebagai alat bukti yang sah dan legal.[4]

2.4 *Website*

Website adalah halaman informasi yang menampilkan teks, data gambar diam atau gerak, data animasi, suara, video atau gabungan dari semuanya baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan- jaringan halaman (hyperlink). Jaringan tersebut disediakan melalui jalur internet sehingga bisa di akses oleh pengguna internet di seluruh dunia. (Hakim,2015). HTTP dan HTTPS adalah sebuah protokol untuk meminta atau menjawab antara client dan server, client HTTP meminta dengan membuat hubungan TCP/IP ke port 80 sedangkan HTTPS meminta dengan membuat hubungan Secure Socket Layer (SSL) atau Transport Layer Security (TLS) ke port 443. Perbedaaan HTTP dan HTTPS terdapat pada tingkat keamananya, pada protokol HTTP data yang dikirim ke server memiliki informasi kode yang menjelaskan dari permintaan data tersebut, setelah menerima kode, server akan menjawab atau mengirim kembali kode jawaban dari data tersebut, sedangkan protokol HTTPS data yang dikirim ke server akan terenkripsi disertai kunci publik, server bisa membaca permintaan data yang dienkripsi dan mendekripsi data dengan kunci publik. HTTPS di enkripsi dan dekripsi dari data yang diminta oleh pengguna dan data dikembalikan oleh server.(Zanbar,2015)

2.5 *Content Management System (CMS)*

CMS adalah sebuah sistem yang memberikan kemudahan kepada para penggunanya dalam mengelola dan mengadakan perubahan isi sebuah website dinamis tanpa sebelumnya dibekali pengetahuan tentang hal&hal yang bersifat teknis, dengan berbagai keuntungan yang dimiliki CMS. Conten Manajemen Syatem (CMS) merupakan aplikasi berbasis web yang memiliki sistem sedemikian sehingga memberi kemudahan kepada para pengguna sekaligus juga pengelolanya. Pemisahan antara isi dan desain turut menjaga konsistensi tampilan yang mempermudah penggunaan kembali berbagai informasi yang ada dalam

[4] https://accounting.binus.ac.id/2020/07/20/komputer-forensik/

server. Fitur&fitur yang terdapat dalam CMS juga sangat bervariasi, mulai dari manajemen layout situs (yang berfungsi untuk mengubah layout situs),fitur pencarian, editing berita, foto, editing produk dan lain sebagainya.

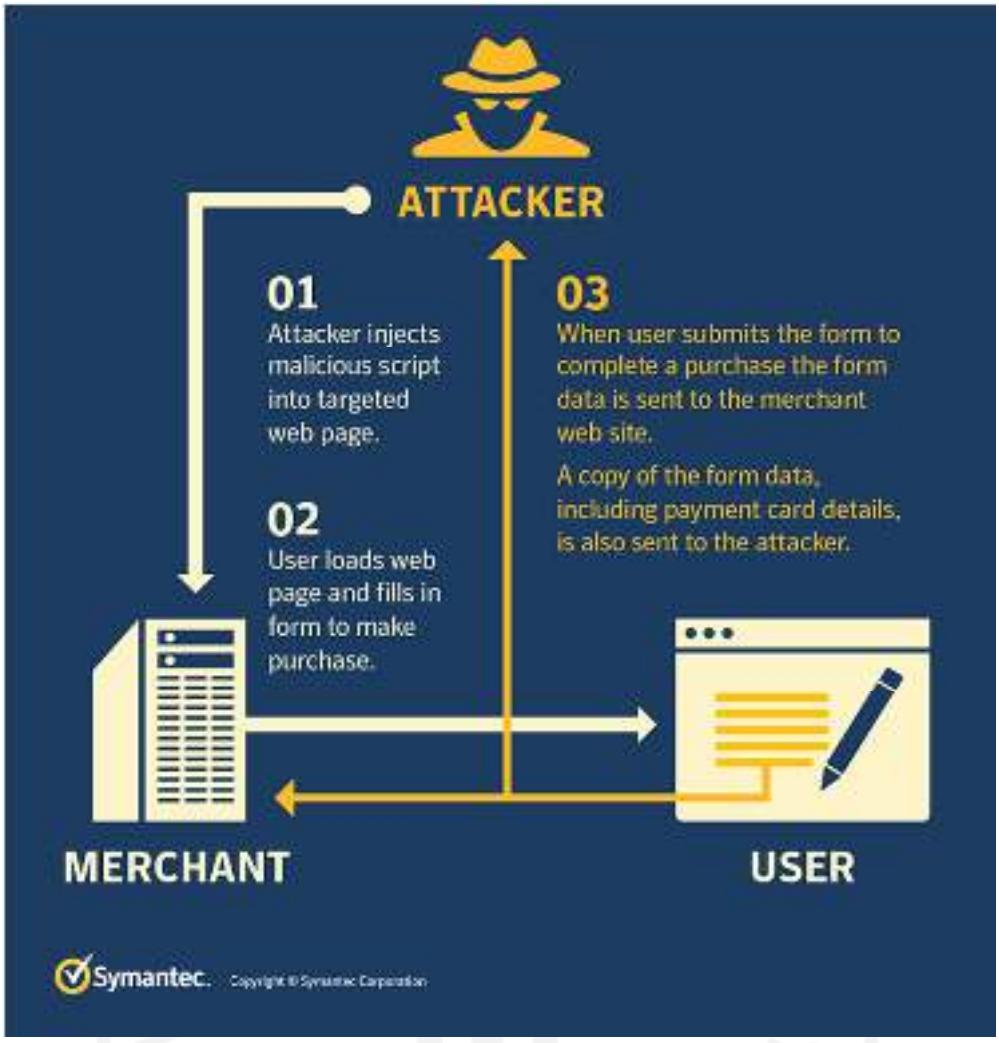
2.6 *E-Commerce*

E-commerce merupakan perkembangan terbaru dalam upaya mempengaruhi pelanggan dengan mempermudah hidup mereka dalam melakukan transaksi jual beli (Travis, 2004). Keuntungan menggunakan e-commerce adalah memungkinkan organisasi untuk mempromosikan pertumbuhan ekonomi, meminimalkan hambatan di pasar, meningkatkan efisiensi dan efektivitas, dan mengurangi biaya pemasaran produk mereka. Manfaat bagi konsumen adalah kemudahan dalam memilih produk, memperoleh lebih banyak pilihan produk dan jasa, serta tidak membuang waktu terlalu lama. Transaksi jual beli online dapat berjalan dengan baik jika didukung oleh kepercayaan konsumen terhadap jaringan e-commerce, karena kepercayaan sangat penting untuk keberhasilan interaksi antara pemasok dan konsumen. Karena banyak keuntungan yang didapatkan oleh pelaku usaha dengan mencoba membutka website e-commerce (Purbasari, 2017).

2.7 *Formjacking*

Formjacking aktifitas baru penggunaan kode JavaScript berbahaya untuk mencuri detail kartu kredit dan informasi lainnya dari formulir pembayaran di halaman web checkout situs e-commerce. Formjacking adalah nama yang diberikan oleh Symatec untuk memberi label serangan cyber yang sering disebut dengan web skimming[5]. Serangan ini merupakan varian dari skimming kartu kredit fisik dimana pencuri yang membaca data kartu kredit yang berada di ATM umum contohnya di POM bensin. Dalam perbuatan pencurian data dengan teknik ini pelaku melakukan metode berbeda, melalui akses website dan menginfeksi website dengan kode javascript berbahaya. Alur yang dilakukan seperti ini, ketika pengunjung situs memasukkan informasi kartu pembayaran mereka dan mengirimkan, kode berbahaya itu mengumpulkan nomor kartu pembayaran - serta informasi lain seperti nama pelanggan, alamat, dan nomor telepon. Kode kemudian mengirimkan informasi ini ke lokasi lain yang dipilih penyerang. Berikut adalah cara kerja sederhana dalam melakukan formjacking.

[5] https://www.symantec.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time diakses pada 1 Desember 2019



Gambar 2.2 Cara kerja Formjacking[6]

2.8 *Live Forensik*

Menurut (Rafique & Khan, 2013) Ada dua metode forensik digital, yaitu forensik real-time dan forensik statis. Forensik real-time adalah proses forensik yang dilakukan dengan mengumpulkan data yang mudah menguap (mudah hilang) dan menganalisis informasi bukti digital saat sistem sedang berjalan (on). Forensik real-time dirancang untuk menganalisis bukti tanpa mempengaruhi fungsionalitas sistem, memungkinkan seluruh fungsi yang dilakukan oleh sistem tidak terganggu selama proses analisis digital. Forensik statis menggunakan metode tradisional, yaitu, bukti elektronik diproses menjadi gambar bit demi bit untuk pemrosesan forensik. Proses forensik itu sendiri berjalan pada sistem yang tidak berjalan (shutdown). Secara tradisional, forensik statis digunakan untuk menyelidiki hasil

