Laman web jurnal: https://ejournal.unama.ac.id/index.php/processor

Jurnal Processor

P-ISSN: 1907-6738 | E-ISSN: 2528-0082

Analisis Forensik Keamanan Data Pribadi pada Mode Privasi Browser Menggunakan Metode National Institute of Standards and Technology (NIST)

Muhammad Syukri[1*], Imam Riadi[2], Tole Sutikno[3]

[1]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta 55191, Indonesia.
[1]Program Studi Teknik Informatika, STMIK Mardira Indonesia, Bandung 40233, Indonesia.
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta 55191, Indonesia.
[3]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta 55191, Indonesia.
*Penulis Korespondensi, Email: 2437083011@webmail.uad.ac.id

Abstrak−Privasi pengguna saat berselancar di internet menjadi perhatian utama, terutama dengan adanya fitur mode privat pada browser yang diklaim dapat melindungi data pribadi. Penelitian ini menganalisis sejauh mana mode privat pada browser Google Chrome dan Mozilla Firefox dapat menjaga keamanan data pribadi dengan pendekatan standar dari National Institute of Standards and Technology (NIST). Empat skenario simulasi dilakukan untuk mengevaluasi efektivitas mode privat dalam mencegah penyimpanan informasi pengguna. Hasil penelitian menunjukkan bahwa meskipun mode privat berhasil mencegah penyimpanan riwayat penelusuran dan data pengguna di hard disk, informasi sensitif seperti akun dan kata sandi tetap dapat diakses dalam memori (RAM) pada kondisi tertentu. Temuan ini mengindikasikan bahwa mode privat belum sepenuhnya aman dalam menjaga privasi pengguna, terutama terhadap serangan yang mengeksploitasi data sementara dalam RAM. Implikasi dari penelitian ini menyoroti perlunya pengembangan lebih lanjut dalam keamanan mode privat, baik oleh pengembang browser maupun pengguna yang ingin meningkatkan perlindungan data pribadi mereka. Penelitian ini juga merekomendasikan strategi tambahan secara lebih efektif, untuk mengurangi risiko kebocoran data saat menggunakan mode privat.

Kata Kunci: Forensik digital; Keamanan data pribadi; Mode privat browser; Metode NIST; Memori RAM.

Abstract−User privacy while browsing the internet has become a major concern, especially with the presence of the private mode feature in browsers, which is claimed to protect personal data. This study analyzes the extent to which private mode in Google Chrome and Mozilla Firefox browsers can safeguard personal data using the standard approach from the National Institute of Standards and Technology (NIST). Four simulation scenarios were conducted to evaluate the effectiveness of private mode in preventing user information from being stored. The research findings indicate that although private mode successfully prevents the storage of browsing history and user data on the hard disk, sensitive information such as accounts and passwords can still be accessed in memory (RAM) under certain conditions. These findings suggest that private mode is not entirely secure in protecting user privacy, particularly against attacks that exploit temporary data in RAM. The implications of this study highlight the need for further development in private mode security, both by browser developers and users who seek to enhance their personal data protection. This study also recommends additional strategies to be implemented more effectively in order to reduce the risk of data leakage when using private mode.

Keywords: Digital forensics; Personal data security; Private browser mode; NIST method; RAM memory.

1. PENDAHULUAN

Gangguan keamanan yang dilakukan oleh para *intruder* untuk mengambil atau merusak data pribadi yang tersimpan pada sebuah *computer server* atau *personal computer* yang terhubung ke jaringan internet semakin marak. Bahkan data pribadi yang ada dalam penyimpanan nasional di negara inipun sempat bocor dan dijual dipasar gelap tentu sangat membutuhkan penanganan yang serius. Keamanan data pribadi memainkan peran penting dalam menurunkan risiko crash saham, terutama bagi perusahaan yang terlibat dalam pengumpulan data digital[1]. Teknik penanganan serangan dengan tujuan membuktikan bahwa para *intruder* ini telah melakukan kegiatan illegal dikenal sebagai forensik digital. Peningkatan keamanan dalam aplikasi web melalui penerapan teknik digital forensik untuk mencegah serangan SQL Injection dengan cara menambahkan SSL dan kode captcha, artikel ini menunjukkan bahwa keamanan login pada website dapat ditingkatkan, sehingga risiko terhadap akses tidak sah melalui SQL Injection dapat diminimalkan[2].

Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025

Alat forensik digital digunakan untuk memudahkan validasi dan deteksi kesalahan dengan output terstandardisasi pada tiap lapisan abstraksi[3]. Metode forensik digital dalam menganalisis tanda tangan online dengan menggunakan teknik biometrik yang menggabungkan lintasan di permukaan dan di udara digunakan untuk meningkatkan akurasi dalam mengidentifikasi pemalsuan dan mempertimbangkan pergerakan pena yang tidak terlihat saat proses penandatanganan, yang dapat membantu dalam analisis forensik tanda tangan[4] dan kejahatan pemalsuan tanda tangan[5]. Forensik digital sangat penting digunakan untuk menganalisis mode pribadi dari berbagai browser pada perangkat Android, meskipun mode pribadi dirancang untuk tidak menyimpan informasi, data seperti kata kunci pencarian dan kredensial login masih dapat ditemukan dalam memori perangkat setelah sesi privat ditutup, menunjukkan tantangan[6]. Analisa forensik digital untuk menilai efektivitas mode privasi pada peramban Mozilla Firefox dan Google Chrome di sistem operasi Linux dilakukan dengan menguji empat lingkungan berbeda, hasil menunjukkan bahwa walaupun mode privasi berhasil mencegah penyimpanan informasi pada hard disk, sejumlah besar informasi terkait aktivitas browsing tetap dapat dipulihkan dari memori (RAM) dalam beberapa kondisi tertentu, terutama saat browser dijalankan di lingkungan virtualisasi[7]. Analisa forensik digital terhadap mode privasi pada berbagai peramban web, meneliti sejauh mana mode privasi ini benar-benar mampu melindungi informasi sesi browsing dari potensi pemulihan data dengan pengujian pada 30 peramban, hasil menunjukkan bahwa sejumlah peramban, termasuk Avant, Comodo Dragon, Edge, Epic, dan Internet Explorer, mengalami "kebocoran" data sesi privasi, yang menunjukkan adanya keterbatasan dalam fitur privasi lokal yang ditawarkan[8]. Analisis forensik digital dalam memastikan keamanan data sensitif, seperti data genomik, dari ancaman pelanggaran yang dapat membahayakan privasi pengguna[9]. Penemuan forensik digital dalam kasus hoax lowongan kerja melalui proses investigasi melibatkan pengumpulan bukti digital menggunakan berbagai alat, seperti Andriller, Root Browser, Autopsy, dan MOBILedit, yang berhasil menemukan bukti berupa log aktivitas, status update, serta data lainnya pada perangkat Android[10]. Peran teknologi kecerdasan buatan dan pembelajaran mesin dalam forensik digital, dengan fokus pada peningkatan efisiensi dan ketepatan investigasi forensik digital serta respons insiden digunakan untuk mengidentifikasi peluang, tantangan, serta arah penelitian masa depan yang berpotensi untuk memperkuat praktik forensik digital dalam menangani kejahatan siber modern[11].

Proses penanganan tindakan kejahatan siber menggunakan analisa forensik telah terbukti dalam kesuksesannya untuk mengumpulkan bukti-bukti tindakan kejahatan tersebut. Selain menggunankan analisa forensic, penelitian yang mengkaji tindakan kejahatan siber juga menggunakan metode NIST yang terdiri dari pengumpulan, pemeriksaan, analisis, dan pelaporan, yang membantu dalam menjaga integritas dan keabsahan bukti digital untuk pembuktian di pengadilan telah ddilakukan untuk mengidentifikasi bukti digital dari Facebook Messenger[12], Android Based Facebook Lite[13], Jaringan Virtual Router[14], Optical Drive[15], Viber Messenger Android[16], pengembalian data[17], dan media social twitter[18]. Metode ini juga dikembangkan dengan cara mengkombinasikannya dengan Teknik dan metode lainnya guna mendapatkan hasil yang lebih optimal dalam mengumpulkan bukti forensik digital. Model ekonomi Gordon-Loeb (GL) dapat diintegrasikan ke dalam NIST untuk menganalisis investasi keamanan siber secara lebih efektif berdasarkan pendekatan biaya-manfaat[19]. Metode investigasi forensik digital NIST telah dibandingkan dengan metode National Institute of Justice (NIJ) dalam konteks analisis MicroSD dengan hasil yang menunjukkan bahwa metode NIST lebih efisien untuk investigasi cepat, sementara metode NIJ menawarkan pendekatan yang lebih komprehensif dan detail[20].

Fasilitas mode privasi sudah banyak digunakan oleh banyak aplikasi browsing internet arus utama seperti Avant, Brave, Chrome, Chromium, Comodo IceDragon, Comdo Dragon, Dooble, Edge, Epic, Falkon, Firefox, GreenBrowser, IE, Konqueror, Links, Lynx, Maxthon, Midori, Netsurf, Opera, Pale Moon, Puffin, Seamonkey, Sleipnir, SlimJet, Tor Browser, Torch, UC Browser, Vivaldi, dan WaterFox dengan kesadaran pengguna tentang fungsi dan tujuannya yang semakin meningkat. Namun perlu dilakukan penelitian lebih lanjut untuk memahami efektivitas dan memastikan privasi data pengguna[21].

