Analisis Keamanan Menggunakan Metode *Live Forensic* pada Web

Nur Dwi Putri[1)*)], Dahliyusmanto[2)]

[1)2)] Program Studi Teknik Informatika, Universitas Riau
[*)]Correspondence Author: nur.dwi1145@student.unri.ac.id, Pekanbaru, Indonesia
DOI: https://doi.org/10.37012/jtik.v10i1.1918

Abstrak

Perkembangan teknologi informasi dan konektivitas internet di Indonesia menciptakan perubahan signifikan dalam gaya hidup masyarakat. Dengan lebih dari 212,9 juta pengguna internet pada Januari 2023, terjadi peningkatan 5.2% dari tahun sebelumnya, menandai transisi besar ke aktivitas digital. Terutama di saat pandemi, kegiatan berbelanja di toko fisik berkurang, dan platform belanja online atau sering disebut *e-commerce* mulai diminati oleh masyarakat. Namun, peralihan ke lingkungan digital juga membawa risiko kejahatan siber yang meningkat. Salah satu ancamannya adalah pencurian data digital berupa email dan password pengguna *e-commerce*. Dengan menggunakan metode *live forensic* yang tahapannya mengacu pada kerangka kerja *National Institute of Justice,* penelitian ini bertujuan untuk menunjukkan bagaimana metode *live forensic* pada RAM di komputer dapat digunakan untuk mendapatkan data yang terekam pada RAM (*Random Access Memory*), dengan menggunaan FTK Imager sebagai *tools forensics*. Langkah kerja pada metode *live forensic* ini mengacu pada 5 tahap langkah yaitu *Identification*, *Collection, Examination, Analyses,* dan *Reporting*. Dapat diketahui bahwa pada 2 simulasi yang dilakukan yang melibatkan 5 akun yang berbeda saat membuka website e-commerce menggunakan browser Google Chrome, dalam kedua simulasi tersebut, email pengguna dapat terdeteksi pada tools FTK Imager, tetapi password yang digunakan untuk mengakses tidak dapat terdeteksi pada alat tersebut. Hasil dari penelitian ini menunjukkan bahwa web *e-commerce* yang digunakan pada penelitian ini aman untuk di akses oleh pengguna.

Kata Kunci: *Live Forensic, Digital Forensic*, *E-Commerce, FTK Imager*

Abstract

The development of information technology and internet connectivity in Indonesia has created significant changes in people's lifestyles. With more than 212.9 million internet users in January 2023, there was a 5.2% increase from the previous year, marking a major transition to digital activity. Especially during the pandemic, shopping activities in physical stores are reduced, and online shopping platforms or often called e-commerce are starting to be popular with the public. However, the shift to a digital environment also brings with it an increased risk of cybercrime. One of the threats is the theft of digital data in the form of emails and passwords of e-commerce users. By using a live forensic method whose stages refer to the framework of the National Institute of Justice, this research aims to show how the live forensic method in RAM on a computer can be used to obtain data recorded in RAM (Random Access Memory), using FTK Imager as a tool forensics. The work steps in this live forensic method refer to 5 stages, namely Identification, Collection, Examination, Analysis, and Reporting. It can be seen that in the 2 simulations carried out involving 5 different accounts when opening an e-commerce website using the Google Chrome browser, in both simulations, the user's email can be detected in the FTK Imager tool, but the password used to access cannot be detected in the tool. the. The results of this research indicate that the e-commerce website used in this research is safe for users to access.

Keywords: *Live Forensics, Digital Forensics, E-Commerce, FTK Imager*

PENDAHULUAN

Perkembangan zaman yang diikuti dengan perkembangan teknologi membuat tuntutan terhadap kehidupan menjadi serba mudah dan instan. Perkembangan teknologi terutama informasi memberi pengaruh yang sangat signifikan terhadap perubahan gaya hidup di masyarakat. Teknologi informasi memudahkan seluruh kegiatan masyarakat dalam berbagi hal, misalkan melakukan transaksi keuangan, melakukan pembayaran, sampai kepada melakukan pembelian (berbelanja) (Purnama & Putri, 2021).

Reportal Digital Indonesia (2023), memaparkan bahwa terdapat 212,9 juta pengguna internet di Indonesia terhitung dari Januari 2023, meningkat 5.2% dari 2022. Bertambahnya jumlah pengguna internet ini berhubungan signifikan terhadap total pengguna platform digital seperti media sosial dan *marketplace* di Indonesia. Terutama di saat pandemi, kegiatan berbelanja di toko fisik berkurang, dan platform belanja online atau sering disebut *e-commerce* mulai diminati oleh masyarakat. Namun, seiring dengan peralihan aktivitas ke lingkungan digital, risiko kejahatan *cyber* juga meningkat. Badan Siber dan Sandi Negara (BSSN) memprediksi peningkatan tren serangan siber, termasuk *ransomware*, kebocoran data, *phising*, dan *social engineering* pada tahun 2023.

