JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 2, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i2.6108

ANALISIS MEMORI FORENSIK PADA APLIKASI TIKTOK BERBASIS WEB MENGGUNAKAN METODE *NATIONAL INSTITUTE OF JUSTICE* (*NIJ*)

Aditya Primukti[1], Putri Kartika Sari[2], Didit Suhartono[3*], Khairunnisak Nur Isnaini[4]

[1,2,3,4]Universitas Amikom Purwokerto; Jl. Letjend Pol. Soemarto No.127, Watumas, Purwanegara, Kec. Purwokerto Utara, Kabupaten Banyumas, Jawa Tengah; Telp : (0281) 623321

Received: 23 Januari 2025
Accepted: 19 Maret 2025
Published: 14 April 2025

Keywords:

TikTok, analisis memori forensik, website, *National Institute of Justice* (*NIJ*), Jejak Digital.

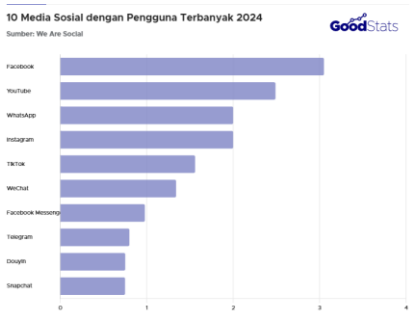
Corespondent Email:
didit@amikompurwokerto.ac.id

Kemajuan teknologi dalam penggunaan aplikasi berbasis web, seperti TikTok, meningkatkan kebutuhan akan analisis forensik digital untuk mengungkap jejak aktivitas pengguna. Penelitian ini bertujuan untuk menganalisis memori forensik pada aplikasi TikTok berbasis web menggunakan metode National Institute of Justice (NIJ), dengan bantuan perangkat lunak FTK Imager 4.7.1 dan HxD. Proses analisis dilakukan untuk mengidentifikasi informasi penting yang tersimpan dalam memori aplikasi selama sesi penggunaan. Hasil analisis menunjukkan bahwa data browser dari situs TikTok dengan alamat https://www.tiktok.com mengungkap beberapa informasi penting, seperti nomor telepon yang digunakan untuk *login*, riwayat pencarian pengguna, dan nama pengguna (*username*) yang aktif selama sesi akses. Namun, data sensitif seperti kode OTP tidak ditemukan, menunjukkan adanya langkah keamanan yang diterapkan TikTok untuk melindungi informasi autentikasi. Temuan ini memberikan gambaran tentang jejak digital yang dihasilkan oleh aplikasi TikTok berbasis web dan langkah-langkah keamanan yang diterapkan. Penelitian ini merekomendasikan agar pengguna tetap menggunakan browser yang aman dan terkini, sementara pengembang aplikasi seperti TikTok terus memperkuat keamanan data, termasuk mencegah penyimpanan informasi sensitif pada sesi browser. Dengan pendekatan ini, analisis forensik memori dapat digunakan sebagai alat yang efektif dalam investigasi digital.

Technological advances in the use of web-based applications, such as TikTok, increase the need for digital forensic analysis to reveal traces of user activity. This research aims to analyze forensic memory in the web-based TikTok application using the National Institute of Justice (NIJ) method, with the help of FTK Imager 4.7.1 and HxD software. The analysis process was carried out to identify important information stored in the application's memory during the usage session. The results of the analysis showed that browser data from the TikTok site with the address https://www.tiktok.com revealed some important information, such as the phone number used for login, the user's search history, and the username that was active during the access session. However, sensitive data such as OTP codes were not found, suggesting that TikTok has security measures in place to protect authentication information. These findings provide an overview of the digital footprint generated by the web-based TikTok app and the security measures implemented. The research recommends that users continue to use secure and up-to-date browsers, while app developers like TikTok continue to strengthen data security, including preventing the storage of sensitive information in browser sessions. With this approach, memory forensic analysis can be used as an effective tool in digital investigations.

1. PENDAHULUAN

Penggunaan media sosial terus mengalami peningkatan signifikan seiring dengan digitalisasi global yang semakin dalam. Tercatat pada Januari 2024, jumlah pengguna media sosial di seluruh dunia mencapai sekitar 5,04 miliar orang, atau sekitar 62,3% dari total populasi global. Angka ini menunjukkan peningkatan sebesar 75 juta pengguna dibandingkan akhir tahun 2023[1]. Tren ini juga mencakup popularitas platform seperti TikTok, yang terus berkembang pesat dan menarik perhatian pengguna muda di seluruh dunia, menjadikanya sosial media favorit di peringkat kelima setelah *WhatsApp*, *Facebook*, *YouTube*, dan *Instagram*[2].