2. METODOLOGI PENELITIAN

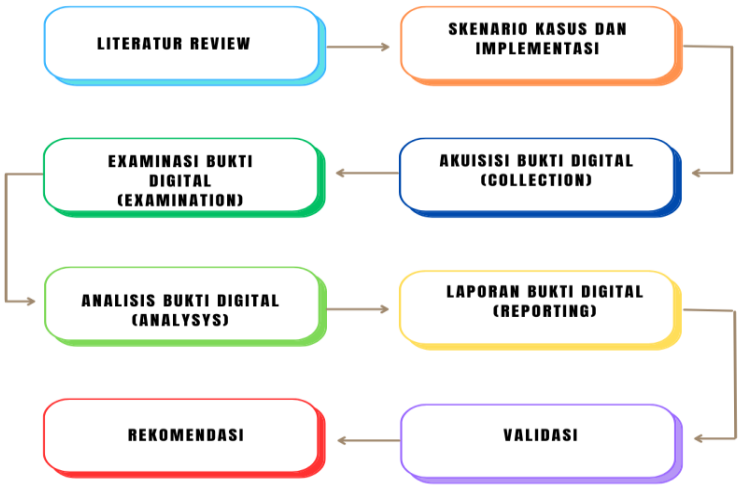
2.1 Tahapan Penelitian

Pada penelitian ini menggunakan metode National Institute of Standard and Technology[20]. Metode ini terdiri dari empat tahap yakni Collection, Examination, Analysis, dan Reporting, seperti yang terlihat di gambar 1.

https://doi.org/10.33998/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025

Gambar 1. Metodelogi Penelitian

Supaya alur penelitian menjadi lebih sistematis sehingga memudahkan dalam penelitian ini maka dibuatkan kerangka kerja penelitian berdasarkan metode gambar 1. Adapun kerangka kerja tersebut disusun dengan 8 tahapan dengan memasukkan metode NIST didalamnya yakni *literatur riview* yaitu melakukan pengumbulan informasi penelitian sebelumnya dari berbagai sumber sebagai rujukan, kemudian melakukan skenario kasus dan menyiapkan alat dan bahan untuk implementasi simulasi kasus. Selanjutnya masuk kedalam tahap metode NIST yaitu *collection* bukti digital yang telah disimulasikan dari data-data yang dihapus sebelumnya. Kemudian melakukan tahap *examinition* yakni tahap pemeriksaan dan pengambilan barang bukti simulasi. Berikutnya adalah tahap *analysis* merupakan tahap analisis secara detil dari hasil akuisisi data. Tahap *reporting* merupakan hasil pelaporan dari tahapan proses sebelumnya. Tahap validasi merupakan tahapan yang memastikan bahwa proses uji forensik yang dilakukan benar, akurat, kredibel dan menjaga integritas data untuk menjadi acuan dalam melakukan pengambilan keputusan [22]. Tahap terakhir adalah rekomendasi untuk menjaga keamanan data pribadi. Pada tahap ini dijelaskan apa saja yang harus dilakukan agar data privasi pada *browser* mode privat dapat terjaga keamanannya dengan memberikan rekomendasi yang dapat dilakukan sejak dini.



Gambar 2. Tahapan Penelitian

2.2 Literatur Riview

Agar penelitian yang dilakukan lebih terpercaya maka perlu dilakukan *literatur review*. Tabel 1 adalah hasil rangkuman penelitian sebelumnya yang sesuai dengan topik penelitian yang dilakukan.

Tabel 1. Hasil Rangkuman Penelitian Sebelumnya

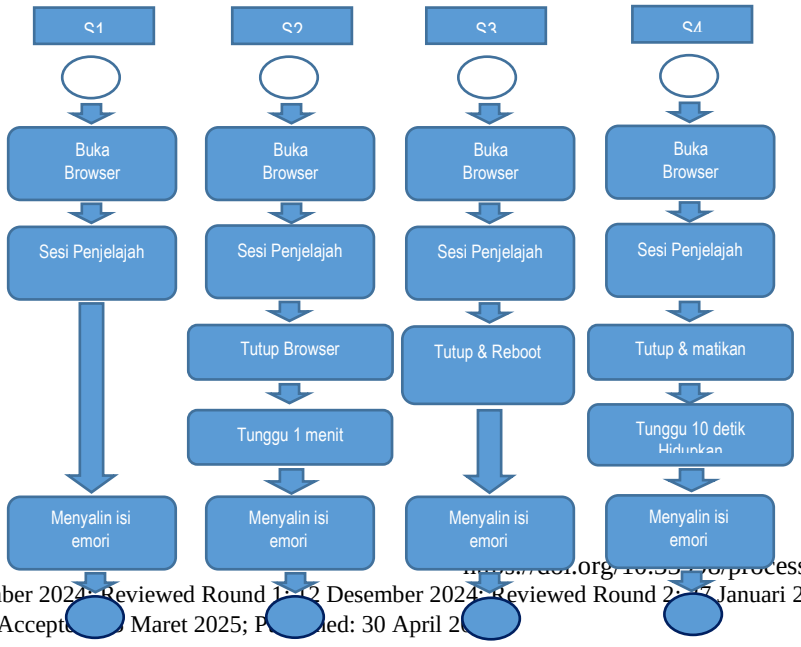
Penulis dan Tahun	Judul Penelitian	Hasil Penelitian	Kelebihan	Kekurangan
Fernández-Fuentes et al., (2022)	Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study	Mode pribadi Firefox dan Chrome mencegah penyimpanan data di hard disk, tetapi hanya Firefox di Linux yang sepenuhnya menghapus data dari memori.	Metode forensik sistematis, bukti data tetap bisa diambil dari RAM, uji di berbagai lingkungan, temuan penting di virtualisasi	Tidak uji OS lain, belum bahas mitigasi enkripsi RAM, fokus hanya di Linux
Fernández-Fuentes et al., (2023)	Digital forensic analysis of the private mode of browsers on	Penelitian menunjukkan bahwa mode privat masih	Menguji mode privat berbagai browser Android dengan perangkat	Hanya fokus pada Android, tidak membahas mitigasi

https://doi.org/10.33998/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025