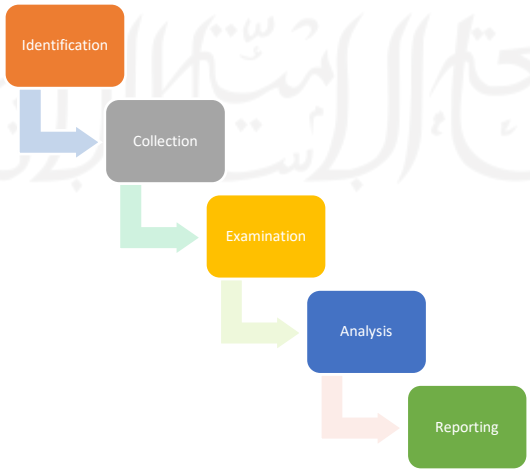
[6] https://www.symantec.com/blogs/threat-intelligence/formjacking-attacks-retailers diakses pada 1 Desember 2019

pencitraan dan menganalisis konten bukti digital, seperti file yang dihapus, riwayat browser web, fragmentasi file, koneksi jaringan, file yang diakses, riwayat login pengguna. Teknik live forensics telah berkembang dalam dasawarsa terakhir, seperti analisis konten memory untuk mendapatkan gambaran dan informasi yang lebih baik mengenai proses aplikasi yang sedang berjalan (Rahman & Khan, 2015). Teknik live forensics juga diterapkan pada Random Access Memory (RAM). Metode live forensic bertujuan agar penanganan investigasi lebih cepat, integritas data lebih terjamin, teknik enkripsi lebih memungkinkan bisa dibaca dan kapasitas memori yang lebih minim apabila dibandingkan dengan teknik forensik tradisional (Yudhistira, 2018). Data pada RAM bersifat data volatile (data sementara) jika komputer mati maka data itu akan hilang. Data volatile ini berisi data penting seperti username dan password dalam suatu akun seperti email (Faiz et al., 2016).

Kemudian menurut (Adelstein, 2006) teknik live forensics bisa dilakuan dengan cara mengumpulkan data ketika sistem yang terkena serangan dan sistem masih berjalan (running). Bukti digital forensik yang dikumpulkan melalui sistem yang berjalan tersebut dapat memberikan bukti yang tidak dapat diperoleh dari forensik konvensional (static disk image). Bukti digital yang dikumpulkan tersebut merupakan data yang bisa berubah-ubah dari sistem yang dinamis dan tidak mungkin untuk diproduksi ulang pada waktu berikutnya.

2.9 *National Institute Of Justice (NIJ)*

Penggunaan metode penelitian ini diadaptasi dari Metode Analisis Forensik National Institute of Justice (NIJ). Metode digunakan untuk menjelaskan bagaimana berbagai tahapan penelitian dilakukan agar proses penelitian dapat diselesaikan secara sistematis dan dapat digunakan sebagai pedoman untuk memecahkan masalah yang ada.



Gambar 2.3 Tahapan National Institute of Justice (NIJ)

Tahap metodologi National Institute of Justice (NIJ) dibagi menjadi lima tahap, yaitu identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan yang dapat dijelaskan sebagai berikut:

1. Identifikasi : yaitu mengidentifikasi dan menyiapkan skenario penelitian dan menyiapkan alat forensik yang akan digunakan dalam proses penelitian ini.
2. Akuisisi : yaitu penggunaan alat FTK Imager untuk menangkap data dari proses akuisisi yang berfungsi sebagai 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.

2.10 FTK Imager

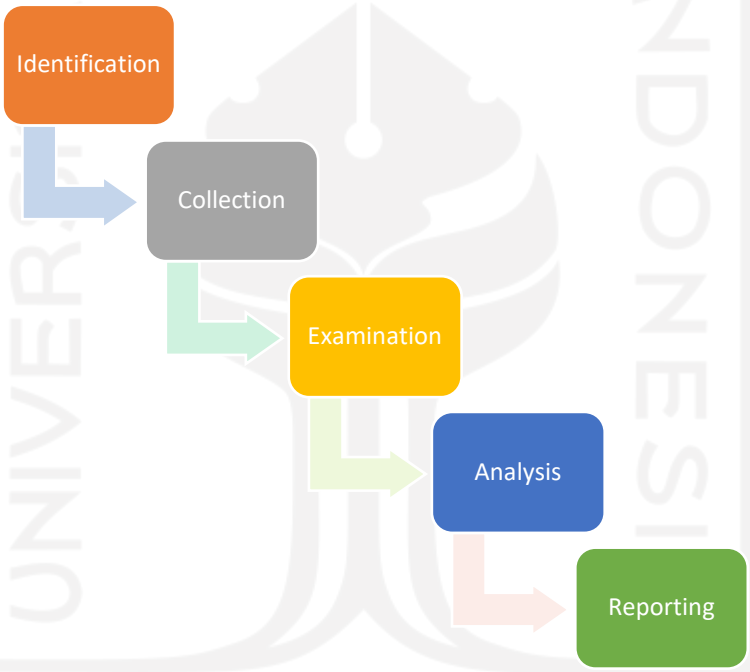
FTK Toll kit adalah alat forensik yang dapat membantu melakukan pengujian forensik yang baik pada Windows. FTK menyediakan penyaringan file dan kemampuan pencarian serta analisis email. Untuk memastikan file yang digunakan untuk pekerjaan tidak berubah, penyidik dapat membandingkan hash dari file asli dengan file gambar. Hash ini akan memberikan validitas matematis, sehingga citra forensik harus sesuai dengan aslinya. Perangkat lunak AccessData dapat mencari ribuan file untuk menemukan bukti yang Anda inginkan dengan cepat. Sebuah fungsi yang cocok untuk konsultan keamanan untuk menyelesaikan pemeriksaan forensik komputer. FTK juga dapat membaca berbagai format data bukti digital, termasuk yang dibuat oleh EnCase (Rosita, 2018).

Toolkit Forensik hanya menganalisis sistem Windows, jadi jika Anda menyelidiki sistem Unix atau Linux, Anda akan memerlukan alat lain seperti EnCase atau The Coroner's Toolkit. Setelah pustaka KFF terinstal dan Anda berada di direktori program FTK, Anda dapat memulai penyelidikan dengan memilih Opsi Kasus yang biasanya akan mengaktifkan pencarian KFF atau pengindeksan teks lengkap. Dua hal ini akan sangat memudahkan penyidikan. FTK dilengkapi dengan dtSearch, mesin pencari yang memungkinkan penyidik mencari informasi secara langsung dalam bentuk teks. Langkah-langkah investigasi (peristiwa) secara otomatis dicatat dalam log, yang menyederhanakan produksi catatan percobaan untuk pekerjaan investigasi

BAB 3
Metodologi Penelitian

3.1 Metodologi Yang Diusulkan

Pada bab ini akan menjelaskan metode yang akan digunakan untuk investigasi Formjacking pada website ecommerce. Dalam bab ini juga menjelaskan bagaimana cara penelitian yang dilakukan sehingga dapat diketahui rincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Adapun langkah sebagai berikut pada Gambar 3.1.



Gambar 3.1 Alur Metode Penelitian(metode Live Forensik NIJ)

Gambar 3.1 menjelaskan bahwa sebuah langkah kerja forensik yang digunakan untuk menjabarkan tahapan-tahapan dan langkah-langkah penelitian yang akan dilakukan tanpa mengurangi proses yang telah di kemukakan oleh metode NIJ. Dengan kata lain, langkah kerja forensik pada penelitian ini mengacu pada 4 tahap standar metode forensik dari NIJ

3.2 Identifikasi Masalah dan Study Literatur

Pada tahapan ini dilakukan identifikasi masalah yang ada. Masalah yang diambil dalam penelitian ini adalah tentang pencurian data kartu kredit pada form checkout website ecommerce atau dikenal dengan formjacking. Identifikasi dilakukan berdasarkan banyaknya

kasus percurian data kartu kredit. Permasalahan yang ada tepat diangkat untuk menjadi objek penelitian. Selanjutnya dilakukan studi literatur dilakukan penulis untuk mengumpulkan bahan-bahan referensi yang terkait dengan penelitian, baik melalui buku, artikel, paper, jurnal, makalah, mengunjungi beberapa situs yang terdapat pada internet terkait dengan digital forensik, live forensic, pengumpulan data dengan FTK Imager, dan Digital Forensics Investigation Model sehingga dapat menunjukan tujuan akhir penelitian.

3.3 Skenario Kasus

Dalam penelitian ini menggunakan skenario kasus untuk dapat menjelaskan langkah-langkah dalam melakukan penelitian ini. Penelitian ini menggunakan cms ecoomerce woocomerce dari wordpress yang sudah dimasukan kode sample formjacking terletak di server. Pada skenario kasus gambar 3.2 User mengakses laman website ecommerce dengan web browser diantaranya Microsoft Edge, Opera, FireFox dan Google Crome dengan menggunakan detail kartu yang berbeda untuk melakukan checkout. Setelah melakukan pemilihan barang user akan dibawa dilaman checkout dimana dilaman tersebut user diminta memasukan informasi alamat pengiriman dan method pembayaran dengan kartu kredit. Setelah berhasil melakukan pengisian dan klik tombol checkout akan muncul pesan notifikasi konfirmasi pada laman checkout klik ok maka orderan telah berhasil dilakukan. Kemudian user akan melakukan akuisisi data aktifitas di web browser yang digunakan dengan menggunakan FTK Imager. Setelah data berhasil di akusisi, maka user akan melakukan analisis hasil dari akuisisi data tersebut.