Gambar 1. 10 Media Sosial dengan Pengguna Terbanyak 2024

TikTok adalah platform media sosial sekaligus layanan berbagi video musik yang berasal dari Tiongkok dan diluncurkan pada September 2016[3]. Sebagai salah satu media sosial terkemuka, platform ini dilaporkan memiliki lebih dari 1,6 miliar pengguna aktif bulanan pada tahun 2023, menjadikannya salah satu aplikasi terpopuler, terutama di kalangan anak muda[4]. TikTok menawarkan layanan berbasis aplikasi seluler dan web. TikTok versi web menjadi pilihan bagi pengguna yang ingin mengakses platform tanpa perlu mengunduh aplikasi. Akses melalui browser menawarkan kemudahan untuk pengguna perangkat dengan penyimpanan terbatas atau yang hanya membutuhkan akses sesaat. Beberapa fitur TikTok pada browser yaitu mencakup pencarian video, unggah konten, hingga pengelolaan akun, mirip dengan aplikasi seluler. Sebelum mengakses fitur tertentu, pengguna diharuskan untuk melakukan otentikasi melalui kredensial akun yang disediakan, seperti alamat email, nomor telepon, atau akun media sosial lainnya. Setelah proses otentikasi selesai, pengguna dapat mengakses fitur platform yang dilindungi.

Namun, seperti pada layanan berbasis web lainnya, data yang dimasukkan pengguna ke TikTok, seperti kredensial *login*, metadata video, hingga informasi interaksi, secara otomatis tersimpan sementara di memori volatil (*RAM*) perangkat pengguna selama sesi aktif[5]. *Volatile memory*, menyimpan data untuk akses cepat selama sesi, tetapi akan kehilangan semua data ketika perangkat kehilangan daya. Berbeda dengan non-volatil, Baik dalam kondisi hidup maupun mati tidak menyebabkan data tersebut hilang[6].

Data yang tersimpan sementara di *RAM* menghadirkan sejumlah ancaman keamanan yang perlu diperhatikan, terutama jika data tersebut mencakup informasi sensitif seperti kredensial login atau metadata pengguna. Salah satu ancamannya adalah *memory scraping malware*[7]. *Memory scraping malware* merupakan ancaman siber yang memindai memori komputer untuk mencuri data sensitif yang sedang diproses, seperti kata sandi, informasi kartu kredit, dan kunci enkripsi. Menurt [8] *memory scraping malware* adalah metode ekstraksi data pribadi dari memori yang tersisa setelah proses dihentikan, yang dapat mengekspos informasi sensitif yang tidak terlindungi, Dimana Ancaman ini berbahaya karena dapat mengekstrak data langsung dari *RAM*, yang seharusnya bersifat sementara, sebelum perangkat dimatikan. Selain itu ketika pengguna tidak menyadari bahwa data tersebut masih dapat diakses oleh pihak ketiga yang berpotensi jahat. Misalnya, jika seseorang mengakses TikTok melalui komputer publik, data yang tersimpan di *RAM* dapat dieksploitasi oleh pengguna lain setelah sesi selesai, sebelum memori tersebut ditimpa atau perangkat dimatikan. Oleh karena itu, meskipun RAM bersifat sementara dan kehilangan data saat daya mati, potensi kebocoran informasi sensitif selama sesi aktif tetap menjadi risiko yang harus diperhatikan oleh pengguna media sosial.

Untuk menyelesaikan masalah ini, diperlukan analisis mendalam terhadap memori forensik dengan menggunakan Metode National Institute of Justice (NIJ). Proses ini

mencakup tahapan identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan[9]. Metode *NIJ* dipilih karena menyediakan kerangka kerja forensik yang standar dan konsisten, memungkinkan langkah-langkah penelitian dilakukan secara sistematis dan menjadi panduan dalam menyelesaikan permasalahan yang dihadapi.[10].

Adapun beberapa penelitian terdahulu yang membahas tentang memori forensik yaitu penelitian yang dilakukan oleh [11]. Penelitian ini membahas penerapan *memory forensic* dengan menggunakan metode *live forensic*. Hasilnya menunjukkan bahwa investigasi terhadap data volatile di RAM dapat mengungkap berbagai aktivitas pengguna yang terekam, termasuk log dari aktivitas tersebut. Informasi yang diperoleh dari investigasi ini dapat digunakan sebagai bukti dalam penyidikan, serta memberikan data tentang penggunaan sistem, seperti nama komputer, waktu operasional, dan aplikasi yang digunakan.

Penelitian terdahulu yang dilakukan oleh [12]. Penelitian mengungkapkan jejak aktivitas pengguna yang tersimpan dalam *RAM* tidak hanya penting untuk analisis teknis tetapi juga memiliki implikasi hukum. Data tersebut dapat digunakan sebagai bukti dalam pengadilan untuk mendukung atau membantah klaim tertentu terkait aktivitas digital pengguna. Dengan demikian, pemahaman mendalam tentang cara kerja *RAM* dan teknik forensik digital menjadi semakin penting dalam konteks keamanan siber dan hukum.

Penelitian yang dilakukan oleh [13]. Penelitian menunjukkan bahwa analisis memori forensik pada keamanan browser seperti Google Chrome, Mozilla Firefox, dan Microsoft Edge sangat penting, terutama dalam mengidentifikasi data *volatile* yang tersimpan di *Random Access Memory* (*RAM*). Data *volatile*, seperti *username*, *password*, dan aktivitas sistem yang sedang berjalan, hanya dapat diakses saat sistem masih aktif, sehingga membutuhkan teknik analisis khusus. Kemampuannya untuk merekam semua aktivitas komputer, termasuk data sensitif, menjadikannya elemen krusial dalam penyelidikan keamanan digital, terutama dalam kasus yang melibatkan ancaman terhadap privasi dan data pengguna.