Sebagai contoh, kasus peretasan Tokopedia pada tahun 2020 menunjukkan ancaman nyata. Seorang peretas internasional dengan nama samaran 'Why So Dank' berhasil meretas Tokopedia, menyebabkan informasi pribadi 15 juta pengguna bocor. Data tersebut kemudian dijual di dark web seharga US$5.000, menyebabkan dampak negatif berupa ulasan buruk terhadap e-commerce lain dan penurunan pengunjung situs Tokopedia. Keamanan web menjadi hal yang penting, dan metode *live forensic* menjadi salah satu pendekatan untuk menganalisis keamanan web. Metode ini dilakukan secara langsung saat perangkat masih aktif dan dapat menghasilkan bukti ilmiah terkait keamanan situs web, terutama dalam konteks e-commerce yang mengandung informasi sensitif seperti email dan password pengguna.

Pada penelitian Rauhulloh Ayatulloh Khomeini Noor Bintang, dkk yang berjudul “Perancangan Perbandingan *Live Forensics* Pada Keamanan Media Sosial Instagram, Facebook Dan Twitter Di Windows 10”(Bintang et al., 2018), menunjukan bahwa dalam melakukan analisis forensik terhadap media sosial pada perangkat laptop atau komputer, diperlukan suatu metode dan perangkat yang dapat membantu peneliti dalam mencari dan

menginvestigasi data. Penelitian dimulai dengan pembuatan akun media sosial di platform seperti Facebook, Instagram, dan Twitter. Selanjutnya, penelitian ini melibatkan pemilihan alat-alat yang digunakan untuk mengambil data dari akun media sosial tersebut. Pada tahap ini, digunakan alat FTK Imager sebagai pengelola data yang akan dianalisis. Ketika membuat akun media sosial di Facebook, Instagram, dan Twitter, dilakukan proses *cloning* data dan *hashing* data untuk memastikan bahwa akun media sosial tersebut mewakili data atau akun asli. Langkah berikutnya adalah menganalisis akun media sosial tersebut untuk mendapatkan data yang dapat digunakan sebagai bukti forensik yang sah. Pada tahap akhir, dilakukan pelaporan hasil penelitian yang mencakup data dari media sosial sebagai bukti forensik yang valid. Dalam laporan ini juga dijelaskan tahapan-tahapan atau proses yang digunakan untuk mendapatkan bukti yang memastikan keaslian dan validitas data tersebut.

Berdasarkan permasalahan yang telah dijelaskan diatas, maka penulis akan meneliti keamanan web e-commerce yang melibatkan 5 akun yang berbeda untuk mengetahui keamanan web, menggunakan metode *Live Forensic* untuk mendapatkan data yang terekam pada RAM (*Random Access Memory*), dan menggunakan FTK Imager sebagai *tools forensics.*

METODE

Dalam penelitian ini ada beberapa metodologi yang digunakan yaitu studi literatur, identifikasi masalah, identifikasi kebutuhan, perancanagn sistem, implementasi, pengujian sistem, analisis *live forensic*.

a. Studi Literatur

   Metode penelitian ini menggunakan review literatur, mencakup sumber seperti jurnal, paper, artikel ilmiah, buku, dan makalah terkait dengan judul penelitian. Penulis mengembangkan literatur yang ditemukan untuk mengidentifikasi masalah penelitian, sehingga memberikan kontribusi dalam menyelesaikan penelitian ini.

b. Identifikasi Masalah

   Penelitian ini mengangkat permasalahan maraknya kasus kebocoran data pada web e-commerce yang dapat menyebabkan penyalahgunaan data dan kerugian. Penelitian

berfokus pada penggunaan metode *live forensic* sebagai panduan untuk mengevaluasi keamanan web e-commerce.

c. Identifikasi kebutuhan

Penelitian ini mengidentifikasi kebutuhan dengan mencari spesifikasi perangkat yang dibutuhkan untuk membuat sistem yang akan diteliti, termasuk perangkat keras seperti laptop dan hardisk *external*. Perangkat lunak yang digunakan yaitu AccessData FTK Imager, Google Chrome, dan CMS.

d. Perancangan sistem

Pada perancangan sistem ini akan dijelaskan langkah-langkah dalam mengimplementasikan *live forensic* pada web e-commerce. Pada tahapan ini dilakukannya insalasi FTK Imager, setelah itu membuat layanan e-commerce, konfigurasi domain dan hosting, dan melakukan *live forensic* pada sistem.