Gambar 3.2 Alur Skenario Kasus

3.4 Persiapan Tools

Persiapan alat yang digunakan yaitu berupa perangkat hardware dan software, desain 24cenario kasus dan bukti yang diperoleh, serta pengimplementasian investigasi 24cenario

digital atas kasus dan bukti yang diperoleh dari 25cenario kasus dimaksud. Hardware dan software yang digunakan dalam penelitian ini sebagaimana table berikut:

Table 3.1 Persiapan Spesifikasi Tools yang digunakan

No	Hardware / Software	Keterangan
1	Laptop GL503GE, Core i7 8th SSD 512GB SSHD 1TB	Hardware
2	HDD 3.0 2TB WDBlue Ext	
3	Sistem Operasi Windows 10 Pro 64Bit	Sistem Operasi
4	AccessData FTK Imager Versi 4.5.0.3	Tools Forensik
5	Opera Browser Versi 74.0.3911.160	Web Browser
6	Microsoft Edge Versi 91.0.864.48	Web Browser
7	Mozilla Firefox Versi 89.0	Web Browser
8	Google Crome Versi 91.0.4472.101	Web Browser
9	CMS WooCommerce	Aplikasi Web CMS

Persiapan sistem merupakan tahapan menyediakan kebutuhan software dan hardware untuk menjalankan proses skenario sampai dengan proses selesai. Dimana kebutuhan perangkat sudah tertera pada tabel diatas.

3.5 Analisa Investigasi Forensik

Menurut Muh Al Azhar forensik adalah suatu proses ilmiah atau suatu usaha ilmiah yang didasari ilmu pengetahuan dalam memngumpulkan, menganalisa dan menghadirkan bukti dalam suatupersidangan di pengadilan untuk membantu pengungkapan suatu kejahatan melalui pengungkapa bukti-bukti yang sah menurut undang-undang dan peraturan yang berlaku. Digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (pro justice), yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau computer crime secara ilmiah (scientific) sehingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut. Disinilah tugas untuk para investigator dalam menangani kasus penyelidikan untuk dapat merecover ulang ejadian peristiwa tindak kriminal.

Berdasarkan metode penelitian pada Gambar 3.1 dibuatlah sebuah langkah kerja forensik yang digunakan untuk menjabarkan tahapan-tahapan dan langkah-langkah

penelitian yang akan dilakukan tanpa mengurangi proses yang telah di kemukakan oleh metode NIJ. Dengan kata lain, langkah kerja forensik pada penelitian ini mengacu pada 4 tahap standar metode forensik dari NIJ untuk melakukan proses investigasi sebagai berikut:

3.5.1 Collection

Pada tahap ini dilakukan pengumpulan data dan barang bukti terkait dengan aktifitas formjacking berupa leptop yang digunakan user mengakses website ecommerce. Proses ini dilakukan secara live forensik dimana leptop masih dalam kondisi menyala. Aktifitas meliputi identifikasi, pengumpulan, pengambalian dan perekaman barang bukti. Tahapan penelitian ini proses awal melakukan capturing paket data pada website menggunakan tools forensics FTK Imager, proses collection data pada RAM leptop dilakukan akuisisi dan disimpan untuk menghindari terjadinya perubahan atau hilangnya barang bukti

3.5.2 Examination

Proses pemeriksaan barang bukti untuk yang dikumpulkan menggunakan skenario. Proses pengujian barang bukti menggunakan tool FTK dengan menu Disk Image untuk mendapatkan informasi dari file hash sama dengan nilai file hash pada file capture.

3.5.3 Analysis

Proses analisis yang dilakukan investigator pada barang bukti dari hasil pengumpulan data dan akuisisi pada tahap sebelumnya untuk memperoleh barang bukti yang terkait dengan kasus tersebut. Pemeriksaan meliputi bukti IP Server yang digunakan oleh pelaku, data kartu kredit, nomer, nama korban dan cvv.

3.5.4 Reporting

Proses pelaporan hasil investigasi dan data yang didapatkan dari penyelidikan. Laporan berisi tentang hasil identifikasi capture data dari barang bukti URL phishing. Laporan hasil analisis meliputi gambaran yang perlu dilakukan terkait kasus tersebut.

3.6 Hasil Penelitian / Report

Table 3.2 Laporan Analisis Data

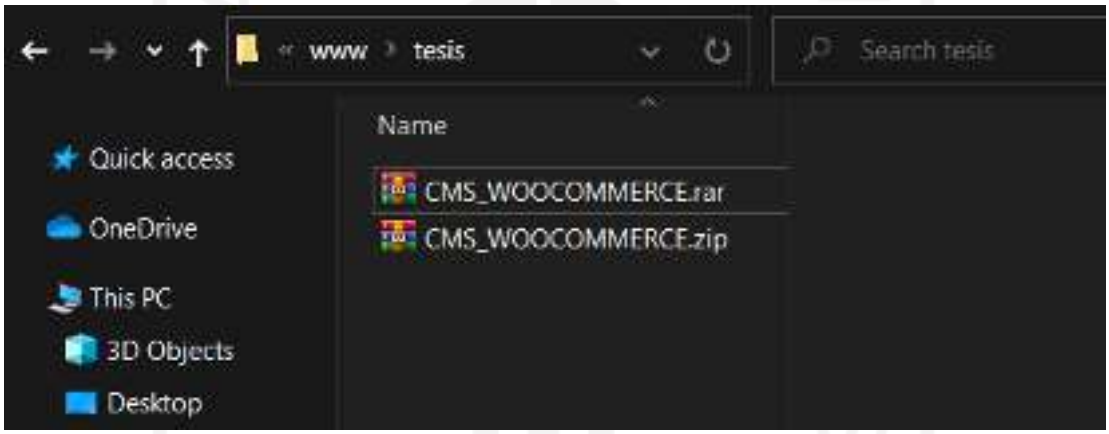
No	Artefak BB	Internet Protocol	Hasil Capture RAM	Tools FTK Forensik				Keterangan
				Crome	Mozilla	Edge	Opera	
	Md5							
	SHA1							
	Nomer Kartu Kredit							
	IP Server							
	Data							

Merupakan tahap pembuatan laporan dan hasil pembuktian identifikasi serangan formjacking untuk pengujian mendeteksi penyusupan serta dapat mendapatkan informasi mengenai penyerang berdasarkan Tabel 3.2.

BAB 4
Hasil Dan Pembahasan

4.1 Akusisi Bukti Digital (Collection)

Collection merupakan tahap paling awal dalam metode NIJ, tahap ini adalah tindakan untuk pengamanan barang bukti. Pada tahapan ini dilakukan proses untuk mengamankan barang bukti *webiste CMS ecommerce* yang berapada pada server xampp. Proses backup dilakukan pada asset website yang terindikasi adanya kode jahat *formjacking.* File backup dibuat dalam beberapa jenis *extention* seperti, zip, rar dan beberapa jenis *extention* yang lain sehingga dapat dibuka dalam beberapa tools forensik.

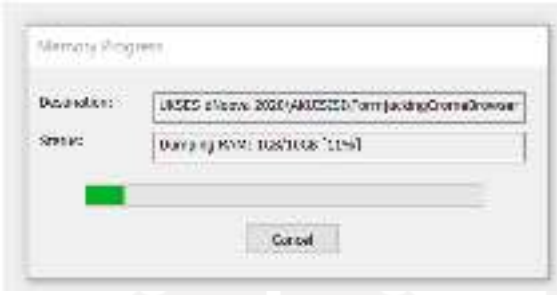


Gambar 4.1 Hasil dari backup asset ecommerce

Proses collection menggunakan simulasi yang telah disusun oleh peneliti diman skenario tersbut mengacu pada kondisi real untuk mendapatkan pengalaman olah tkp yang sesuai dengan kejadian kejahatan formjacking. Pada skema gambar 4.2 dilakukan simulasi menggunakan akses empat browser untuk mengakses website.

Gambar 4.2 Skenario Olah TKP

Pada saat yang bersamaan Tool FTK Imager dijalankan untuk mengumpulkan data dari aktivitas yang dilakukan pada laman checkout website ecommerce. Memori RAM dilakukan proses capture ketika membukan browser dan mengakses laman checkout, dan akan dianalisis untuk mendapatkan proses yang berjalan di sistem. Proses ini dilakukan secara berurutan untuk menghindari proses ram yang tertupuk. Setelah proses satu browser selesai dilakukan restar leptop dan dimulai kembali tahapan untuk browser kedua sampai dengan selesai ke empat browser.



Gambar 4.3 Memory Progress

Hasil dari memory progress akuisisi yaitu file dengan ekstensi.mem yang dapat dilihat pada Gambar 4.3.