Penelitian yang dilakukan oleh [14]. Penelitian ini menerapkan metode NIJ yang mencakup tahapan persiapan, pengumpulan, pemeriksaan, analisis, dan pelaporan untuk memperoleh bukti digital dari aplikasi Instagram Messenger yang digunakan pada perangkat Android. Data berupa gambar dan percakapan yang terkait dengan kasus *cyberbullying* berhasil diperoleh menggunakan aplikasi *OXYGEN* forensik. Penelitian ini menyoroti pentingnya forensik digital dalam mengungkap bukti dari perangkat mobile untuk mendukung investigasi hukum terkait kejahatan dunia maya. Hasil penelitian menunjukkan bahwa perangkat yang telah di-root mampu memberikan data yang lebih lengkap dibandingkan perangkat yang belum di-*root*.

Penelitian yang dilakukan oleh [15]. Penelitian mengungkapkan bahwa Memori forensik memainkan peran penting untuk mendapatkan bukti digital, melalui proses *RAM* imaging menggunakan FTK Imager untuk mendapatkan data *volatile* seperti teks percakapan, gambar, video, *cache*, dan log file yang hanya dapat diakses saat perangkat masih aktif. Penelitian ini bertujuan untuk membuktikan kasus penipuan transaksi elektronik dengan menganalisis data memori dari perangkat pelaku dan membandingkannya dengan data yang ada di perangkat korban. Hasil penelitian menunjukkan bahwa memori forensik efektif dalam menghasilkan bukti digital yang relevan dan sah secara hukum, sesuai dengan ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Berdasarkan Penelitian terdahulu diatas menunjukkan bahwa memori *RAM* ini dapat menyimpan jejak aktivitas pengguna, termasuk pola penggunaan, log aktivitas, hingga kredensial yang dapat digunakan untuk mengungkap akses tidak sah atau sebagai alat bukti dalam kasus hukum. Misalnya, data seperti *timestamp* dan metadata pengguna dapat membantu dalam pengungkapan tindak kejahatan berbasis platform media sosial[16]. Kerentanan dalam memori volatil membuka peluang bagi penyelidikan lebih lanjut, baik untuk tujuan investigasi kriminal maupun peningkatan keamanan platform berbasis web[17].

Penelitian ini akan dianalisis menggunakan langkah-langkah forensik berdasarkan metode

National Institute of Justice[18]. *National Institute of Justice* adalah metode yang digunakan untuk menggambarkan tahapan-tahapan dalam penelitian, sehingga alur penelitian dapat diselesaikan secara sistematis dan menjadi panduan dalam mengatasi permasalahan yang ada[19]. Dengan menerapkan langkah-langkah Metode *National Institute of Justice* mencakup *identification*, *collection*, *Examination*, *analysis*, dan *reporting*, kemudian dikombinasikan dengan tools seperti FTK Imager dan HxD untuk menganalisis data dari memori sistem secara mendalam. FTK Imager akan digunakan untuk melakukan akuisisi bukti digital dengan mengambil snapshot memori ram dari komputer, sementara HxD akan digunakan untuk menganalisis dan mencari bukti digital dalam format heksadesimal. Tujuan penelitian ini adalah untuk mengidentifikasi jejak aktivitas yang mencurigakan atau bukti relevan dalam aplikasi TikTok yang berbasis web, guna memastikan integritas serta keamanan data pengguna dan memberikan dasar yang kuat untuk langkah-langkah hukum lebih lanjut.

2. TINJAUAN PUSTAKA

2.1. Digital Forensik

Digital forensik adalah penerapan ilmu dan metode untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi, dan mempresentasikan bukti digital yang berkaitan dengan suatu kasus, guna keperluan rekonstruksi peristiwa dan validitas proses peradilan[20]. Digital forensik Memiliki tujuan untuk membuktikan kejahatan komputer dengan memperoleh bukti digital yang sah[21].

2.2. Memori *RAM*

Menurut [22] Memori *RAM* (*Random Access Memory*) merupakan komponen vital dalam sistem komputer yang berfungsi sebagai tempat penyimpanan sementara bagi data yang sedang diproses. Sifatnya yang *volatile* berarti bahwa data di dalamnya akan hilang ketika daya dimatikan. Sedangkan menurut [23] penyimpanan komputer yang hanya menyimpan datanya saat perangkat diaktifkan. Dapat disimpulkan bahwa Memori *RAM* (*Random Access Memory*) adalah elemen krusial dalam sistem komputer yang berfungsi menyimpan data sementara untuk data yang sedang diproses, dengan sifat *volatile* yang menyebabkan data hilang saat daya dimatikan.

2.3. Memory Forensics

Memory forensic adalah bagian dari digital forensik yang fokus pada analisis data volatile yang terdapat dalam R*andom Access Memory* (*RAM*) sebuah perangkat. Proses ini melibatkan pengambilan "*memory dump*," yang merupakan snapshot dari memori saat perangkat sedang berjalan, dan menganalisis output tersebut untuk menemukan bukti terkait aktivitas pengguna, malware, atau serangan siber[24]. Memori forensik dapat mengumpulkan data secara real-time yang berkaitan dengan sistem operasi, serta mengekstraksi berbagai jenis informasi dari memori, termasuk proses memori, *image identification*, *networking*, *registry*, (dll)[25].