	Android	menyisakan data sensitif di memori, mengancam privasi karena data bisa diakses kembali bahkan setelah perangkat di-reboot.	fisik dan emulator, menemukan data sensitif masih bisa diambil dari RAM setelah reboot	keamanan lebih lanjut, dan tidak menguji dampak enkripsi RAM
Imam Riadi, Rusydi Umar, dan Muhammad Irwan Syahib (2021)	Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)	Metode NIST efektif untuk akuisisi bukti Viber di Android, dengan MOBILedit dan Belkasoft mencapai 100% kecuali percakapan teks (50%). Autopsy gagal karena tidak ada fitur dekripsi.	Berhasil mengakuisisi bukti digital Viber di Android dengan metode NIST, menggunakan beberapa alat forensik, hasil valid dan bisa diulang	Autopsy gagal mengekstrak data karena keterbatasan dekripsi, hanya fokus pada Android, dan tidak membahas mitigasi keamanan lebih lanjut
Imam Riadi, Rusydi Umar, dan Muhammad Abdul Aziz (2020)	Komparatif Web-based Instant Messaging Vulnerability Menggunakan Metode Association of Chief Police Officers	Penelitian ini membandingkan kerentanan WhatsApp, Telegram, dan Skype berbasis web. Hasilnya, Skype paling rentan (92%), sementara WhatsApp dan Telegram sama-sama rentan (67%) dengan metode ACPO, FTK Imager, dan OSForensic.	Menggunakan metode investigasi terstruktur dan alat forensik canggih	Fokus terbatas dan tidak membahas penyebab kerentanan secara rinci

2.3 Skenario Kasus dan Implementasi

Skenario kasus dilakukan dengan mengacu pada gambar 3.



https://doi.org/10.35746/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 17 Januari 2025; Review Round 3: 07 Februari 2025; Accepted: 03 Maret 2025; Published: 30 April 2025

Gambar 3. Skenario Studi Kasus

Skenario pertama browser dibuka, lakukan penjelajahan situs seperti membuka youtube, mencari gambar, mendownload file, login ke gmail. Lalu disalin isi memori untuk dilakukan analisis. Skenario kedua membuka browser, lalu penjelajahan website youtube, mencari gambar, mendownload file, login ke gmail, tutup browser, tunggu satu menit. Lalu disalin isi memori untuk dilakukan analisis. Skenario ke tiga buka browser, lakukan penjelajahan website youtube, login gmail, mencari gambar, download file, tutup aplikasi browser, dan reboot, lalu lakukan penyalinan isi memori untuk dilakukan analisis. Skenario ke empat buka browser, buka situs youtube, download file, login ke gmail, mencari gambar, tutup browser dan matikan laptop, tunggu 10 detik lalu hidupkan laptop, salin isi memori untuk dilakukan analisis. Pada skenario ke tiga dan ke empat, walaupun dalam kondisi komputer di reboot dan dimatikan tetap menyimpan stamp atau artefak[23].

Tabel 2. Alat Penelitian

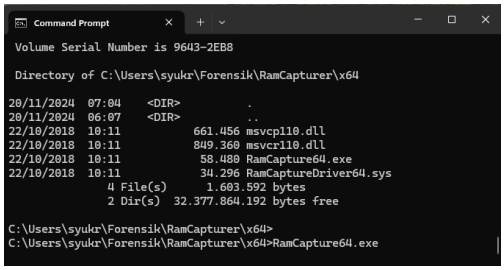
No	Nama Alat	Deskripsi	Ket.
1	Laptop	Lenovo Thinkpad Seri X270 Core i5 Gen 6 RAM 8 GB SSD 256 GB	Peangkat keras
2	Windows	Windows 11 Pro	Sistem Operasi
3	Web Browser	FireFox 132.0.2 (64-bit)	Perambah Situs
4	Web Browser	Google Chrome Version 130.0.6723.119 (Official Build) (64-bit)	Perambah Situs
5	BelkaSoft	RAM Capture	Tools Menyalin isi Memori
6	WinHex	WinHex 21.3	Tools Forensik
7	Volatility Memory Forensic	Volatility Workbench V3.0 Build 1009	Tools Forensik