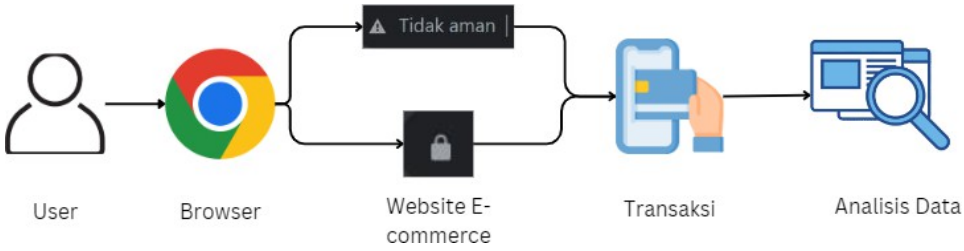
e. Implementasi

Tahap implementasi merupakan langkah lanjutan setelah tahap perancangan. Pada tahap ini, sistem akan dibangun sesuai dengan rencana yang telah disusun sebelumnya. Tujuan utama adalah memastikan efektivitas penerapan metode *live forensic* sesuai dengan perencanaan dan pedoman yang telah ditetapkan sebelumnya.

f. Pengujian sistem

Tahap pengujian ini melibatkan skenario penelitian untuk mendapatkan hasil yang valid seperti tampak pada Gambar 1. Pengguna akan mengakses laman website e-commerce mengunakan browser Google Chrome, kemudian login dengan email dan *password* ke akun website *e-commerce* melalui browser google chrome. Setelah berhasil login, pengguna akan melakukan pemilihan barang yang kemudian dibawa ke laman *checkout* dimana pengguna akan melakukan pembayaran. Setelah selesai melakukan pengisian dan klik tombol checkout, akan muncul pesan notifikasi konfirmasi bahwa pengguna telah melakukan pembelian barang. Pada skenario pertama user akan masuk website e-commerce yang menggunakan protokol SSL/TSL (Secure Socket Layer/Transport Layer Security) yang sering dilihat dengan tanda pengenal HTTPS. Pada skenario kedua user akan masuk ke website yang tidak memiliki protokol SSL/TSL (Secure Socket Layer/Transport Layer Security). Selanjutnya peneliti akan melakukan proses *capture memory* di setiap akun yang ada

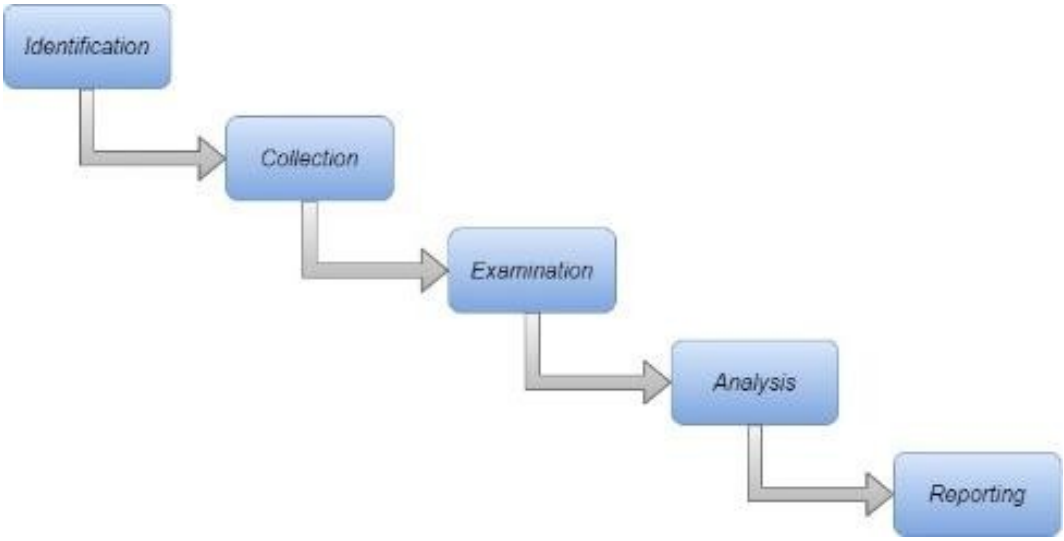
di browser tersebut. Proses *capture memory* ini dilakukan satu per satu, yang nantinya penelitian ini melakukan 10 *capture memory* pada 5 akun yang berbeda. Proses *capture memory* ini dilakukan menggunakan tool FTK Imager, peneliti akan melanjutkan tahapan analisis hasil dari *capture memory* data tersebut.



Gambar 1. Skenario Penelitian

g. Analisis *live forensic*

Pada bagian ini menampilkan hasil analisis keamanan sesuai dengan tahapan-tahapan penelitian yang akan dilakukan. Langkah kerja pada metode *live forensic* ini mengacu pada 5 tahap langkah *National Institute of Justice* yang dapat dilihat pada Gambar 2 dibawah ini.



Gambar 2. Tahapan *Life forensic National Institute of Justice*

1. *Identification*, adalah langkah awal dalam menentukan persiapan dan pemeriksaan alat serta bahan yang diperlukan untuk penelitian. Fokus utamanya adalah memastikan ketersediaan, keberfungsian, dan kesiapan semua peralatan dan materi yang diperlukan sebelum melanjutkan ke tahap

berikutnya dalam proses penelitian. Identifikasi menjadi dasar yang penting sebelum memasuki langkah-langkah selanjutnya.