Gambar 4.4 Hasil Capture Memory

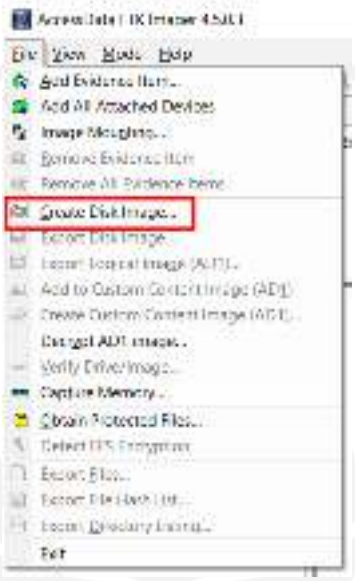
Dari hasil melakukan collection atau akuisisi pada RAM leptop yang mengakses website e-commerce dengan menggunakan 4 browser hasilnya sebagai berikut:

Table 4.1 Hasil Akuisisi RAM Browser

NO	Browser	Nama File	Extension	Size	Keterangan
1	Opera Browser Versi 74.0.3911.160	FormjackingOPERA	.mem	10 GB	
2	Microsoft Edge Versi 91.0.864.48	FormjackingEDGE	.mem	12 GB	
3	Mozilla Firefox Versi 89.0	FormjackingFirefox	.mem	11 GB	
4	Google Crome Versi 91.0.4472.101	FormjackingCrome	.mem	12 GB	

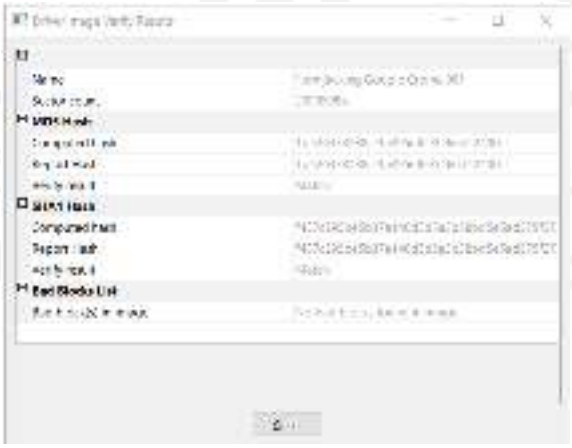
4.2 Examinasi Bukti Digital (Examination)

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 masing-masing file. Proses ini diperlukan untuk melakukan verifikasi pada data barang bukti apakah mengalami perubahan atau tidak. Untuk pengecekan nilai hash maka pada FTK Imager dipilih menu File-pilih Create disk image seperti pada gambar 4.5.



Gambar 4.5 Create Disk Image

Hasil dari disk image akan didapatkan informasi MD5 Hash dan Sha1 Hash. Nilai ini menunjukan bahwa pada barang bukti yang telah di akuisisi tidak mengalami perubahan dan dengan ini dapat menunjukan keaslian file. Verifikasi ini juga dilakukan saat pengujian tidak ada perubahan pada masing-masing barang bukti.



Gambar 4.6 Hash File Fromjacking google crome

Pada gambar 4.6 adalah hasil dari create disk image nilai hash yang menujukan keaslian file bukti digital, terlihat pada kolom Computed hash dan Report Hash sama, sehingga file masih sama dan tidak termodifikasi. Pada hasil verifikasi data nilai hash untuk browser google crome diatas adalah 1d2463758cf1a395ef0e5466d420b Md5 dan

f457c295be5b37a140d5d5a3b38bd5e5ad579f27 SHA1. Proses ini dilakukan untuk barang butkti dengan cara dan tahapan yang sama sehingga menemukan hasil nilai MD5 dan SHA1 sebagai berikut ;

Table 4.2 Nilai Computed Hash

[illegible]	MD5	SHA1
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

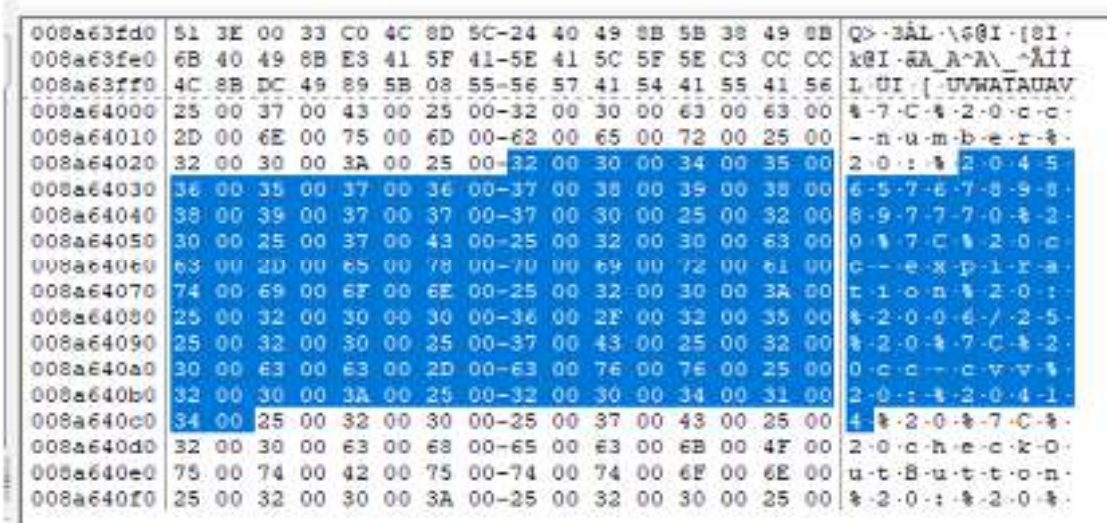
Pada tabel 4.2 yang menunjukan hasil rekap dari nilai Hash pada browser Microsoft Edge, Opera, Firefox dan Crome yang terverifikasi nilai Computed hash dan Report hash memiliki nilai hash yang sama.

4.3 Analisis Bukti Digital (Analysis)

Proses analisis yang dilakukan investigator pada barang bukti dari hasil pengumpulan data dan akuisisi pada tahap sebelumnya untuk memperoleh barang bukti yang terkait dengan kasus formjacking tersebut. Pada tahap analisis ini dilakukan proses melihat dan melalukan crosscheck pada hasil akuisisi file dengan extension .mem dengan tahapan sebagai berikut;

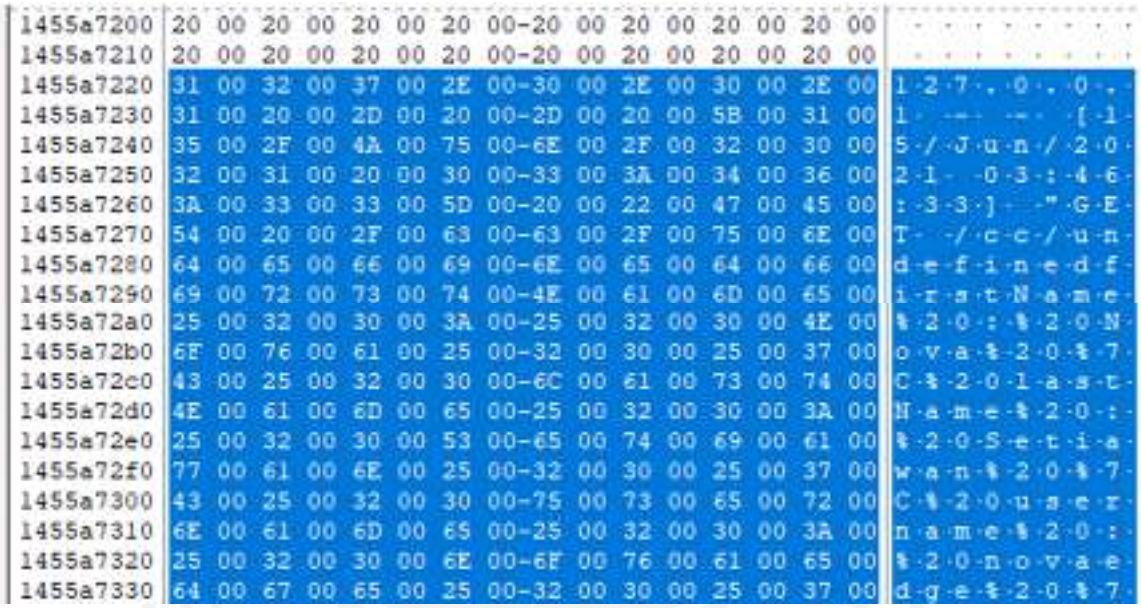
4.3.1 Analisis Microsoft Edge

Setelah dilakukan proses analisis capture memory pada leptop yang maka didapatkan file FormjackingEdgeBrowser.mem. Analisis yang dilakukan untuk mendapatkan hasil sebagai berikut.



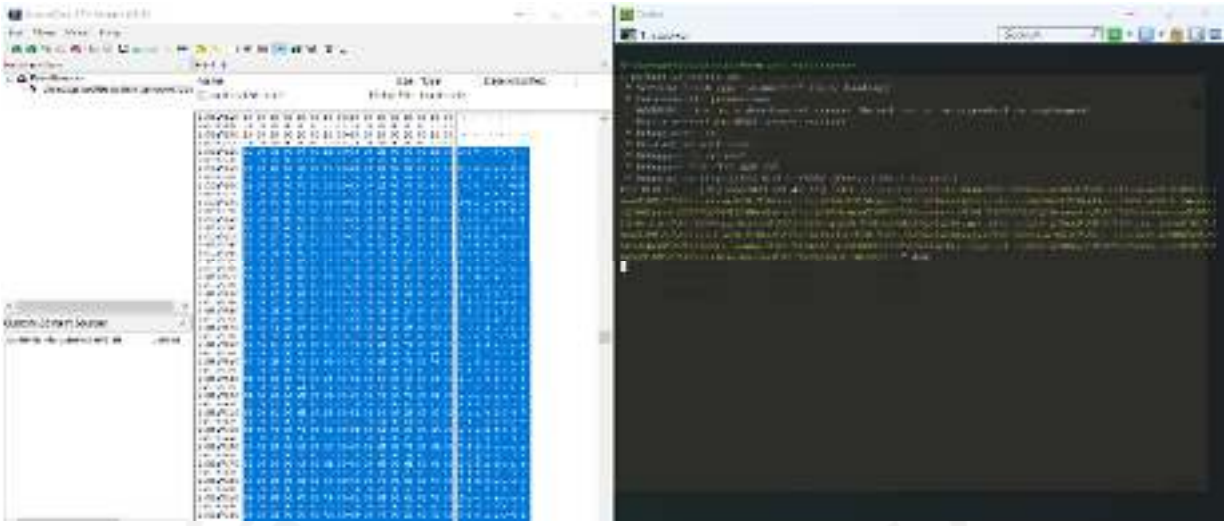
Gambar 4.7 Nomer Kartu Kredit

Pada gambar 4.7 di offset 008a64030 sampai dengan offset 008a640e0, terlihat detail nomer kartu kredit yang digunakan oleh user yang dapat dilihat pada kolom paling kanan. Nomer kartu tersebut tertera dan tercapture oleh FTK Imager telah digunakan untuk bertransaksi pada website.