3. HASIL DAN PEMBAHASAN

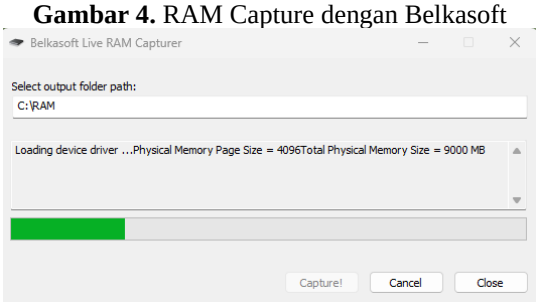
3.1 Akusisi Bukti Digital (*Collection*)

Collection merupakan tahapan awal dari metode NIST yang merupakan tindakan untuk mengamankan barang bukti seperti melakukan koleksi, identifikasi, dan pengambilan data yang diperlukan dengan cara membackup memori menggunakan RAM Capture dengan tahapan skenario yang sudah ditentukan. Pada setiap skenario baik skenario 1 sampai dengan 4, dilakukan forensik digital dengan menggunakan tool forensik Belkasoft, untuk mengakusisi memori dengan melakukan ke empat skenario yang sudah jelaskan sebelumnya untuk mencari bukti digital aplikasi yang berjalan yakni google chrome dan mozila firefox.

https://doi.org/10.33998/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025

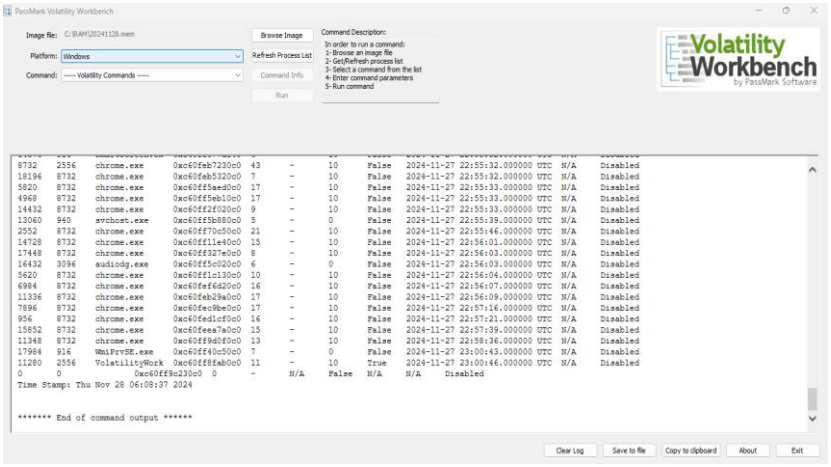


Gambar 4. RAM Capture dengan Belkasoft

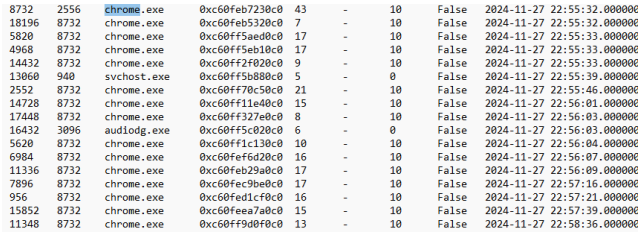


Gambar 5. RAM Capture

Gambar 6. Hasil RAM Capture Skenario



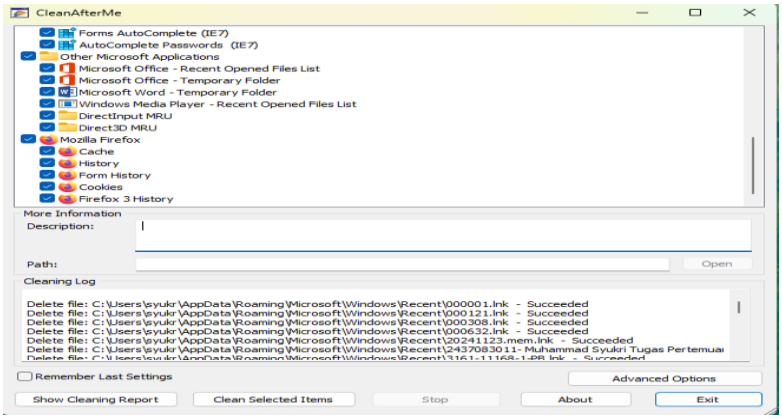
Gambar 7. Hasil Volatility



Gambar 8. Chrome Volatility

Dengan menggunakan RAM Capture untuk menyalin isi memori dengan skenario 1, skenerio 2, dan skenario 3 serta skenario 4 didapatkan raw file untuk digunakan examinasi bukti digital yang sebelumya dilakukan penghapusan registri sebelum akuisisi memori dilakukan.