2. *Collection*, tahap ini melibatkan pengumpulan data digital dari browser dengan melakukan dua simulasi pada 5 akun website e-commerce menggunakan FTK Imager. Data yang terkumpul akan melalui proses analisis lebih lanjut. Langkah-langkah dilakukan saat laptop masih aktif karena data bersifat volatile dan dapat hilang jika laptop dimatikan. Proses ini penting dalam *Live Forensic* untuk memeriksa aktivitas sistem tanpa mengganggu integritas data.
3. *Examination*, adalah tahap pengecekan data yang telah dikumpulkan melalui proses *capture memory* dengan menggunakan skenario yang telah ditetapkan sebelumnya. Tujuan utama tahap ini adalah memastikan integritas dan keaslian data yang telah diakuisisi, serta untuk memverifikasi ketiadaan perubahan tidak sah atau tindakan mencurigakan pada file selama proses akuisisi.
4. *Analysis*, tahapan mendalam data hasil *capture memory* dari *Random Access Memory* melibatkan pengujian parameter seperti hash MD5, hash SHA1, email, dan kata sandi. Evaluasi data pada tahap ini bertujuan untuk mengidentifikasi potensi masalah keamanan dan informasi penting lain yang relevan dengan tujuan penelitian.
5. *Reporting*, adalah langkah akhir di mana semua barang bukti digital dari aktivitas penggunaan browser disusun dan dianalisis secara mendalam, kemudian disajikan secara rinci dalam laporan penelitian. Proses ini bertujuan untuk menyampaikan temuan dengan jelas, memudahkan pengambilan keputusan berdasarkan data dan fakta yang telah dianalisis.

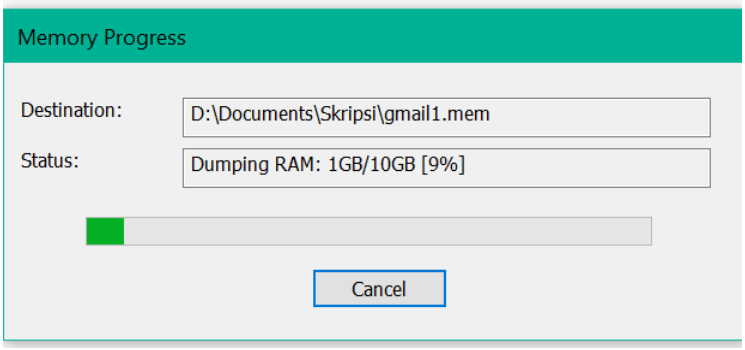
HASIL DAN PEMBAHASAN

Proses Identification telah dilakukan sesuai dengan skenario penelitian pada Gambar 1, identifikasi kebutuhan, dan akun simulasi yang digunakan pada Tabel 1 berikut ini:

Tabel 1. Akun Simulasi

No	Email	Password
1	z48542158@gmail.com	Zahra@mel1aaa
2	jannahraniaa@hotmail.com	N4tureb0ss123
3	shafirahhanifah@outlook.com	sepatu123
4	shakiraamira@tutanota.com	G4rlic0green
5	salsabilahauliaaa@yahoo.com	otent1ktea

Pengumpulan data (tahap *Collection*) dilakukan dengan menggunakan FTK Imager bertujuan untuk mengambil informasi dari aktivitas yang terjadi pada halaman website e-commerce. Data yang terkumpul kemudian dianalisis untuk mengidentifikasi proses yang sedang berjalan di sistem, sebagaimana terlihat pada Gambar 3.



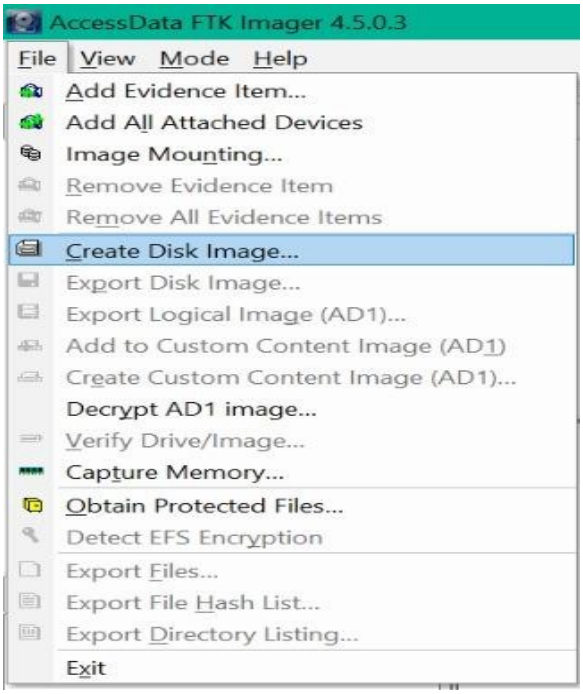
Gambar 3. Proses *Capture Memory*

Hasil dari proses pengakuisisi memori adalah sebuah file dengan eksistensi .mem yang dapat dilihat pada Gambar 4 berikut ini.