Gambar 4.8 Mengirimkan data ke server

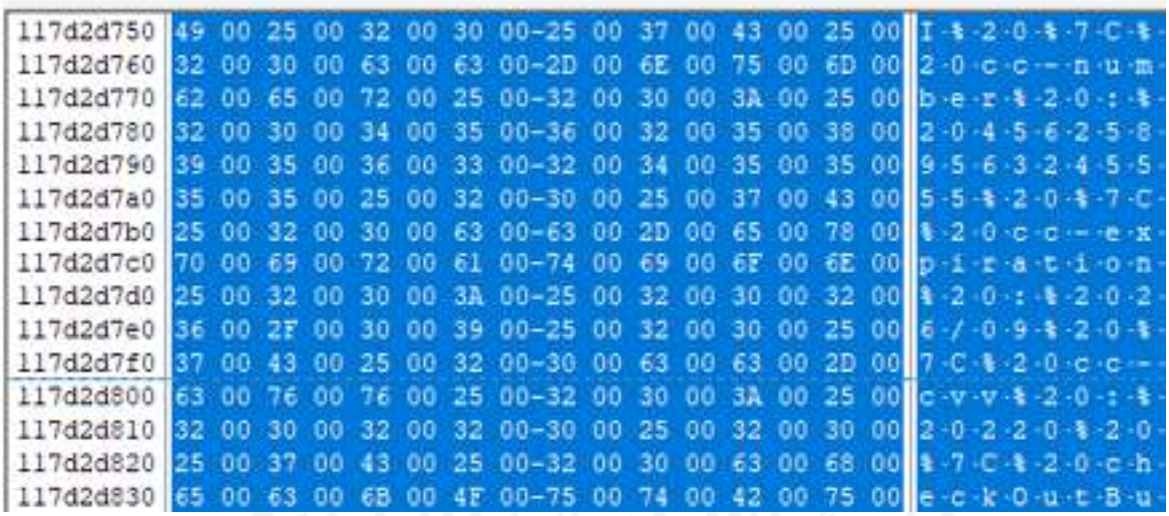
Gambar 4.8 offset 1455a7220 sampai dengan 145517330 menunjukan paket pengiriman detail berupa nomor kartu kredit yang telah digunakan untuk bertransaksi dan klik tombol checkout pada form pembelian di website. Perintah pengiriman copy data nomer kartu di kirimkan ke ip 127.0.0.1 pada tanggal 15 Juni 2021 pukul 03:46:33 UTC. Sehingga dari case ini dapat diketahui aktifitas pada formjacking menjalankan perintah mengirmkan data ke alamat server seperti pada gambar 4.9



Gambar 4.9 Data kartu dikirim ke server

4.3.2 Analisis Opera

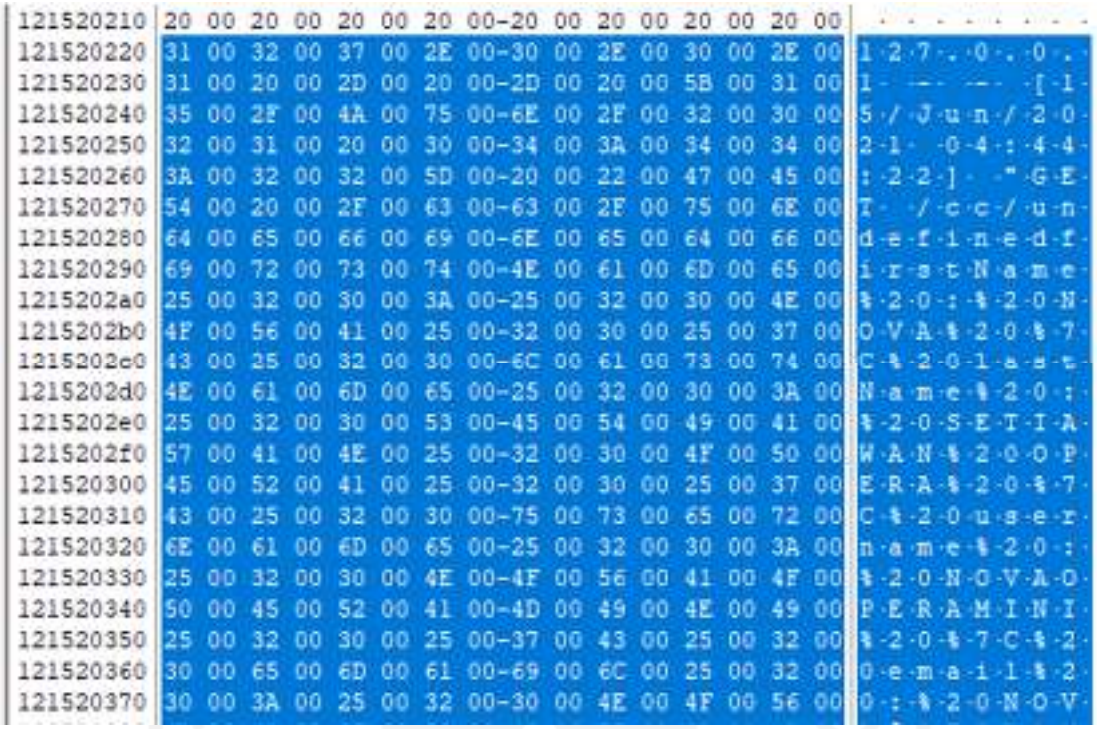
Proses analisis capture memory pada leptop yang maka didapatkan file FormjackingOPERA.mem. Analisis yang dilakukan untuk mendapatkan hasil sebagai berikut.



117d2d750	49 00 25 00 32 00 30 00-25 00 37 00 43 00 25 00	I·%·2·0·%·7·C·%
117d2d760	32 00 30 00 63 00 63 00-2D 00 6E 00 75 00 6D 00	2·0·c·c·-·n·u·m
117d2d770	62 00 65 00 72 00 25 00-32 00 30 00 3A 00 25 00	b·e·r·%·2·0·:·%
117d2d780	32 00 30 00 34 00 35 00-36 00 32 00 35 00 38 00	2·0·4·5·6·2·5·8
117d2d790	39 00 35 00 36 00 33 00-32 00 34 00 35 00 35 00	9·5·6·3·2·4·5·5
117d2d7a0	35 00 35 00 25 00 32 00-30 00 25 00 37 00 43 00	5·5·%·2·0·%·7·C
117d2d7b0	25 00 32 00 30 00 63 00-63 00 2D 00 65 00 78 00	%·2·0·c·c·-·e·x
117d2d7c0	70 00 69 00 72 00 61 00-74 00 69 00 6F 00 6E 00	p·i·r·a·t·i·o·n
117d2d7d0	25 00 32 00 30 00 3A 00-25 00 32 00 30 00 32 00	%·2·0·:·%·2·0·2
117d2d7e0	36 00 2F 00 30 00 39 00-25 00 32 00 30 00 25 00	6·/·0·9·%·2·0·%
117d2d7f0	37 00 43 00 25 00 32 00-30 00 63 00 63 00 2D 00	7·C·%·2·0·c·c·-
117d2d800	63 00 76 00 76 00 25 00-32 00 30 00 3A 00 25 00	c·v·v·%·2·0·:·%
117d2d810	32 00 30 00 32 00 32 00-30 00 25 00 32 00 30 00	2·0·2·2·0·%·2·0
117d2d820	25 00 37 00 43 00 25 00-32 00 30 00 63 00 68 00	%·7·C·%·2·0·c·h
117d2d830	65 00 63 00 6B 00 4F 00-75 00 74 00 42 00 75 00	e·c·k·O·u·t·B·u