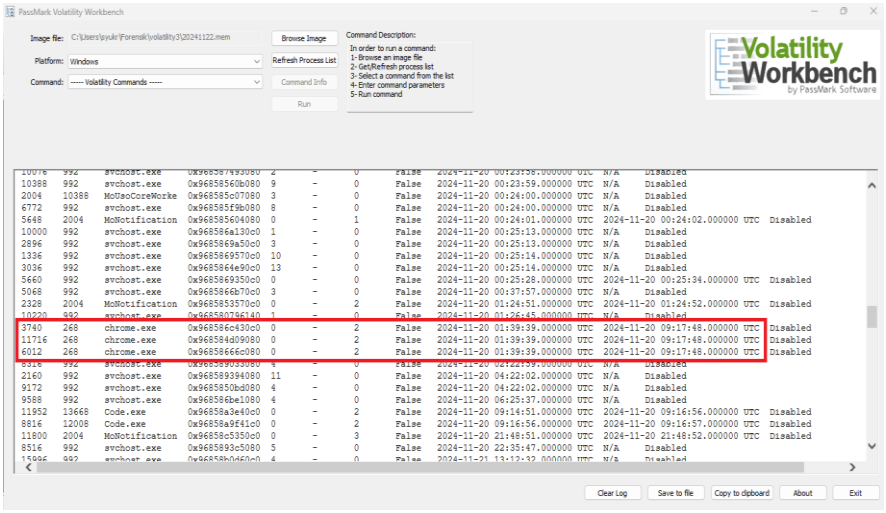
https://doi.org/10.33998/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025



Gambar 9. Menghapus Registri

3.2 Examinasi Bukti Digital (*Examination*)

Dari hasil scaning *Belkasoft* lalu dieksekusi dengan tool *Volatility* untuk mendapatkan informasi dan proses aplikasi *browser Chrome* dan Firefox yang berjalan di sistem. Hasil tangkapan dengan *belkasoft* untuk skenario satu berhasil mendapatkan berbagai informasi seperti aplikasi *Chrome* dan *Firefox* yang berjalan beserta informasi proses ID, dan *timestamp*. Namun tidak demikian ketika skenario kedua dilakukan, hasil tangkapan bukti digital untuk *Chrome* dan *Firefox* tidak berhasil, begitu juga yang dilakukan dengan skenario ke tiga ketika dijalankan, hasilnya *Chrome* dan Firefox tidak ditemukan di saat tool *belkasoft* melakukan *scaning* terhadap file memori, demikian juga skenario ke empat dijalankan.



Gambar 10. Hasil Chrome yang sedang berjalan pada Skenario 1

Dari gambar 10 terlihat ada tiga aplikasi browser *Chrome* yang berjalan dengan ditunjukkan nomor PID yang berbeda yakni 3740, 11716 dan 6012.
Dilakukan pengujian dengan menggunakan *browser Mozila firefox* dengan skenario 1, didapatkan hasil volatility firefox terlihat seperti gambar 7.

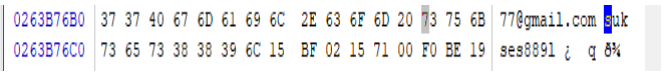
Gambar 11. Hasil volitility Firefox pada skenario 1

Pengujian volatility dengan skenario 2 tidak mendapatkan hasil apa-apa untuk *Chrome* dan *Firefox*. Dilanjutkan dengan skenario 3, dan skenario 4 juga tidak mendapatkan hasil untuk *Chrome* dan *Firefox* yang berjalan yang tersimpan di memori.

https://doi.org/10.33998/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025

3.3 Analisis Bukti Digital (*Analysis*)

Dari hasil *Volatility browser Chrome* dan *Firefox* yang berjalan, lalu dilakukan analisis dengan menggunakan *tool WinHex* mendapatkan *user login* dan password *gmail*.

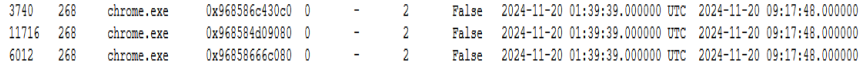


Gambar 12. Hasil user login dan password gmail pada Skenario 1

Pada skenario 1 menggunakan tool Image Capture RAM untuk melakukan *collection* bukti digital

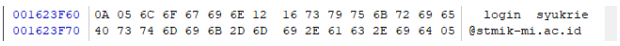
Gambar 13. Capture Image RAM

Kemudian dilakukan e*xamination* untuk pengambilan barang bukti dengan *tool Volatility Forensic*



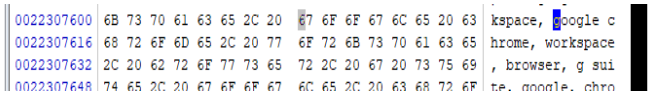
Gambar 14. Hasil ExaminationVolatility Forensic Browser Google Chrome pada Skenario 1

Dari hasil yang dilakukan dengan *Volatility forensik* ternyata tidak ditemukan bukti digital untuk aplikasi *google chrome* pada Skenario 2, 3 dan 4.
Dilakukan pengujian kembali dengan tools *WinHex* untuk skenario 4, Hasil skenario 4 dengan *WinHex*

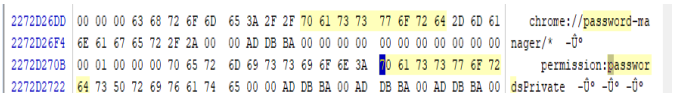


Gambar 15. Login Gmail Terdeteksi dengan WinHex

Kemudian dilakukan analisis dari bukti digital yang diperoleh menggunakan *WinHex* untuk skenario 1 sampai dengan skenario 4. Hasilnya hanya pada skenario 1 mendapatkan hasil akun dan *password gmail* seperti gambar 12.