Gmail	13/11/2023 19:52	MEM File	9.936.896 KB
gmail1	04/11/2023 13:02	MEM File	9.936.896 KB
hotmail	13/11/2023 20:11	MEM File	9.936.896 KB
hotmail1	04/11/2023 19:56	MEM File	9.936.896 KB
Outlook	13/11/2023 21:50	MEM File	9.936.896 KB
outlook1	05/11/2023 9:12	MEM File	9.936.896 KB
tutanota	14/11/2023 21:29	MEM File	9.936.896 KB
tutanota1	04/11/2023 20:43	MEM File	9.936.896 KB
Yahoo	13/11/2023 22:06	MEM File	9.936.896 KB
Yahoo1	05/11/2023 9:50	MEM File	9.936.896 KB

Gambar 4. Hasil *Capture Memory*

Setelah melakukan proses *capture memory* atau proses akuisisi data dari RAM yang menghasilkan file dengan eksistensi .mem, langkah selanjutnya adalah pengecekan nilai hash pada hasil capture memory untuk masing-masing file dengan memilih menu "create disk image" pada FTK Imager seperti pada Gambar 5 berikut ini.



Gambar 5. Menu "Create Disk Image"

Hasil dari *disk image* akan menghasilkan informasi mengenai MD5 Hash dan SHA1 Hash seperti pada Gambar 6. Nilai-nilai ini mengindikasikan bahwa file yang telah diakuisisi tidak mengalami perubahan dan dengan ini dapat menunjukkan keaslian file.

Gambar 6. Nilai Hash File Gmail1

Pada Tabel 2 yang menunjukkan hasil rekapitulasi dari nilai hash pada website e-commerce di simulasi pertama yang terverifikasi nilai *Computed hash* dan *Report hash* memiliki nilai hash yang identik.

Tabel 2. Nilai Hash Simulasi 1

Nama File	MD5	SHA1
gmail1.mem	4e90e76667f8bde8f3614c030c372397	34df26d1c68509ce199125a228d177fb7fd17864
hotmail1.mem	960112a261284438c3e0680fc7cbc1e9	047b90617f10916d8ef08cf95380f5cf748d1ae1
outlook1.mem	2a3dbac5081bd043bbfcbb9f4b3beb51	6a5e637e88c7ec73965ae4ea6e77d55a5301bd15
tutanota1.mem	65a80035cf0f67eb680093f790124cc9	a43aa51529516b08dbd242ec957791670bd12295
Yahoo1.mem	8632b980eb38a3147dbda1623a867708	1992f9c78d59b88b7b8be6f65b65c226c7daa8e5

Pada Tabel 3 yang menunjukkan hasil rekapitulasi dari nilai hash pada website e-commerce di simulasi kedua yang terverifikasi nilai *Computed hash* dan *Report hash* memiliki nilai hash yang identik.

Tabel 3. Nilai Hash Simulasi 2

Nama File	MD5	SHA1
Gmail.mem	2bfa8b6e9243544b7ec5b9e429b6f85e	4a2effb963df0a7cee333e09dcb6878658bc4388
hotmail.mem	ed307ed946547c9940c0d817867befaa	589c441f2e55db3bbaeb70e61cffeb0d388ab3cf
Outlook.mem	c6c8bce1aa4bdd485a9a28160e5dc318	ca36da09536bb03514db65f08b0935ebb8560c88
tutanota.mem	a9a4f99500d6b42f12b978c4b099b5d3	040a84e48775d7b04f68987bef1bef654da994db
Yahoo.mem	a8122de19bb0b3b3567cecbfdfe297c2	dfe512ddaf6f7480874378684c81544a31bc5a0a

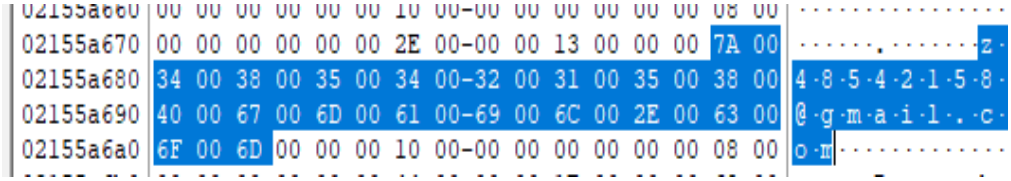
Pada proses Analysis dilakukan analisis pada hasil akuisisi file extension .mem pada simulasi 1 dan simulasi 2.

1. Analisis Simulasi Pertama

a. Akun 1

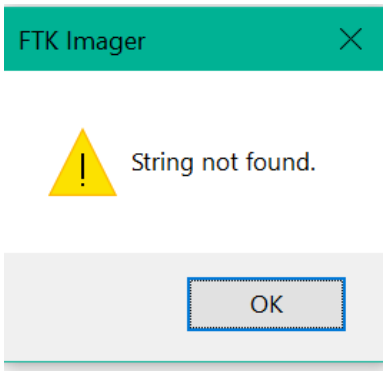
Setelah melakukan *capture memory* didapatkan file gmail1.mem. Analisis yang dilakukan mendapatkan hasil sebagai berikut:

Pada Gambar 7 dibawah ini pada offset 02155a670 sampai dengan 02155a6a0, terlihat detail email yang digunakan oleh user yaitu z48542158@gmail.com.