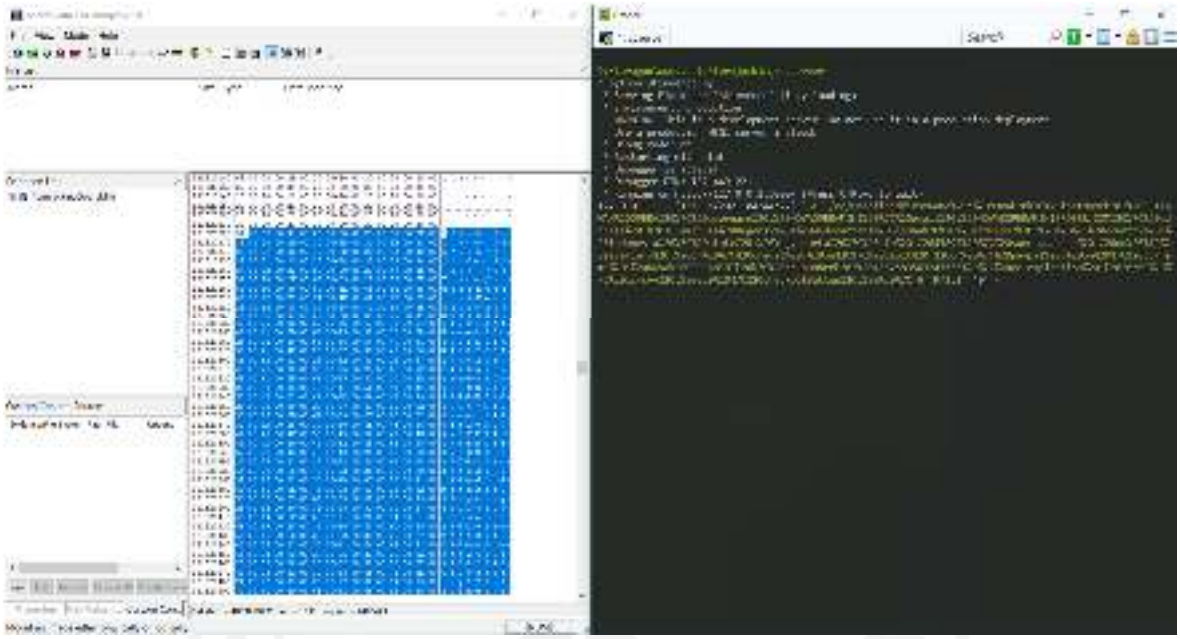
Gambar 4.10 Data Kartu Kredit Opera Browser

Pada gambar 4.10 di offset 117d2d750 sampai dengan offset 117d2d7f0, terlihat detail nomer kartu kredit yang digunakan oleh user yang dapat dilihat pada kolom paling kanan. Terdapat juga untuk nomer CVV tertera pada offset 117d2df0. Nomer kartu tersebut tertera dan tercapture oleh FTK Imager telah digunakan untuk bertransaksi pada website.



Gambar 4.11 Detail Server Opera Browser

Gambar 4.11 offset 121520210 sampai dengan 121520370 menunjukan paket pengiriman detail berupa nomor kartu kredit yang telah digunakan untuk bertransaksi dan klik tombol checkout pada form pembelian di website. Perintah pengiriman [GET] data nomer kartu di kirimkan ke ip 127.0.0.1 pada tanggal 15 Juni 2021 pukul 04:44:22 UTC. Tertera Nama pemegang kartu NOVA last name SETIAWAN dengan browser diketahui NOVAOPERAMINI.Sehingga dari case ini dapat diketahui aktifitas pada formjacking menjalankan perintah mengirmkan data ke alamat server seperti pada gambar 4.9Pada opera browser menunjukan hal yang sama yaitu dapat merecord proses pencurian data kartu kredit yang diguanakan user untuk melakukan pembelian. Sehingga dari case ini dapat diketahui aktifitas pada formjacking menjalankan perintah mengirmkan data ke alamat server seperti pada gambar 4.12



Gambar 4.12 Data kartu dikirim ke server dari Opera Browser

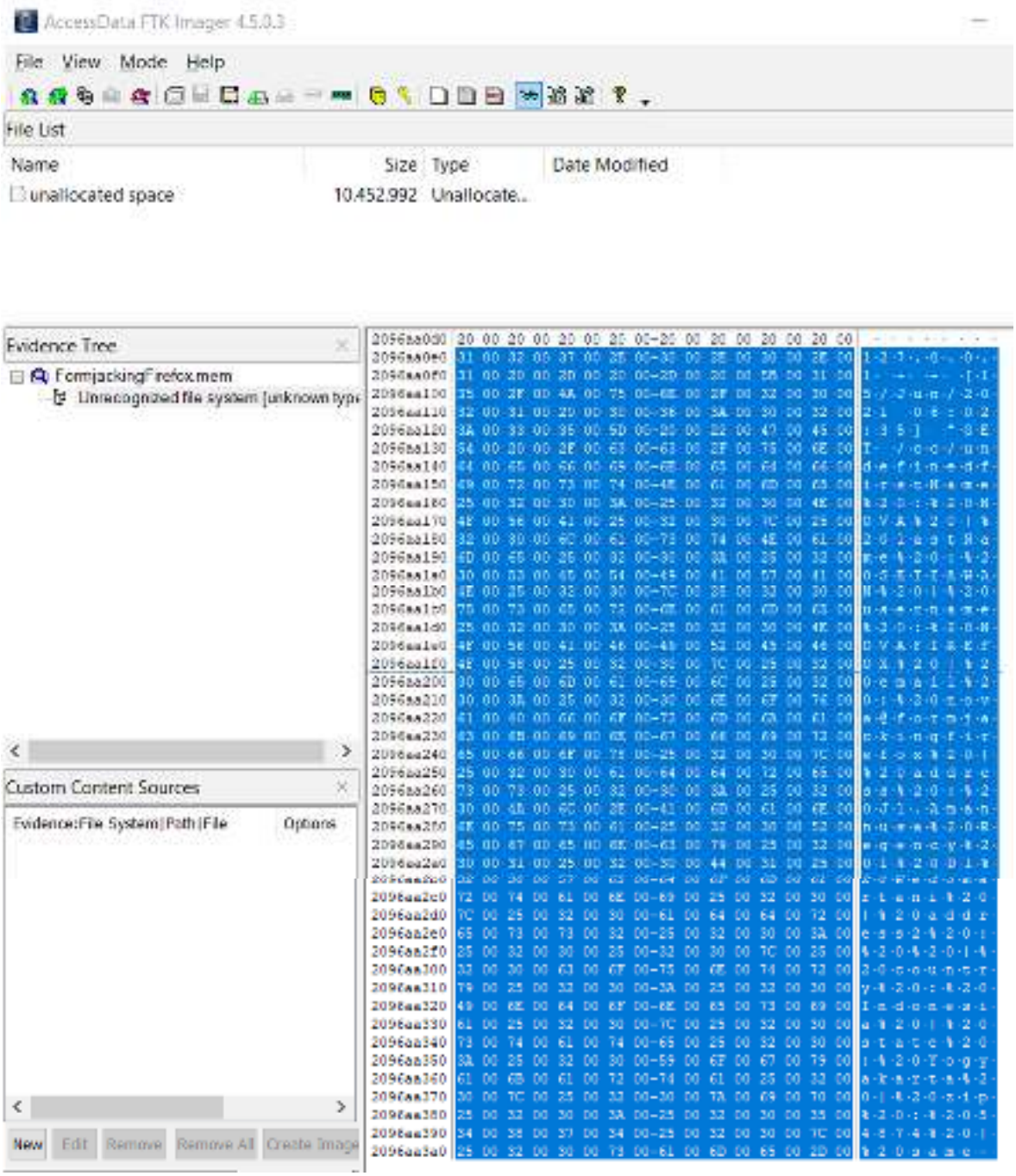
4.3.3 Analisis Mozila Firefox

Proses analisis capture memory pada leptop yang maka didapatkan file FormjackingFirefox.mem. Analisis yang dilakukan untuk mendapatkan hasil sebagai berikut.

2096aa480	6F 00 6E 00 25 00 32 00-30 00 7C 00 25 00 32 00	o·n·%·2·0·|·%·2·
2096aa490	30 00 63 00 63 00 2D 00-6E 00 61 00 6D 00 65 00	0·c·c·-·n·a·m·e·
2096aa4a0	25 00 32 00 30 00 3A 00-25 00 32 00 30 00 4E 00	%·2·0·:·%·2·0·N·
2096aa4b0	4F 00 56 00 41 00 25 00-32 00 30 00 53 00 45 00	O·V·A·%·2·0·S·E·
2096aa4c0	54 00 49 00 41 00 57 00-41 00 4E 00 25 00 32 00	T·I·A·W·A·N·%·2·
2096aa4d0	30 00 7C 00 25 00 32 00-30 00 63 00 63 00 2D 00	0·|·%·2·0·c·c·-·
2096aa4e0	6E 00 75 00 6D 00 62 00-65 00 72 00 25 00 32 00	n·u·m·b·e·r·%·2·
2096aa4f0	30 00 3A 00 25 00 32 00-30 00 37 00 37 00 37 00	0·:·%·2·0·7·7·7·
2096aa500	37 00 34 00 35 00 38 00-36 00 32 00 32 00 31 00	7·4·5·8·6·2·2·1·
2096aa510	32 00 33 00 33 00 33 00-33 00 25 00 32 00 30 00	2·3·3·3·3·%·2·0·
2096aa520	7C 00 25 00 32 00 30 00-63 00 63 00 2D 00 65 00	|·%·2·0·c·c·-·e·
2096aa530	78 00 70 00 69 00 72 00-61 00 74 00 69 00 6F 00	x·p·i·r·a·t·i·o·
2096aa540	6E 00 25 00 32 00 30 00-3A 00 25 00 32 00 30 00	n·%·2·0·:·%·2·0·
2096aa550	32 00 35 00 2F 00 31 00-32 00 25 00 32 00 30 00	2·5·/·1·2·%·2·0·
2096aa560	7C 00 25 00 32 00 30 00-63 00 63 00 2D 00 63 00	|·%·2·0·c·c·-·c·
2096aa570	76 00 76 00 25 00 32 00-30 00 3A 00 25 00 32 00	v·v·%·2·0·:·%·2·
2096aa580	30 00 30 00 30 00 38 00-25 00 32 00 30 00 7C 00	0·0·0·8·%·2·0·|·
2096aa590	25 00 32 00 30 00 63 00-68 00 65 00 63 00 6B 00	%·2·0·c·h·e·c·k·
2096aa5a0	4F 00 75 00 74 00 42 00-75 00 74 00 74 00 6F 00	O·u·t·B·u·t·t·o·
2096aa5b0	6E 00 25 00 32 00 30 00-3A 00 25 00 32 00 30 00	n·%·2·0·:·%·2·0·
2096aa5c0	25 00 32 00 30 00 7C 00-20 00 48 00 54 00 54 00	%·2·0·|· ·H·T·T·
2096aa5d0	50 00 2F 00 31 00 2E 00-31 00 22 00 20 00 34 00	P·/·1·.·1·"· ·4·