Gambar 16. Hasil akun dan password Gmail Skenario 1



Gambar 17. Pencarian berdasarkan keyword password

3.4 Laporan Bukti Digital (*Reporting*)

Tahap reporting adalah tahap untuk memberikan laporan terkait dengan data-data analisis yang sudah dilakukan sebelumnya. Terlihat pada tabel 3.

Tabel 3. Bukti Digital yang didapat pada Chrome pada 4 Skenario

Activity	Tools		
	BelkaSoft	Volatility	WinHex
S1	Ada	Ada	Ada
S2	Tidak Ada	Tidak Ada	Tidak Ada
S3	Tidak Ada	Tidak ada	Tidak ada
S4	Tidak Ada	Tidak ada	Tidak ada

https://doi.org/10.33998/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025

3.5 Validasi

Dari analisis dan reporitng yang dilakukan, kemudian dilakukan validasi untuk menguji apakah hasil proses forensik yang diperoleh merupakan hasil yang benar, akurat, kredibel dan terjaga integritas datanya. Maka dilakukan kembali dengan menguji setidaknya dengan dua hasil tes forensik yang harus *repeatable* (dapat diulang kembali) dan *reproducible* (dapat diproduksi kembali). Hasil analisis yang dilakukan dengan beberapa kali percobaan menggunakan tool forensik digital dengan 4 skenario yang berbeda didapatkan hasil yang sama dengan uji yang dilakukan sebelumnya.

Tabel 4. Hasil Validasi

Keyword	**Chrome**				**Firefox**			
Searches	S1	S2	S3	S4	S1	S2	S3	S4
History	√	√	√	√	√	√	√	√
Timestamp	√	√	√	√	√	√	√	√
Password	√	0	0	0	0	0	0	0

3.6 Rekomendasi

Dari hasi validasi diberikan rekomendasi berupa saran-saran terkait dengan keamanan data pribadi mode private browser.

a. Gunakan browser dengan mode privat yang lebih aman untuk aktivitas sensitif seperti login ke akun email atau transaksi online.
b. Tutup browser segera setelah penggunaan untuk memastikan data dalam memori dilepaskan.
c. Lakukan restart atau matikan perangkat setelah selesai menggunakan *browser* untuk menghapus jejak data dari memori.
d. Pertimbangkan penggunaan alat tambahan seperti ekstensi keamanan *browser* untuk perlindungan privasi lebih lanjut.
e. Tingkatkan kesadaran pengguna tentang batasan keamanan mode privat dan pentingnya menjaga keamanan perangkat lunak.

4. UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini yakni Prof. Imam Riadi, Prof. Tole Sutikno, rekan-rekan seperjuangan di kampus S3 DIFA UAD Jogjakarta angkatan satu, dan buat istri dan anak-anak tercinta serta tim Areta Informatics College yang selalu mendukung setiap apa yang dilakukan untuk kemajuan pendidikan khususnya dibidang Informatika.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa mode privat pada browser, seperti Google Chrome dan Mozilla Firefox, belum sepenuhnya aman dalam melindungi data pribadi. Informasi sensitif seperti akun dan kata sandi pengguna masih dapat ditemukan di memori (RAM) perangkat, meskipun mode privat dirancang untuk tidak menyimpan data. Hal ini mengindikasikan bahwa mode privat hanya memberikan perlindungan terbatas, khususnya dalam situasi tertentu. Dengan menggunakan metode NIST, penelitian ini berhasil mengidentifikasi celah keamanan tersebut, sehingga penting untuk meningkatkan fitur keamanan pada browser. Sarannya perlu dilakukan penelitian lebih lanjut untuk di mesin virtual dan dengan browser yang lain menggunakan 4 skenario yang sudah dilakukan.

REFERENCES

[1] Z. Song, “Personal data security and stock crash risk: Evidence from China’s Cybersecurity Law,” *China J. Account. Res.*, vol. 17, no. 4, p. 100393, 2024, doi: 10.1016/j.cjar.2024.100393.
[2] R. Yulia Andarini, P. Hendradi, and S. Nugroho, “Meningkatkan Keamanan Terhadap Sql Injection Studi Kasus

 https://doi.org/10.33998/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025