Gambar 7. Email Pengguna Akun 1

Pada Gambar 8 saat dilakukan analisis atau mencari password pengguna akun1, hasil yang didapatkan tidak ada atau tidak ditemukan.

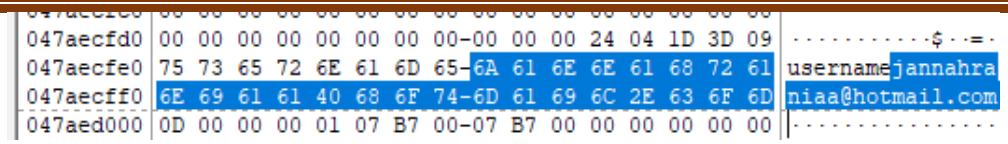


Gambar 8. Password Pengguna Tidak Ditemukan

b. Akun 2

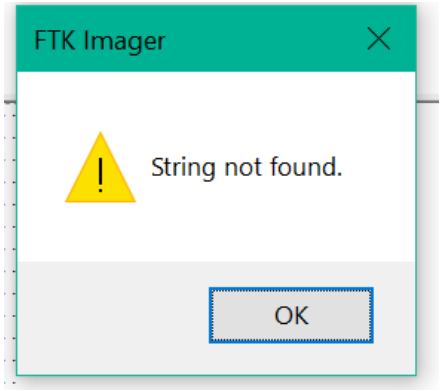
Setelah melakukan *capture memory* didapatkan file gmail1.mem. Analisis yang dilakukan mendapatkan hasil sebagai berikut:

Pada Gambar 9 dibawah ini pada offset 047aecfe0 sampai dengan 047aecff0, terlihat detail email yang digunakan oleh user yaitu jannahraniaa@hotmail.com.



Gambar 9. Email Pengguna Akun 2

Pada Gambar 10 saat dilakukan analisis atau mencari password pengguna akun 2, hasil yang didapatkan tidak ada atau tidak ditemukan.

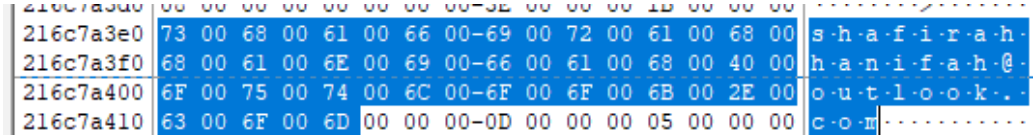


Gambar 10. Password Pengguna Tidak Ditemukan

c. Akun 3

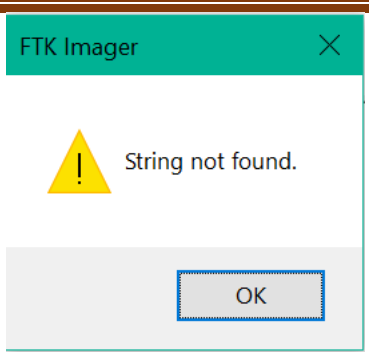
Setelah melakukan *capture memory* didapatkan file gmail1.mem. Analisis yang dilakukan mendapatkan hasil sebagai berikut:

Pada Gambar 11 dibawah ini pada offset 216c7a3e0 sampai dengan 216c7a410, terlihat detail email yang digunakan oleh user yaitu shafirahhanifah@outlook.com.



Gambar 11. Email Pengguna Akun 3

Pada Gambar 11 saat dilakukan analisis atau mencari password pengguna akun 3, hasil yang didapatkan tidak ada atau tidak ditemukan.

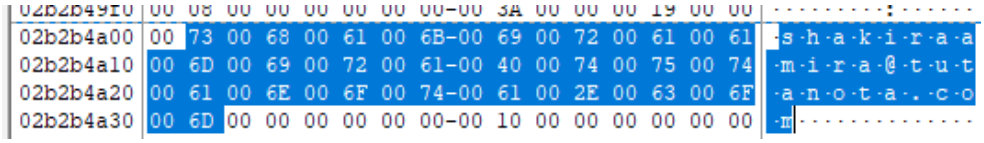


Gambar 12. Password Pengguna Tidak Ditemukan

d. Akun 4

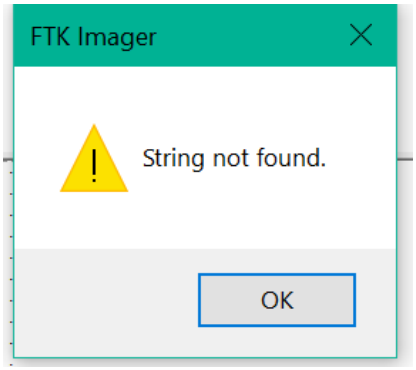
Setelah melakukan *capture memory* didapatkan file gmail1.mem. Analisis yang dilakukan mendapatkan hasil sebagai berikut:

Pada Gambar 13 dibawah ini pada offset 02b2b4a00 sampai dengan 02b2b4a30, terlihat detail email yang digunakan oleh user yaitu shakiraamira@tutanota.com.



