AICOMS
Applied Information Technology and Computer Science
e-ISSN: 2964-7703
Vol. 5 No. 1, Juni-2026, pp. 230-243

Analisis *Host-Based Digital Forensics* terhadap Artefak Penggunaan *Tor browser* pada Sistem Operasi *Linux*

Rico Saputra [1], dan Ghufron Zaida Muflih [2]*

[1,2] Universitas Ma'arif Nahdlatul Ulama Kebumen; kangrico689@gmail.com; ghufron.zaida@umnu.ac.id
* Korespondensi: e-mail@e-mail.com

Info Artikel:
Dikirim: 20 April 2026
Direvisi: 30 Mei 2026
Diterima: 30 Mei 2026

Abstrak: The use of Tor Browser as a digital anonymity platform continues to increase alongside the growing demand for internet privacy. Although Tor is designed to conceal user identities and activities through onion routing mechanisms, previous studies have shown that digital artifacts can still be recovered from the host system. This study aims to analyze the existence of digital artifacts generated by Tor Browser usage on the BackBox Linux operating system using a host-based digital forensics approach. The research employed an experimental method consisting of seven testing scenarios, namely behavioral forensic leakage, session persistence, cross-session correlation, host versus virtualization comparison, memory footprint analysis, network pattern consistency, and passive onion observation. Data acquisition and analysis were conducted using Autopsy, Hindsight, Plaso, LiME, Volatility, Bulk Extractor, and Wireshark. The results indicate that Tor Browser usage still leaves digital artifacts within storage media, volatile memory, and network traffic. This study concludes that the host-based digital forensics approach remains effective for identifying Tor Browser activities in Linux environments.

Kata Kunci: *Tor Browser; host-based digital forensics; Linux; digital artifacts; memory forensics; network forensics.*

Intisari: Penggunaan *Tor Browser* sebagai media anonimitas digital semakin meningkat seiring berkembangnya kebutuhan privasi pengguna internet. Meskipun *Tor* dirancang untuk menyembunyikan identitas dan aktivitas pengguna melalui mekanisme *onion routing*, beberapa penelitian menunjukkan bahwa artefak digital masih dapat ditemukan pada sisi sistem pengguna (*host system*). Penelitian ini bertujuan untuk menganalisis keberadaan artefak digital yang dihasilkan dari penggunaan *Tor Browser* pada sistem operasi *BackBox Linux* menggunakan pendekatan *host-based digital forensics*. Metode penelitian menggunakan pendekatan eksperimental dengan tujuh skenario pengujian yang meliputi *behavioral forensic leakage*, *session persistence*, *cross-session correlation*, virtualisasi, analisis memori, pola trafik jaringan, dan observasi layanan *onion*. Proses akuisisi dan analisis data dilakukan menggunakan *Autopsy*, *Hindsight*, *Plaso*, *LiME*, *Volatility*, *Bulk Extractor*, dan *Wireshark*. Hasil penelitian menunjukkan bahwa penggunaan *Tor Browser* masih meninggalkan artefak digital pada media penyimpanan, memori volatil, dan lalu lintas jaringan. Penelitian ini menyimpulkan bahwa pendekatan *host-based digital forensics* masih efektif untuk mengidentifikasi aktivitas penggunaan *Tor Browser* pada lingkungan Linux.

Kata Kunci: *Tor Browser*; *host-based digital forensics*; Linux; artefak digital; *memory forensics*; *network forensics*

1. Pendahuluan

Perkembangan teknologi informasi pada era digital turut meningkatkan potensi terjadinya *cybercrime* yang memanfaatkan anonimitas jaringan untuk menyembunyikan identitas pengguna. Kondisi tersebut mendorong kebutuhan terhadap metode investigasi digital yang mampu mengungkap aktivitas pengguna secara akurat dan dapat dipertanggungjawabkan secara ilmiah [1];[2]. Salah satu teknologi yang banyak digunakan untuk menjaga privasi pengguna internet adalah *Tor Browser*. *Tor Browser* menggunakan mekanisme *onion routing* untuk menyamarkan alamat IP dan aktivitas penelusuran pengguna sehingga proses pelacakan menjadi lebih sulit dilakukan [3].