2.4. Data *Volatile*

Data volatile atau data sementara adalah data yang hanya ada saat komputer dalam keadaan menyala, dan akan hilang ketika komputer dimatikan. Data volatile ini mengandung informasi penting seperti nama pengguna, kata sandi, file yang diakses, file yang dimodifikasi, aplikasi yang digunakan, serta kata kunci pencarian[26]. Data Volatile yang ada di ram sangat berharga untuk keperluan forensik, karena RAM pada sistem komputer mencerminkan seluruh aktivitas yang telah terjadi di sistem tersebut[27].

2.5. FTK Imager

FTK Imager adalah perangkat lunak forensik digital yang memanfaatkan teknologi statis, real-time, atau keduanya dalam proses investigasi. dirancang khusus untuk mengakuisisi dan membuat citra forensik dari berbagai jenis media digital[28]. Salah satu fitur utama FTK Imager adalah fitur "*Capture Memory*," yang memungkinkan untuk mengambil snapshot dari memori volatile (RAM)[29].

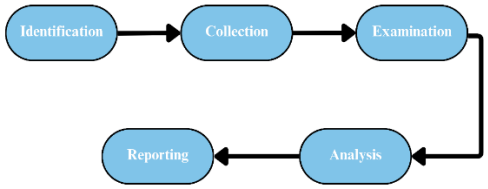
2.6. HxD

Menurut [30] HxD adalah alat *Hex Editor* yang memungkinkan pengguna melihat, mencari dan mengedit nilai heksadesimal dari file yang Dikembangkan oleh Maël Hörz, dirancang untuk sistem operasi *Windows*. Editor heksadesimal ini digunakan untuk membuka hasil *memory dump*, membaca dan mencari pola tertentu dalam data mentah[31] .

3. METODE PENELITIAN

Penelitian ini mengadopsi dan menerapkan metode analisis forensik dari

National Institute of Justice (*NIJ*). Metode ini bertujuan untuk menjelaskan tahapan-tahapan dalam penelitian, sehingga alur dan langkah-langkah penelitian dapat dipahami secara sistematis dan digunakan sebagai pedoman dalam menyelesaikan permasalahan. Tahapan penelitian ini adalah sebagai berikut:



Gambar 2. Tahapan Metode *National Institute of Justice*

3.1. Identification

Penelitian dimulai dengan Identifikasi (*Identification*) perangkat yang digunakan untuk mengakses aplikasi TikTok versi web. Perangkat yang digunakan diidentifikasi untuk memastikan bahwa memori yang akan dianalisis relevan dengan tujuan penelitian. Proses ini melibatkan persiapan perangkat uji, seperti komputer dengan browser aktif, serta konfigurasi aplikasi TikTok berbasis web untuk simulasi aktivitas pengguna, termasuk login dan penelusuran konten. Langkah ini bertujuan untuk memetakan sumber data yang potensial.

3.2. Collection

Tahap berikutnya adalah Pengumpulan Data (*Collection*) Pada tahap ini, alat FTK Imager digunakan untuk mengambil snapshot memori (*RAM*) dari perangkat yang digunakan dalam simulasi. Pengumpulan data dilakukan setelah pengguna menjalankan aktivitas tertentu pada TikTok berbasis web, seperti login dan melihat konten. FTK Imager akan membuat file dump memori yang berisi data sementara, seperti metadata aktivitas pengguna, log aplikasi, dan potensi kredensial. Proses ini dilakukan dengan menjaga integritas data menggunakan hashing (MD5/SHA1).

3.3. Examination

Setelah data dikumpulkan, dilanjutkan dengan pemeriksaan data, yang melibatkan penggunaan editor heksadesimal HxD. File dump dari FTK Imager dimuat ke HxD untuk melakukan analisis mendalam. Pada tahap ini, dicari pola tertentu seperti string teks atau artefak spesifik yang dihasilkan oleh TikTok, seperti jejak login atau metadata aktivitas pengguna. Pemeriksaan ini juga melibatkan validasi integritas data dengan menggunakan hash MD5 dan SHA1 untuk memastikan bahwa data tetap utuh dan tidak mengalami perubahan selama proses akuisisi.

3.4. Analysis

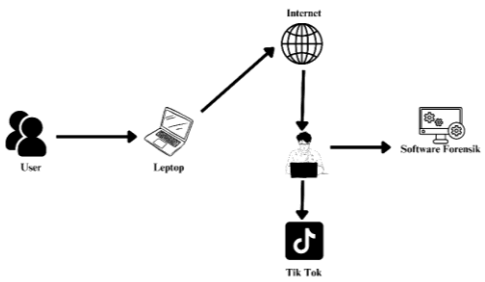
Tahap keempat adalah analisis, di mana data yang telah diperiksa dikategorikan berdasarkan relevansinya terhadap tujuan penelitian. Data yang ditemukan dianalisis untuk memahami pola penyimpanan informasi dalam memori volatil. Analisis ini membantu menjelaskan bagaimana aplikasi TikTok menangani data pengguna, dan potensi risiko yang bisa dieksploitasi oleh pihak yang tidak bertanggung jawab.