Gambar 13. Email Pengguna Akun 4

Pada Gambar 14 saat dilakukan analisis atau mencari password pengguna akun 4, hasil yang didapatkan tidak ada atau tidak ditemukan.

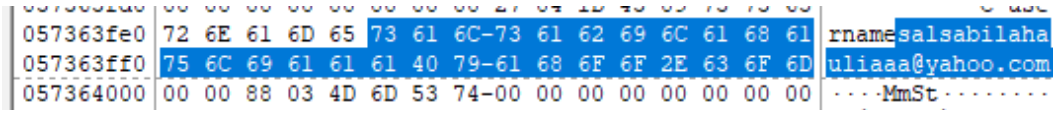


Gambar 14. Password Pengguna Tidak Ditemukan

e. Akun 5

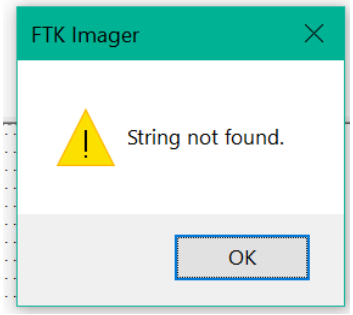
Setelah melakukan *capture memory* didapatkan file gmail1.mem. Analisis yang dilakukan mendapatkan hasil sebagai berikut:

Pada Gambar 15 dibawah ini pada offset 057363fe0 sampai dengan 057363ff0, terlihat detail email yang digunakan oleh user yaitu salsabilahauliaaa@yahoo.com.



Gambar 15. Email Pengguna Akun 5

Pada Gambar 16 saat dilakukan analisis atau mencari password pengguna akun 5, hasil yang didapatkan tidak ada atau tidak ditemukan.



Gambar 16. Password Pengguna Tidak Ditemukan

Hasil dari penelitian ini adalah 5 akun yang digunakan dalam simulasi pertama pada penelitian ini di website *e-commerce* yang menggunakan Browser Google Chrome sama sama mencatat artefak digital berupa email yang digunakan oleh user untuk login ke website e-commerce. Namun password yang digunakan pada 5 akun tersebut tidak dapat ditemukan. berikut ini tabel 4 berisi hasil validasi Analisa *Random access Memory* pada simulasi pertama:

Tabel 4. Hasil Analisis Simulasi 1

Nama File	Hash MD5	Hash SHA 1	Email	Password
gmail1.mem	4e90e76667f8bde8f3614c030c372397	34df26d1c68509ce199125a228d177fb7fd17864	Ada	Tidak Ada
hotmail1.mem	960112a261284438c3e0680fc7cbc1e9	960112a261284438c3e0680fc7cbc1e9	Ada	Tidak Ada
outlook1.mem	2a3dbac5081bd043bbfcbb9f4b3beb51	6a5e637e88c7ec73965ae4ea6e77d55a5301bd15	Ada	Tidak Ada
tutanota1.mem	65a80035cf0f67eb680093f790124cc9	a43aa51529516b08dbd242ec957791670bd12295	Ada	Tidak Ada
Yahoo1.mem	8632b980eb38a3147dbda1623a867708	1992f9c78d59b88b7b8be6f65b65c226c7daa8e5	Ada	Tidak Ada

2. Analisis Simulasi Kedua

Simulasi kedua dilakukan dengan cara yang sama dengan simulasi pertama. Pada simulasi kedua 5 akun yang digunakan pada penelitian ini di website *e-commerce* yang menggunakan Browser Google Chrome sama sama mencatat artefak digital

berupa email yang digunakan oleh user untuk login ke website e-commerce. Namun password yang digunakan pada 5 akun tersebut tidak dapat ditemukan. Berikut ini tabel 5 hasil validasi Analisa *Random access Memory* pada simulasi kedua:

Tabel 5. Hasil Analisis Simulasi 2

Nama File	Hash MD5	Hash SHA 1	Email	Password
Gmail.mem	2bfa8b6e9243544b7ec5b9e429b6f85e	4a2effb963df0a7cee333e09dcb6878658bc4388	Ada	Tidak Ada
hotmail.mem	ed307ed946547c9940c0d817867befaa	589c441f2e55db3bbaeb70e61cffeb0d388ab3cf	Ada	Tidak Ada
outlook.mem	c6c8bce1aa4bdd485a9a28160e5dc318	ca36da09536bb03514db65f08b0935ebb8560c88	Ada	Tidak Ada
tutanota.mem	a9a4f99500d6b42f12b978c4b099b5d3	040a84e48775d7b04f68987bef1bef654da994db	Ada	Tidak Ada
Yahoo.mem	a8122de19bb0b3b3567cecbfdfe297c2	dfe512ddaf6f7480874378684c81544a31bc5a0a	Ada	Tidak Ada