Selain digunakan untuk menjaga privasi dan kebebasan akses informasi, *Tor Browser* juga sering dikaitkan dengan aktivitas pada *dark web*, seperti perdagangan data curian, distribusi *malware*, dan berbagai aktivitas *cybercrime* lainnya [4].Tingginya tingkat anonimitas pada jaringan Tor menyebabkan proses investigasi digital menjadi lebih kompleks. Meskipun demikian, beberapa penelitian menunjukkan bahwa penggunaan *Tor Browser* masih dapat meninggalkan artefak digital pada sistem host, seperti *cache*, basis data SQLite, metadata sistem, dan residu memori volatil yang dapat dianalisis menggunakan metode *digital forensics* [5];[6];[7].

Dalam konteks *browser forensics*, artefak seperti file SQLite, *log system*, *memory dump*, dan pola trafik jaringan memiliki peran penting dalam proses rekonstruksi aktivitas pengguna [6];[8]. Penelitian sebelumnya menunjukkan bahwa artefak penggunaan *Tor Browser* dapat ditemukan melalui pendekatan *offline forensics* maupun *live forensics* pada sistem Linux dan Android [9];[10];[11];[12]. Selain itu, penelitian terkait analisis *dark web* juga menegaskan pentingnya investigasi terhadap penggunaan *Tor Browser* dalam mendukung penanganan kejahatan siber [13].

Meskipun penelitian sebelumnya telah membahas artefak digital pada *Tor Browser*, sebagian besar penelitian masih berfokus pada teknik forensik tunggal atau lingkungan sistem tertentu [14]. Penelitian yang mengintegrasikan analisis artefak berbasis perilaku pengguna, persistensi lintas sesi, residu memori volatil, perbandingan lingkungan host dan virtualisasi, serta pola trafik jaringan dalam satu kerangka eksperimen terpadu masih terbatas.

Berdasarkan celah penelitian tersebut, penelitian ini menganalisis artefak digital yang dihasilkan oleh penggunaan *Tor Browser* menggunakan pendekatan *host-based digital forensics* pada sistem operasi Linux. Penelitian dilakukan melalui tujuh skenario eksperimen terkontrol yang meliputi variasi perilaku pengguna, persistensi sesi, korelasi lintas sesi, perbandingan host dan virtualisasi, analisis memori, analisis trafik jaringan, dan observasi layanan *onion*. Selain pengujian pada Linux, penelitian ini melakukan pengujian pembanding pada lingkungan Windows berbasis virtualisasi untuk melihat perbedaan karakteristik artefak yang dihasilkan.

Kontribusi penelitian ini terletak pada integrasi pendekatan *disk forensics*, *memory forensics*, dan *network forensics* dalam satu kerangka eksperimen yang terstruktur untuk menganalisis artefak penggunaan *Tor Browser* [15]. Hasil penelitian diharapkan dapat memberikan pemahaman mengenai karakteristik artefak digital yang masih tertinggal pada sistem host, sekaligus mendukung pengembangan metode investigasi forensik digital terhadap aktivitas anonim pada jaringan Tor.

4. Metode dan Hasil Penelitian

4.1. Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimental dalam bidang *host-based digital forensics* untuk menganalisis artefak digital yang dihasilkan dari penggunaan *Tor Browser* pada sistem operasi *BackBox Linux*. Pendekatan ini dipilih karena memungkinkan proses observasi, akuisisi, dan analisis bukti digital dilakukan secara

terkontrol pada sisi sistem pengguna (*host system*). Fokus penelitian diarahkan pada identifikasi artefak penyimpanan, residu memori, dan pola lalu lintas jaringan yang masih tersisa setelah penggunaan *Tor Browser*. Penelitian dilakukan melalui tujuh skenario eksperimen seperti pada tabel 1.

Tabel 1. Skenario Penelitian

No	Skenario	Deskripsi
1	*Behavioral Forensic Leakage*	Menguji pengaruh perilaku pengguna seperti membuka banyak tab, copy-paste URL, dan perubahan ukuran jendela terhadap jumlah artefak digital yang tersimpan pada sistem.
2	*Session Persistence*	Mengidentifikasi artefak yang masih tersisa setelah Tor Browser ditutup dan sistem direstart.
3	*Cross-Session Correlation*	Menganalisis kemungkinan korelasi artefak antar beberapa sesi penggunaan Tor Browser yang berbeda.
4	*Host vs Virtualization*	Membandingkan karakteristik artefak digital pada lingkungan host BackBox Linux dan virtual machine Windows.
5	*Memory Footprint Analysis*	Mengidentifikasi residu data volatil yang masih tersimpan pada RAM menggunakan pendekatan memory forensics.
6	*Network Pattern Consistency*	Menganalisis pola komunikasi jaringan Tor berdasarkan ukuran paket, interval transmisi, dan burst traffic.
7	*Passive Onion Observation*	Mengamati artefak digital yang dihasilkan dari aktivitas akses layanan onion atau dark web tanpa melakukan interaksi aktif.