3.5. Reporting

Tahapan terakhir adalah pelaporan, di mana hasil penelitian dirangkum dalam bentuk laporan forensik. Laporan ini mencakup semua temuan, mulai dari langkah-langkah pengumpulan data, hasil pemeriksaan memori, hingga interpretasi data yang ditemukan. Laporan ini dirancang untuk menjadi sumber informasi yang berguna bagi praktisi forensik digital dan pengembang aplikasi dalam meningkatkan keamanan data pada platform berbasis web.

4. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan dengan melakukan simulasi aktivitas pada aplikasi TikTok yang berbasis web untuk menganalisis data yang tersimpan di memori komputer. Peneliti melakukan akuisisi memori (RAM) dengan menggunakan aplikasi FTK Imager. File hasil akuisisi yang disimpan dalam format *.raw kemudian diproses lebih lanjut menggunakan Tools HxD. Alur simulasi dapat dilihat pada gambar di bawah ini.



Gambar 3. Alur Simulasi Peristiwa Penelitian

Berdasarkan Gambar 3, Penelitian dimulai dengan Pengguna menyalakan komputer yang terhubung ke internet. Setelah komputer menyala, sistem operasi akan memuat dan pengguna dapat melihat desktop. Koneksi internet yang stabil sangat penting agar pengguna dapat mengakses berbagai layanan online, termasuk Tiktok versi web.

Setelah komputer berfungsi dengan baik, langkah berikutnya adalah membuka Google Chrome. Di bilah alamat, pengguna dapat langsung memasukkan URL TikTok (www.tiktok.com) di bilah alamat dan menekan Enter. Proses ini akan membawa pengguna ke situs resmi TikTok, di mana mereka dapat menemukan berbagai fitur seperti versi mobile. Meskipun fitur tertentu mungkin terbatas, TikTok Web tetap menawarkan aksesibilitas dan kenyamanan bagi pengguna yang lebih memilih menggunakan komputer.

Setelah berhasil mengakses TikTok versi web, pengguna dapat mulai berinteraksi dengan aktifitas Login, melakukan pencarian, Mengirim Pesan, dan menonton beberapa video.

Selanjutnya FTK Imager digunakan untuk mengambil snapshot memori (*RAM*) dari perangkat yang digunakan dalam simulasi. Proses ini dimulai dengan menjalankan perangkat lunak FTK Imager pada komputer yang telah dikonfigurasi untuk akuisisi memori. Pengguna memilih opsi "Capture Memory" dari menu File untuk memulai proses pengambilan gambar memori. Setelah itu, pengguna menentukan perangkat memori yang akan dianalisis, seperti *RAM* komputer, sebagai sumber data. Lokasi penyimpanan file dump dan format file yang sesuai, seperti RAW atau E01, juga ditentukan pada tahap ini. Selama proses akuisisi, FTK Imager melakukan hashing pada file hasil akuisisi menggunakan algoritma MD5 atau SHA1 untuk memastikan integritas data tetap terjaga. Hasil dump yang telah selesai dibuat kemudian digunakan sebagai bahan utama untuk analisis data di tahap berikutnya. Dalam konteks ini, FTK Imager akan membuat file *dump* memori yang berisi data sementara, termasuk metadata aktivitas pengguna, log aplikasi, dan potensi kredensial.

Setelah mendapatkan file *dump* memori, tahap berikutnya adalah pemeriksaan data menggunakan editor heksadesimal HxD. HxD digunakan untuk membaca dan menganalisis file dump yang dihasilkan oleh FTK Imager. File dump tersebut dimuat ke dalam HxD, di mana pengguna dapat memanfaatkan fitur pencarian untuk menemukan pola data tertentu, seperti string teks, metadata, atau artefak spesifik yang terkait dengan aktivitas TikTok. Proses ini memungkinkan identifikasi data sensitif yang tersembunyi di dalam memori, termasuk informasi login atau aktivitas pengguna.

4.1. Identification

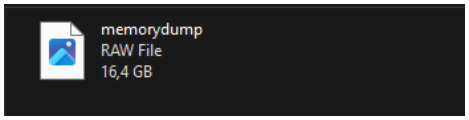
Identification bertujuan untuk mempersiapkan bukti digital yang mendukung proses identifikasi dalam kasus kejahatan digital. Berikut ini adalah alat dan bahan yang digunakan dalam penelitian ini:

Table 1. Hasil Identifikasi Alat

No	Alat Dan Bahan	Keterangan
1	Laptop	HP 14s-fq2002AU dengan prosesor AMD Ryzen 5 5625U, RAM 16 GB, SSD 512 GB, dan sistem operasi Windows 11 Home
2	Chrome	Aplikasi browser yang digunakan untuk mengakses TikTok berbasis web.
3	Ftk imager	Perangkat lunakyang digunakan untuk melakukan akuisisi memori pada sistem operasi Windows
4	HxD	Editor hexadecimal yang digunakan untuk membuka dan menganalisis file .raw hasil akuisisi.

4.2. Collection

Pada tahap *Collection*, bukti digital berupa data atau file yang relevan dikumpulkan dari objek yang diduga terkait kasus kejahatan digital. Dalam penelitian ini, barang bukti yang dikumpulkan adalah hasil akuisisi memori dari laptop yang digunakan untuk mengakses aplikasi TikTok berbasis web. File hasil akuisisi disimpan dalam format *.raw untuk dianalisis lebih lanjut.