KESIMPULAN DAN REKOMENDASI

Penelitian ini menggunakan metode *Live forensic* yang didasarkan pada kerangka kerja yang disusun oleh *National Institute of Justice* (NIJ) untuk mengevaluasi tingkat keamanan pada website e-commerce. Dalam pengimplementasian *Live forensic*, penelitian ini memanfaatkan perangkat *forensic* yang dikenal sebagai FTK Imager sebagai pendukung untuk mengetahui keamanan website. Hasil menunjukkan bahwa pada simulasi pertama, 5 akun yang digunakan saat membuka website e-commerce menggunakan browser Google Chrome email yang digunakan terdeteksi pada tools FTK Imager. Namun password yang digunakan untuk mengakses tidak dapat terdeteksi pada tools FTK Imager. Hasil menunjukan bahwa pada simulasi kedua 5 akun saat membuka website e-commerce menggunakan browser Google Chrome email dapat terdeteksi pada tools FTK Imager. Namun, password yang digunakan untuk mengakses tidak dapat terdeteksi pada tools FTK Imager. Dapat diketahui bahwa pada 2 simulasi yang dilakukan yang melibatkan 5 akun yang berbeda saat membuka website e-commerce menggunakan browser Google Chrome, dalam kedua simulasi tersebut, email pengguna dapat terdeteksi pada tools FTK Imager, tetapi password yang digunakan untuk mengakses tidak dapat terdeteksi pada alat tersebut.

Untuk penelitian selanjutnya disarankan menggunakan *tools forensic* dan metode yang berbeda, dan juga analisis lebih lanjut terhadap log aktivitas pada *server website* e-commerce untuk mendeteksi pola-pola atau tanda-tanda aktivitas mencurigakan yang mungkin mengindikasikan serangan keamanan.

REFERENSI

Ahmadi, A.-. (2018). Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ). *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, *4*(1), 8. https://doi.org/10.24014/coreit.v4i1.5803

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

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.

Daulay, Z. S., & Indrayani, R. (2022). Analisis Keamanan Browser Dalam Bersosial Media Menggunakan Metode Institute of Justice (Nij). *Djtechno: Jurnal Teknologi Informasi*, *3*(2), 167–175. https://doi.org/10.46576/djtechno.v3i2.2598

Hafizh, M. N., Riadi, I., & Fadlil, A. (2020). Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic. *Jurnal Telekomunikasi Dan Komputer*, *10*(2), 111. https://doi.org/10.22441/incomtech.v10i2.8757

Kinasih, R. A., Wirawan Muhammad, A., & Adi Prabowo, W. (2020). Analisis Live Forensics Pada Keamanan Browser Untuk Mencegah Pencurian Akun (Studi Kasus: Facebook dan Instagram). *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, *11*(2), 174–185. https://doi.org/10.31849/digitalzone.v11i2.4678

Muhammad Fathur. (2020). Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen (Tokopedia's Responsibility for the Leakage of Consumers Personal Data). *Procceding: Call for Paper 2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era*, 43–60. http://jurnal.unissula.ac.id/index.php/PH/article/view/1476

Mu'Minin, & Anwar, N. (2020). Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome , Mozilla Firefox , Opera Mode Incognito). *Busiti*, *1*(3), 1–9.

Purnama, N. I., & Putri, L. P. (2021). Analisis Penggunaan E-Commerce Di Masa Pandemi. *Seminar Nasional Teknologi Edukasi Sosial Dan Humaniora*, *1*(1), 556–561. http://jurnal.ceredindonesia.or.id/index.php/sintesa/article/view/357

Putri, A. S., & Zakaria, R. (2020). Analisis pemetaan e-commerce terbesar di indonesia berdasarkan model kekuatan ekonomi Digital. *Seminar Dan Konferensi Nasional IDEC*, *1*(November), 1–14.

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij). *Elinvo (Electronics, Informatics, and Vocational Education)*, *3*(1), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

Rizki Setyawan, M., Hermansa, H., & Fadli Hasa, M. (2022). Analisis Forensik Digital Pada Skype Berbasis Windows 10 Menggunakan Framework Acpo. *Jurnal Ilmiah Betrik*, *13*(2), 111–119. https://doi.org/10.36050/betrik.v13i2.469

Setiawan, N., Pratama, A. R., & Ramadhani, E. (2022). Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, *7*(1), 1–9. https://doi.org/10.32528/justindo.v7i1.5356

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

Yahya, A. Z., Dirman, Buru, D. J., & Sugiantoro, B. (2022). Analisis Bukti Digital Pada Random Access Memory Android Menggunakan Metode Live Forensic Kasus Penjualan Senjata Illegal. *Cyber Security Dan Forensik Digital*, *5*(1), 6–11. https://doi.org/10.14421/csecurity.2022.5.1.1724

Zuhriyanto, I., Yudhana, A., & Riadi, I. (2018). Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics. *Seminar Nasional Informatika 2008 (SemnasIF 2008)*, *2018*(November), 86–91.