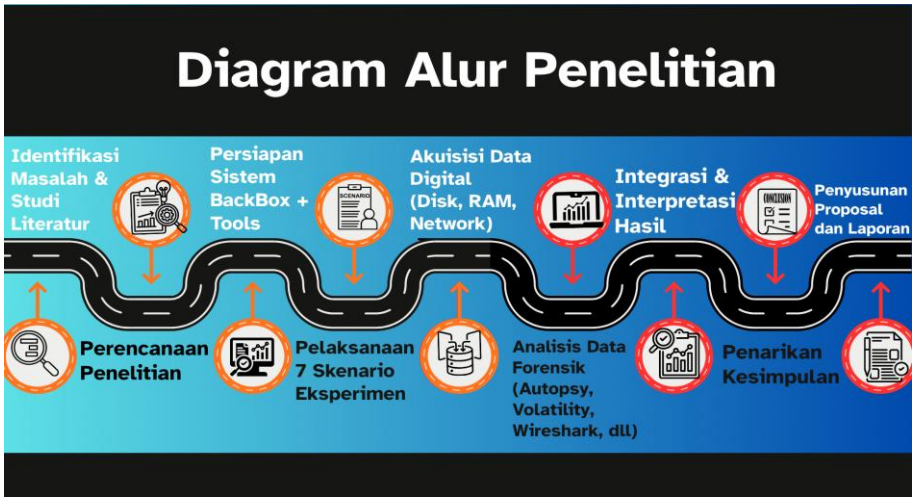
Tujuh skenario dirancang untuk merepresentasikan berbagai kondisi penggunaan Tor Browser yang umum ditemukan pada lingkungan nyata. Penelitian tidak hanya berfokus pada satu jenis artefak digital, tetapi mengevaluasi keterkaitan antara artefak penyimpanan, memori, dan jaringan dalam mendukung proses investigasi digital berbasis *host*. Lingkungan penelitian menggunakan *BackBox Linux* sebagai *host operating system* serta Windows berbasis Oracle VirtualBox sebagai lingkungan pembanding.

Proses pengumpulan data melalui tiga tahapan utama, yaitu *disk forensics*, *memory forensics*, dan *network forensics*. Akuisisi media penyimpanan dilakukan menggunakan Autopsy dan Hindsight untuk mengekstraksi artefak seperti basis data *SQLite, cache,* metadata sistem, dan *temporary files* [16]. Akuisisi memori dilakukan menggunakan *LiME* untuk memperoleh *RAM dump*, selanjutnya dianalisis menggunakan *Volatility* dan *Bulk Extractor* guna mengidentifikasi proses aktif, URL sementara, dan residu data volatil.

Pada sisi jaringan, *Wireshark* digunakan untuk merekam pola komunikasi jaringan Tor dalam format PCAP. Analisis difokuskan pada ukuran paket, interval transmisi, dan pola *burst traffic* tanpa melakukan dekripsi isi komunikasi. Seluruh proses analisis dilakukan secara terintegrasi menggunakan *Plaso* untuk menyusun *timeline* aktivitas digital lintas sumber data. Validasi artefak dilakukan menggunakan metode *hashing* dan *cross-validation* antar-*tools* untuk menjaga integritas bukti digital selama proses investigasi [17];[18].

4.1.1 Alur Penelitian

Tahapan penelitian diawali dengan proses perencanaan penelitian dan persiapan lingkungan eksperimen menggunakan sistem operasi *BackBox Linux* beserta tools forensik digital yang digunakan. Selanjutnya dilakukan pelaksanaan tujuh skenario eksperimen untuk memperoleh artefak digital penggunaan *Tor Browser* melalui pendekatan *disk forensics, memory forensics, dan network forensics.* Proses akuisisi data dilakukan pada media penyimpanan, memori volatil, dan lalu lintas jaringan menggunakan tools *Autopsy, Volatility, Wireshark, Hindsight, dan Plaso*. Data hasil akuisisi kemudian dianalisis dan diintegrasikan untuk mengidentifikasi karakteristik artefak digital yang ditemukan pada sistem *host*. Tahap akhir penelitian dilakukan melalui interpretasi hasil, penarikan kesimpulan, Iserta penyusunan laporan penelitian. Diagram alur penelitian seperti pada gambar 1.