Sistem Kepegawaian Bnn," *Indones. J. Bus. Intell.*, vol. 6, no. 1, 2023, doi: 10.21927/ijubi.v6i1.3161.
[3] C. Hargreaves, A. Nelson, and E. Casey, "An abstract model for digital forensic analysis tools - A foundation for systematic error mitigation analysis," *Forensic Sci. Int. Digit. Investig.*, vol. 48, no. S, p. 301679, 2024, doi: 10.1016/j.fsidi.2023.301679.
[4] S. Ebbers, S. Gense, M. Bakkouch, F. Freiling, and S. Schinzel, "Grand theft API: A forensic analysis of vehicle cloud data," *Forensic Sci. Int. Digit. Investig.*, vol. 48, no. S, p. 301691, 2024, doi: 10.1016/j.fsidi.2023.301691.
[5] M. Okawa, "Synergy of on-surface and in-air trajectories: Exploratory analysis of forensic online signatures implementing lessons learned from biometrics," *Forensic Sci. Int. Reports*, vol. 8, no. August, p. 100340, 2023, doi: 10.1016/j.fsir.2023.100340.
[6] X. Fernández-Fuentes, T. F. Pena, and J. C. Cabaleiro, "Digital forensic analysis of the private mode of browsers on Android," *Comput. Secur.*, vol. 134, Nov. 2023, doi: 10.1016/j.cose.2023.103425.
[7] X. Fernández-Fuentes, T. F. Pena, and J. C. Cabaleiro, "Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study," *Comput. Secur.*, vol. 115, Apr. 2022, doi: 10.1016/j.cose.2022.102626.
[8] V. R. Kebande, S. O. Baror, R. M. Parizi, K. K. R. Choo, and H. S. Venter, "Mapping digital forensic application requirement specification to an international standard," *Forensic Sci. Int. Reports*, vol. 2, Dec. 2020, doi: 10.1016/j.fsir.2020.100137.
[9] B. Lerner, D. Passey, N. Sperber, and S. Knight, "OP043: The evolving attitude towards privacy and security of personal genomic data," *Genet. Med.*, vol. 24, no. 3, p. S369, 2022, doi: 10.1016/j.gim.2022.01.590.
[10] I. Riadi, A. Yudhana, and M. Al Barra, "Forensik Mobile pada Layanan Media Sosial LinkedIn," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 6, no. 1, pp. 9–20, 2021, doi: 10.14421/jiska.2021.61-02.
[11] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Sci. Int. Digit. Investig.*, vol. 48, Mar. 2024, doi: 10.1016/j.fsidi.2023.301675.
[12] V. H. V. Suhardjono, Arman Syah Putra, Nurul Aisyah, "Analysis of NIST Methods on Facebook Messenger for Forensic Evidance," *J. Innov. Res. Knowl.*, vol. 1, no. 10, p. 8, 2022, doi: 10.53625/jirk.v1i8.1122.
[13] R. N. Bintang, R. Umar, and A. Yudhana, "Assess of Forensic Tools on Android Based Facebook Lite with the NIST Method," *Sci. J. Informatics*, vol. 8, no. 1, pp. 1–9, 2021, doi: 10.15294/sji.v8i1.26744.
[14] F. Yasin, Abdul Fadlil, and Rusydi Umar, "Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 91–98, 2021, doi: 10.29207/resti.v5i1.2784.
[15] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 820–828, 2020, doi: 10.29207/resti.v4i5.2224.
[16] Imam Riadi, Rusydi Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 45–54, 2021, doi: 10.29207/resti.v5i1.2626.
[17] D. Julian and T. Sutabri, "Analisa Kinerja Aplikasi Digital Forensik Autopsy untuk Pengembalian Data menggunakan Metode NIST SP 800-86," *J. Inform. Terpadu*, vol. 9, no. 2, pp. 136–142, 2023, doi: 10.54914/jit.v9i2.984.
[18] A. Dan, P. Bukti, F. Digital, A. Media, S. Twitter, and M. Metode, "Analisa dan pencarian bukti forensik digital pada aplikasi media social twitter menggunakan metode national institute standard of technology," pp. 24–33, 1979.
[19] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost-benefit analysis into the NIST cybersecurity framework via the gordon-loeb model," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–8, 2020, doi: 10.1093/CYBSEC/TYAA005.
[20] N. Anwar, A. M. Widodo, B. A. Sekti, M. B. Ulum, M. Rahaman, and H. D. Ariessanti, "Comparative Analysis of NIJ and NIST Methods for MicroSD Investigations: A Technopreneur Approach," *Aptisi Trans. Technopreneursh.*, vol. 6, no. 2, pp. 169–181, Jul. 2024, doi: 10.34306/att.v6i2.407.
[21] G. Horsman *et al.*, "A forensic examination of web browser privacy-modes," *Forensic Sci. Int. Reports*, vol. 1, no. October, p. 100036, 2019, doi: 10.1016/j.fsir.2019.100036.
[22] Imam Riadi, Rusydi Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 45–54, Feb. 2021, doi: 10.29207/resti.v5i1.2626.
[23] T. Rochmadi, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," *Indones. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.

 https://doi.org/10.33998/processor.2025.20.1.2012
Submitted: 03 Desember 2024; Reviewed Round 1: 12 Desember 2024; Reviewed Round 2: 27 Januari 2025; Review Round 3: 07 Februari 2025; Accepted; 25 Maret 2025; Published: 30 April 2025