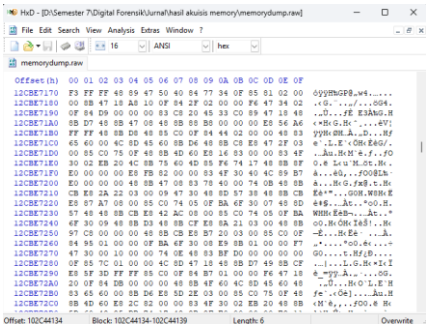


Gambar 4. Hasil *Capture memrory* menggunakan FTK Imager

4.3. Examination

Examination adalah proses analisis terhadap bukti digital yang diperoleh dari tahap Collection. Pemeriksaan dilakukan secara manual maupun otomatis terhadap file .raw yang dihasilkan.

Proses akuisisi data merupakan langkah awal untuk mendapatkan file mentah (.raw) yang mengandung informasi aktivitas TikTok. Hasil dari proses ini berupa file mentah yang kemudian dibuka menggunakan aplikasi HxD untuk dianalisis lebih mendalam. Berikut adalah contoh hasil file .raw yang diperoleh:

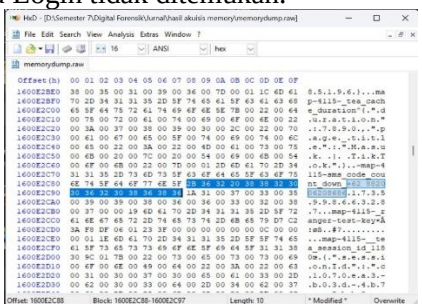


Gambar 5. File .raw dibuka menggunakan HxD

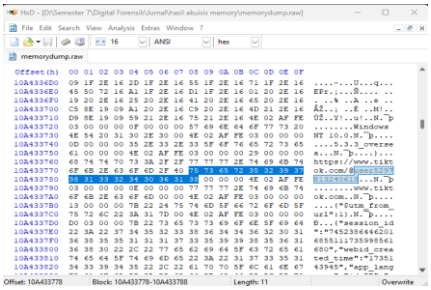
4.4. Analysis

Analysis dilakukan untuk menganalisis bukti digital yang diperoleh dari tahap Examination. Proses analisis menggunakan metode yang sah secara teknis dan hukum untuk memastikan bahwa data yang ditemukan valid dan dapat dipertanggungjawabkan. Pada tahap ini, metode keyword search digunakan untuk mencari string tertentu dalam file .raw. Jika string yang dicari ditemukan, akan di catat sesuai dengan pola penulisan.

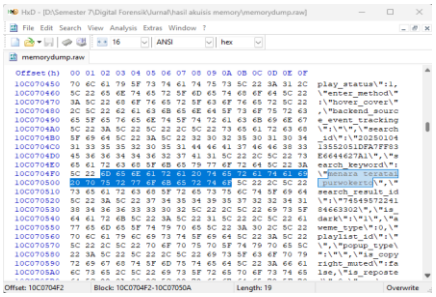
Hasil analisis memori forensik terhadap data browser yang dikumpulkan dari situs TikTok dengan alamat https://www.tiktok.com ditemukan sejumlah informasi penting, yaitu nomor telepon yang digunakan untuk login, beberapa riwayat pencarian yang dilakukan oleh pengguna, serta nama pengguna (username) yang sedang aktif saat akses berlangsung. Namun kode OTP pengguna ketika Login tidak ditemukan.



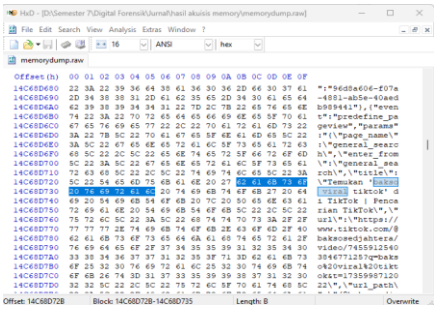
Gambar 6. Nomor telepon yang digunakan untuk login



Gambar 7. Username pengguna tiktok yang berhasil login



Gambar 8. Catatan pencarian yang dilakukan oleh pengguna



Gambar 9. Catatan pencarian yang dilakukan oleh pengguna

4.5. Reporting

Reporting dilakukan setelah proses pemeriksaan dan analisis selesai. Pada tahap ini, hasil analisis disusun dalam sebuah laporan yang mencakup ilustrasi proses yang dilakukan,

seperti penggunaan alat, metode atau kerangka kerja yang diterapkan, langkah-langkah pendukung yang diambil, rekomendasi perbaikan kebijakan, serta alat atau komponen tambahan yang digunakan dalam proses forensik digital.