Gambar 4.13 Data firefox Browser

Pada gambar 4.13 di offset 2096aa490 sampai dengan offset 2096aa590, terlihat detail nomer kartu kredit yang digunakan oleh user yang dapat dilihat pada kolom paling kanan. Terdapat juga untuk nomer CVV tertera pada offset 2096aa580. Nomer kartu tersebut tertera dan tercapture oleh FTK Imager telah digunakan untuk bertransaksi pada website

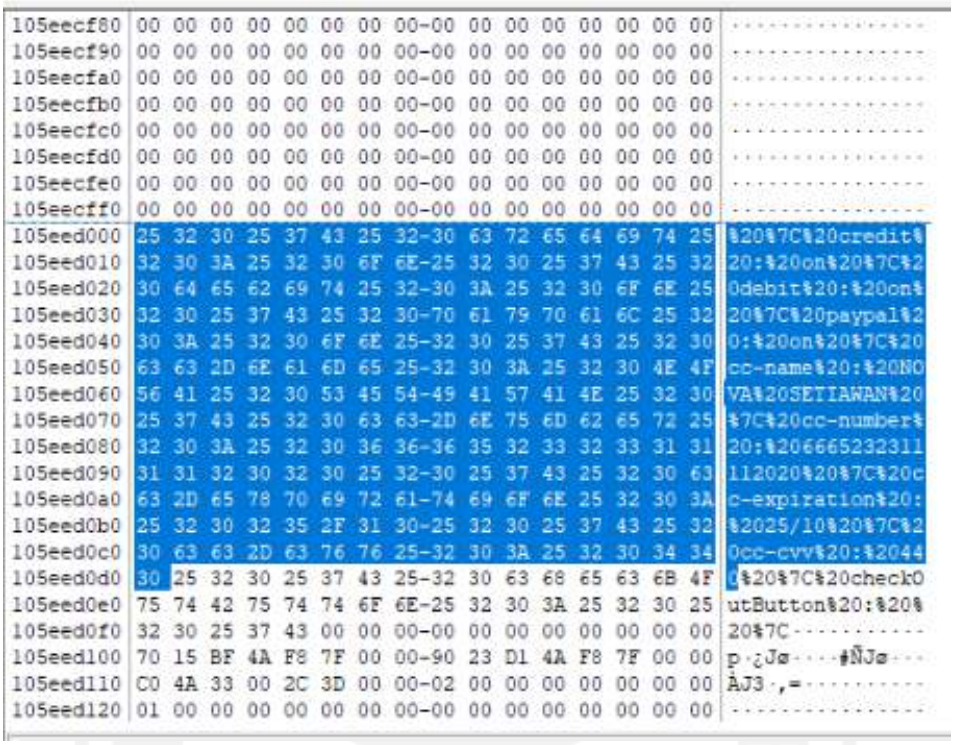


Gambar 4.14 GET Nomer Kartu Firefox Browser

Dari gambar 4.14 menunjukan bahwa mozilla firefox terdapat artefak pengiriman data kartu ke serve pelaku dengan perintah GET. Perintah pengiriman [GET] data nomer kartu di kirimkan ke ip 127.0.0.1 pada tanggal 15 Juni 2021 pukul 06:02:35 UTC.

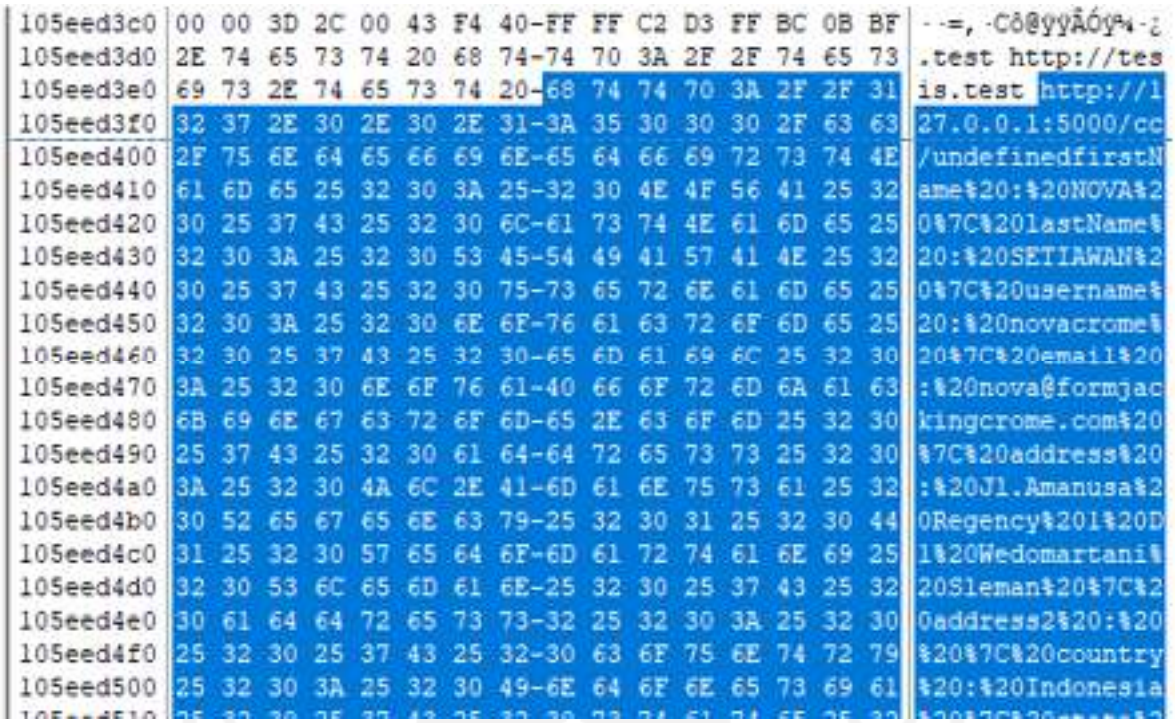
4.3.4 Analisis Google Crome

Proses analisis capture memory pada leptop yang maka didapatkan file FormjackingFirefox.mem. Analisis yang dilakukan untuk mendapatkan hasil sebagai berikut.



Gambar 4.15 Data Kartu Kredit Crome Browser

Pada gambar 4.15 di offset 105eed000 sampai dengan offset 105eed0d0, terlihat detail nomer kartu kredit yang digunakan oleh user yang dapat dilihat pada kolom paling kanan. Tampilan ini berdeda dengan browser lain dimana crome browser manampilkan data dengan padat dan tanpa adanya tanda pemisah nomer kartu dengan nama. Data tertampil sangat lengkap mulai dari Nomer Kartu, Nama pengguna, Terdapat juga untuk nomer CVV tertera pada offset 105eedef00. Nomer kartu tersebut tertera dan tercapture oleh FTK Imager telah digunakan untuk bertransaksi pada website dan telah menekan tombol checkput seperti yang tertera pada offset 105eed100.



Gambar 4.16 Tampilan Kirim Data Ke Server Broswser Crome

Dari gambar 4.16 menunjukan bahwa mozilla crome terdapat artefak pengiriman data kartu ke serve pelaku dengan perintah GET. Perintah pengiriman [GET] data nomer kartu di kirimkan ke ip 127.0.0.1:5000 website http://tesis.test pada tanggal 15 Juni 2021 pukul 09:22:45 UTC.

4.4 Laporan Bukti Digital (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 4.3 Tabel Hasil Analisa

No	Artefak BB	Analisis Tools FTK Forensik						Keterangan
		Hush MD5	SHA 1	Hasil Capture RAM	Nama	Nomor	CVV	
1	M. Edge	7b68457ed77ac3ccbbd7e6b0a0072201	59afafee95390385e7d77a1b7e80ca0065c99a2	FormjackingOPERA.mem	✓	✓	✓	
2	Opera	15ce82d6d4a7aacea26c6ae428532f66	81fdcd0ff3403a36af5d8cbb1fb6ad9fade4be1c5	FormjackingEDGE.mem	✓	✓	✓	
3	FireFox	96ac1fe9df2edb546a1b72cee21a6280	Fb25ea8aa6f4795783349abb1fb6ad9fade4be1c5	FormjackingFirefox.mem	✓	✓	✓	
4	Crome	1d426373538cf1a395ef0e5466d4240b	F457c295be5b37a140d5d5a3b38bd5e5ad579f27	FormjackingCrome.mem	✓	✓	✓	

BAB 5
Kesimpulan dan Saran

5.1 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 sebagai bahan pendukung investigasi bukti digital pencurian data formjacking pada website ecommerce. Dalam menyakinkan bahwa barang bukti adalah asli yaitu dengan hasil hash MD5 dan SHA1 didapat dari analisi data pada ram leptop. Berdasarkan hasil dari tahapan-tahapan metode yang telah dilakukan, proses investigasi bukti digital formjacking pada website ecommerce dapat dikatakan bahwa bukti digital berupa data yang valid.