Hasil pemeriksaan pada aplikasi TikTok berbasis web dengan metode Key Search mengungkapkan data-data sebagai berikut:

Table 2. Hasil Keyword "Search"

No	Kategori Data	Detail Informasi	Keterangan
1	Nomor Telepon	Nomor telepon yang digunakan untuk login	Ditemukan
2	Riwayat Pencarian	Beberapa pencarian yang dilakukan oleh pengguna	Ditemukan
3	Nama Pengguna	Nama Pengguna (username) yang sedang aktif	Ditemukan
4	Kode OTP	Kode OTP untuk Login	Tidak Ditemukan

5. KESIMPULAN

a. Dengan menggunakan metode *NIJ* (*National Institute of Justice*) dan bantuan perangkat lunak FTK Imager 4.7.1 dan HxD. Proses analisis TikTok berbasis web ini berhasil mengidentifikasi sejumlah informasi penting, seperti nomor telepon yang digunakan untuk login, riwayat pencarian yang dilakukan oleh pengguna, dan nama pengguna (*username*) yang aktif selama sesi akses. Namun, data yang bersifat sensitif seperti kode *OTP* (*One-Time Password*) tidak ditemukan dalam hasil analisis. Temuan ini mengindikasikan bahwa TikTok menerapkan langkah-langkah keamanan tertentu, seperti mengenkripsi atau mencegah penyimpanan kode OTP dalam sesi browser.

b. Sebagai langkah mitigasi keamanan, pengguna disarankan untuk selalu menggunakan browser versi terbaru dan mengaktifkan pengaturan keamanan tambahan seperti mode penjelajahan aman (*secure browsing*). Selain itu, penyedia layanan seperti TikTok perlu terus meningkatkan perlindungan terhadap data pengguna dengan memastikan tidak ada informasi sensitif yang tersimpan di *cache* atau log *browser*.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih yang sebesar-besarnya kepada keluarga tercinta atas doa dan dukungannya, dosen pembimbing atas arahan dan bimbingannya, serta semua pihak yang telah memberikan dukungan dan kontribusi selama proses penelitian ini. Berkat dukungan tersebut, penelitian yang berjudul "Analisis Memori Forensik pada Aplikasi TikTok Berbasis Web Menggunakan Metode *National Institute of Justice* (*NIJ*)" ini dapat diselesaikan dengan baik.

DAFTAR PUSTAKA

[1] S. Kemp, "5 billion social media users," DataReportal – Global Digital Insights. [Online]. Available: https://datareportal.com/reports/digital-2024-deep-dive-5-billion-social-media-users

[2] Agnes Z. Yonatan, "10 Media Sosial dengan Pengguna Terbanyak 2024," GoodStats Data. [Online]. Available: https://data.goodstats.id/statistic/10-media-sosial-dengan-pengguna-terbanyak-2024-CaJT1

[3] Y. Fitriani, "Pemanfaatan Media Sosial Sebagai Media Penyajian Konten Edukasi Atau Pembelajaran Digital," *J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 5, no. 4, pp. 1006–1013, 2021, doi: 10.52362/jisamar.v5i4.609.

[4] David Curry, "TikTok App Report 2024 Holistic overview of the most popular app of past three years," bussines off Apps. [Online]. Available: https://www.businessofapps.com/data/tiktok-