5.2 Saran

1. Untuk keperluan penelitian selanjutnya adalah melakukan pengembangan terhadap metode investigasi dengan menerapkan live forensik dalam mode online atau berada dalam server hosting.
2. Perlu dilakukan penelitian lebih lanjut terhadap serangan formjacking pada pada website ecoomerce dengan menggunakan framework cms lainnya.

Daftar Pustaka

Bintang, R. A. K. N., Umar, R., & Yudhana, U. (2018). Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10. *Prosiding SNST Ke-9 Tahun 2018 Fakultas Teknik Universitas Wahid Hasyim*, 125–128.

Casey, E. (2011). Digital Evidence and Computer Crime. In *Securing the Information Infrastructure*. https://doi.org/10.4018/978-1-59904-379-1.ch015

Faiz, M. N., Umar, R., & Yudhana, A. (2016). Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary. *ILKOM Jurnal Ilmiah*, *8*(3), 242–247. https://doi.org/10.33096/ilkom.v8i3.79.242-247

Faiz, M. N., Umar, R., & Yudhana, A. (2017). Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *1*(3), 108. https://doi.org/10.14421/jiska.2017.13-02

Gupta, M. K., Govil, M. C., & Singh, G. (2015). *Predicting Cross-Site Scripting (XSS) Security Vulnerabilities in Web Applications*. 162–167.

Kurniawan, N A. (2014). Pencegahan Kejahatan Carding Sebagai Kejahatan Transnasional Menurut Hukum Internasional. *Kumpulan Jurnal Mahasiswa …*. http://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/632

Kurniawan, Novryan Alfin. (2014). *Jurnal pencegahan kejahatan carding sebagai kejahatan transnasional menurut hukum internasional*.

Marshall, A. M. (2005). Digital evidence. *Measurement and Control*, *38*(3), 79–82. https://doi.org/10.1177/002029400503800302

Nugraha, U. (2016). Pada Perguruan Tinggi Menggunakan Kerangka Kerja Nist Sp 800-300. *Seminar Nasional Telekomunikasi Dan Informatika (SELISIK 2016)*, *Selisik*, 121–126.

Nuh Al-Azhar, M. (2012). *digital forensics*. 302.

Nur Faiz, M., Adi Prabowo, W., & Fajar Sidiq, M. (2018). Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal. *Journal of Informatics, Information System, Software Engineering and Applications (INISTA)*, *1*(1), 63–70. https://doi.org/10.20895/INISTA.V1I1

Pii, G. H., & Horsman, G. (2017). *Accepted Manuscript*.

Purbasari, W. (2017). Model Kepercayaan Konsumen Pada Situs E-Commerce. *Teknikom*, *1*(1), 2598–2958. https://dx.doi.org/10.24034/j25485024.y2020.v4.i2.4163

Puspitaningrum, D. A. (2017). *Faktor – Faktor Yang Loyalitas Pada Konsumen E-Commerce Tokopedia Di Kota Semarang*. *1*(1), 1–13.

Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, *4*(10), 1048–1056. http://www.ijser.org/researchpaper%5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf

Rahman, S., & Khan, M. N. A. (2015). Review of Live Forensic Analysis Techniques. *International Journal of Hybrid Information Technology*, *8*(2), 379–388. https://doi.org/10.14257/ijhit.2015.8.2.35

Ramadhan, R. A., & Mualfah, D. (2020). Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh. *IT Journal Research and Development*, *5*(2), 183–192. https://doi.org/10.25299/itjrd.2021.vol5(2).5750

Riadi, I., Fadlil, A., & Aulia, M. I. (2019). Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ). *Jurnal Teknik Informatika Dan Sistem Informasi (JuTISI)*, *8*(3), 107–118.

Rochmadi, T. (2019). Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar. *Indonesian Journal of Business Intelligence (IJUBI)*, *1*(1), 32. https://doi.org/10.21927/ijubi.v1i1.878

Rosita. (2018). Analisis Computer Forensic. *Sicurezza E Scienze Sociali*, *3*, 99–109. https://doi.org/10.3280/siss2017-003009

Sant, P. (2014). *Digital Forensics : the need for Integration Digital Forensics : the need for Integration Keywords*. *June*.

Sidiq, M. F., & Faiz, M. N. (2019). Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *5*(1), 67. https://doi.org/10.26418/jp.v5i1.31430

Umar, R., Yudhana, A., & Nur Faiz, M. (2016). Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary. *Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM)*, 207–211.

Yudhistira, D. S. (2018). *Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop*.

Saran Perbaikan dari Penguji

LEMBAR REVISI UJIAN TESIS

Nama Mahasiswa/ NIM:	Nova Setiawan	17917120
Judul Tesis:	Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce	
Pembimbing:	Ahmad Rafie Pratam, ST., MIT., Ph.D /	

1. Masukan **Kualitas Akademik** (melaksanakan penelitian)
Perbaiki metodologi dalam pelaksanaan penelitian
2. Masukan Kualitas artefak (melaksanakan penelitian)
Isseu form jacking perlu di pertajam untuk dibahas dalam laporan.
3. Masukan **Kontribusi ke disiplin Ilmu** (melaksanakan penelitian)
Belum ada analisa tentamng form jacking yang komprehensif sesuai dengan latar belakang dan tujuan.
4. Masukan **Kualitas Penulisan** (komunikasi ilmiah)
Perbaiki laporan secara keseluruhan , minimal 40 halaman
5. Masukan **Presentasi Ujian Tesis** (komunikasi ilmiah)

Yogyakarta, 22 Juni 2021

Penguji,

(Dr. Yudi Prayudi, S.Si., M.Kom)

LEMBAR REVISI UJIAN TESIS

Nama Mahasiswa/ NIM:	Nova Setiawan	17917120
Judul Tesis:	Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce	
Pembimbing:	Amad Raf'ie Pratam, ST., MIT., Ph.D /	

1. Masukan **Kualitas Akademik** (melaksanakan penelitian)
Abstrak perlu disesuaikan lagi, detail metode atau tahapan live forensik belum di munculkan, hasil investigasi belum disajikan secara komprehensif, tingkat keberhasilan perlu ditambahkan.
2. Masukan Kualitas artefak (melaksanakan penelitian)
Skenario kasus pada browser perlu di detailkan, e-commerce yang digunakan apa, kemudian tahapan masing-masing yang digunakan seperti NIJ, masing-masing tahapan seperti apa ? perlu di jelaskan dalam hasil dan pembahasan.
3. Masukan **Kontribusi ke disiplin Ilmu** (melaksanakan penelitian)
Hasil investigasi perlu disajikan dalam bentuk tabel dan visualisasi secara grafis untuk memperjelas hasil penelitian ini.
4. Masukan **Kualitas Penulisan** (komunikasi ilmiah)
Perlu di sesuaikan dengan EYD dan KBBI, tulisan di sesuaikan dengan template penulisan tesis terbaru.
5. Masukan **Presentasi Ujian Tesis** (komunikasi ilmiah)
Perlu di tingkatkan lagi kemampuan penyajian data dalam media presentasi

Yogyakarta, 22 Juni 2021

Penguji,

(Dr. Imam Riadi, S.Pd., M.Kom)

LEMBAR REVISI UJIAN TESIS

Nama Mahasiswa/ NIM:	Nova Setiawan	17917120
Judul Tesis:	Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce	
Pembimbing:	Ahmad Raf'ie Pratama, ST., MIT., Ph.D /	

1. Masukan **Kualitas Akademik** (melaksanakan penelitian)
-
2. Masukan Kualitas artefak (melaksanakan penelitian)
-
3. Masukan **Kontribusi ke disiplin ilmu** (melaksanakan penelitian)
-
4. Masukan **Kualitas Penulisan** (komunikasi ilmiah)
Penulisan laporan perlu dilengkapi. Masih banyak hal yang belum disampaikan di dalam laporan.
5. Masukan **Presentasi Ujian Tesis** (komunikasi ilmiah)
-

Yogyakarta, 22 Juni 2021

Penguji,

(Ahmad Raf'ie Pratama, ST., MIT., Ph.D)

Catata pada saat Presentasi Pendadaran

pak Imam

- pada abstrak hasus ada hasilnya (tolong ditambahkan)
- rumusan msalah
- bandingkan pada analisis nij
- referensi harus diperbanyak kajijan penelitian terdahulu.
- ceritakan tahapan dari hasil dari skenario kasusnya dilakukan pada browser

Pak Yudi

- Tinjuan pustakan Formjacking ditambahkan.
- Explorasi metode penelitian
- metode berkaitan dengan tahapan penyelesaikan problem bergantung pada metodologi untuk menyelesaikan forensiknya
- tipe data apa saja yang di ambil oleh
- dimanakah artefak itu
- hal apa yang dilakukan oleh formjacking
- apa yang dapat dilakukan saat formjacking ini terjadidan apa rekomendasi yang harus dilakukan

LAMPIRAN A