report/
[5] M. A. Yaqin, T. A. Cahyanto, and N. Q. Fitriyah, "Metode Live Memory Acquisition untuk Pencarian Artefak Digital Perangkat Memori Laptop Berdasarkan Simulasi Kasus Kejahatan Siber," *BIOS J. Teknol. Inf. dan Rekayasa Komput.*, vol. 2, no. 2, pp. 87–94, 2021, doi: 10.37148/bios.v2i2.28.
[6] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.
[7] Drajad Wiryawan, "Ancaman Tersembunyi – Memory Scraping Malware," BINUS UNIVERSITY. [Online]. Available: https://sis.binus.ac.id/2024/06/12/ancaman-tersembunyi-memory-scraping-malware/
[8] B. Madabhushi, S. Kundu, and D. Holcomb, "Memory Scraping Attack on Xilinx FPGAs: Private Data Extraction from Terminated Processes," *Proc. -Design, Autom. Test Eur. DATE*, 2024, doi: 10.23919/date58400.2024.10546527.
[9] S. Soni, Y. Fatma, and R. Anwar, "Akuisisi Bukti Digital Aplikasi Pesan Instan 'Bip'Menggunakan Metode National Institute Of Justice (NIJ)," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 1, pp. 34–42, 2022, doi: 10.37859/coscitech.v3i1.3694.
[10] H. Hajar, H. Hermansa, and I. Ilcham, "Investigasi Stego File Menggunakan Framework National Institute of Justice," *CONTEN Comput. Netw. Technol.*, vol. 4, no. 1, pp. 31–42, 2024, doi: 10.31294/conten.v4i1.3527.
[11] M. Rifkiansyah, R. Wibowo, … R. P.-, and undefined 2021, "Penerapan Memory Forensic Menggunakan Metode Live Forensic untuk Investigasi Random Access Memory," *Conference.Upnvj.Ac.Id*, vol. 7, no. 1, pp. 531–542, 2022, [Online]. Available: https://conference.upnvj.ac.id/index.php/senamika/article/view/1422
[12] S. Mufti Prasetiyo *et al.*, "Manajemen Penyimpanan Sementara (RAM) Dan Pengelolaannya," vol. 2, no. 1, pp. 145–149, 2024, [Online]. Available: https://jurnalmahasiswa.com/index.php/biikma
[13] R. A. Kinasih, A. Wirawan Muhammad, and W. Adi Prabowo, "Analisis Live Forensics Pada Keamanan Browser Untuk Mencegah Pencurian Akun (Studi Kasus: Facebook dan Instagram)," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 174–185, 2020, doi: 10.31849/digitalzone.v11i2.4678.
[14] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute of Justice (NIJ)," *Akuisisi Bukti Digit. Pada Instagram Messenger Berbas. Android Menggunakan Metod. Natl. Inst. Justice*, vol. 4, pp. 219–227, 2018.
[15] S. D. Utami, C. Carudin, and A. A. Ridha, "Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.
[16] K. Gupta, D. Oladimeji, C. Varol, A. Rasheed, and N. Shahshidhar, "A Comprehensive Survey on Artifact Recovery from Social Media Platforms: Approaches and Future Research Directions," *Inf.*, vol. 14, no. 12, 2023, doi: 10.3390/info14120629.
[17] G. K.-J. of I. and Advanced and undefined 2023, "Implementasi Volatility dalam Mengalanalisa Malware pada Memory Dump," *Journal.Univpancasila.Ac.Id*, vol. 4, no. 1, pp. 36–43, 2023, [Online]. Available: https://journal.univpancasila.ac.id/index.php/jiac/article/view/5491
[18] D. D. Hutagalung, C. Hanifurohman, and D. R. Baskhara, "Analisa Forensik Memori pada Aplikasi E-Commerce Berbasis Web Menggunakan Metode National Institute of Justice (NIJ)," *J. Teknol. Sist. Inf. dan Apl.*, vol. 6, no. 2, pp. 135–146, 2023, doi: 10.32493/jtsi.v6i2.31535.
[19] F. M. Kaffah, S. Nur, A. Fitrianto, U. Syaripudin, and D. Darwan, "Analisis Live Forensics Pada SSD SATA Fungsi Trim Menggunakan Metode National Institute Of Justice (NIJ)," *Teknol. Nusant.*, vol. 4, no. 2, pp. 21–33, 2022, [Online]. Available: http://ojs.uninus.ac.id/index.php/teknologinusantara
[20] R. M. Muria, A. Muntasa, M. Yusuf, and A. Hamzah, "Studi Litelatur: Peningkatan Kinerja Digital Forensik Dan Pencegahan Cyber Crime," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 3, no. 1, pp. 12–20, 2022, doi: 10.31102/jatim.v3i1.1422.
[21] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," *J. Repos.*, vol. 2, no. 10, pp. 1400–1405, 2020, doi: 10.22219/repositor.v2i10.1066.
[22] P. Periyadi, R. Hikmawan, and G. A. Mutiara, "Forensik Digital Random Access Memory Pada Sistem Operasi Linux Digital Forensic Random Access Memory on Linux Operating

System Using Dumpmemory Method," vol. 3, no. 3, 2017, [Online]. Available: https://libraryeproceeding.telkomuniversity.ac.id/index.php/appliedscience/article/view/9253

[23] F. Bahtiar, N. Widiyasono, and A. P. Aldya, "Memory Volatile Forensik Untuk Deteksi Malware," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 242–253, 2018.

[24] Pitra Winarianto & Raymond Nolasco, "The Branches of Cyber Forensic," BINUS UNIVERSITY. [Online]. Available: https://student-activity.binus.ac.id/csc/2022/10/the-branches-of-cyber-forensic/

[25] Bagas Kurnadi, Fachrul Ali Nurfadillah, and Muhammad Tegar Sabila, "Analisis Memory Forensics Windows Subsystem for Linux 2 (WSL2) Berbasis Hyper-V pada Windows 11 Berdasarkan Nist 800-86," *J. Penelit. Sist. Inf.*, vol. 2, no. 1, pp. 178–188, 2024, doi: 10.54066/jpsi.v2i1.1594.

[26] N. Setiawan, A. R. Pratama, and E. Ramadhani, "Metode Live Forensik Untuk Investigasi Serangan Formjacking Pada Website Ecommerce," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 7, no. 1, pp. 1–9, 2022, doi: 10.32528/justindo.v7i1.5356.

[27] Q. adar BakhshBaloch, "STUDI PERBANDINGAN TEKNOLOGI LIVE FORENSIC UNTUK INVESTIGASI RANDOM ACCESS MEMORY," vol. 11, no. 1, pp. 92–105, 2017.

[28] M. R. D. Qibriya, A. Ambarwati, and K. E. Susilo, "Analisis Forensik Digital Pada Aplikasi Instant Messaging Di Smartphone Berbasis Android Untuk Bukti Digital," *J. Teknol. Inf.*, vol. 5, no. 2, pp. 114–121, 2021, doi: 10.36294/jurti.v5i2.2200.

[29] N. D. Putri, "Analisis Keamanan Menggunakan Metode Live Forensic pada Web," vol. 10, no. 1, pp. 51–66, 2024.

[30] R. H. Zhafrant, "[Digital Forensic] Rahasia Dibalik Sebuah Gambar," Medium. [Online]. Available: https://medium.com/@rifqihz/digital-forensic-rahasia-dibalik-sebuah-gambar-f7d1a3a86f15

[31] E. Daraghmi and A. Hamoudi, "Mobile Forensics : Extracting Geo-Location Data from Photos on Android Smartphones," vol. 9, no. 9, pp. 1915–1921, 2024.