Gambar 1. Diagram Alur Penelitian

4.2. Hasil dan Pembahasan

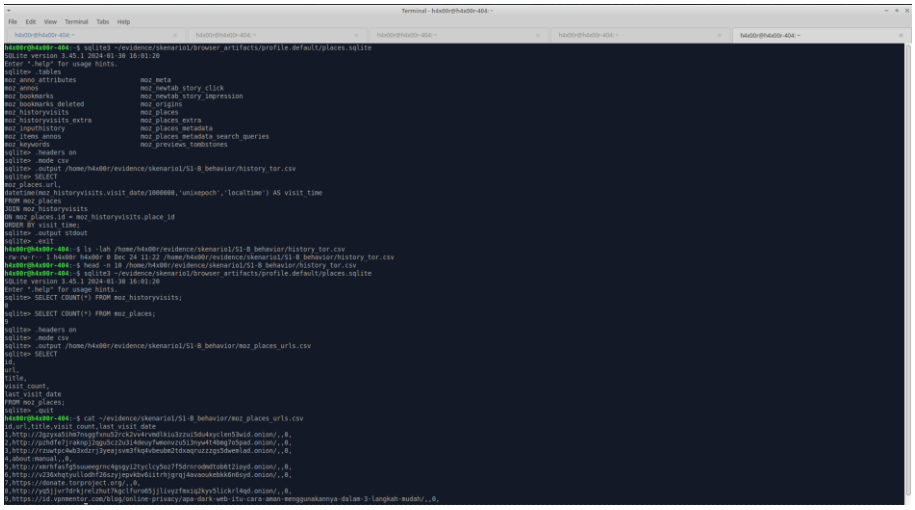
4.2.1 Analisis *Behavioral Forensic Leakage*

Hasil skenario pertama menunjukkan bahwa perubahan perilaku pengguna pada *Tor Browser* menghasilkan variasi artefak digital yang berbeda dibandingkan penggunaan normal. Aktivitas seperti membuka banyak tab, melakukan *copy-paste* URL, dan mengubah ukuran jendela meningkatkan jumlah metadata lokal serta perubahan pada file *SQLite* dan cache browser. Analisis menggunakan *Hindsight* menunjukkan bahwa beberapa artefak aktivitas pengguna masih dapat teridentifikasi meskipun sesi telah ditutup. Selain itu, *Plaso* berhasil menyusun *timeline* aktivitas yang memperlihatkan korelasi waktu antar aktivitas pengguna dan perubahan file sistem. Anonimitas jaringan yang disediakan oleh Tor tidak sepenuhnya menghilangkan residu aktivitas pada sisi *host*. Temuan Behavioral Forensic Leakage seperti pada tabel 2.

Tabel 2. Temuan *Behavioral Forensic Leakage*

Temuan	Keterangan
File SQLite mengalami perubahan	Aktivitas pengguna menghasilkan perubahan metadata lokal pada browser
Cache browser meningkat	Banyak tab dan aktivitas browsing meningkatkan residu cache
Timeline aktivitas terdeteksi	*Plaso* berhasil mengidentifikasi korelasi waktu aktivitas pengguna
Artefak tetap ditemukan setelah sesi ditutup	*Hindsight* masih dapat mengekstraksi sebagian aktivitas browsing

Untuk mendukung temuan pada skenario *Behavioral Forensic Leakage,* ekstraksi artefak browser dari file *places.sqlite* menggunakan SQLite3. Hasil ekstraksi menunjukkan bahwa sejumlah URL yang diakses melalui Tor Browser masih tersimpan di *database browser* meskipun sesi penggunaan telah berakhir [19]. Aktivitas pengguna masih meninggalkan residu artefak lokal yang dapat dianalisis melalui pendekatan *host-based digital forensics.* Ditemukan sembilan entri URL yang masih tersimpan di *database browser*. URL yang ditemukan merupakan alamat layanan onion (.onion) yang sebelumnya diakses melalui Tor Browser. Informasi aktivitas browsing masih dapat ditemukan pada sisi host meskipun Tor Browser telah digunakan untuk menjaga anonimitas pengguna. Hasil Ekstraksi URL dari File *places.sqlite* seperti pada gambar 2.



Gambar 2. Hasil Ekstraksi URL dari File *places.sqlite* pada Skenario *Behavioral Forensic Leakage*

4.2.2 Persistensi Sesi dan Residu Data

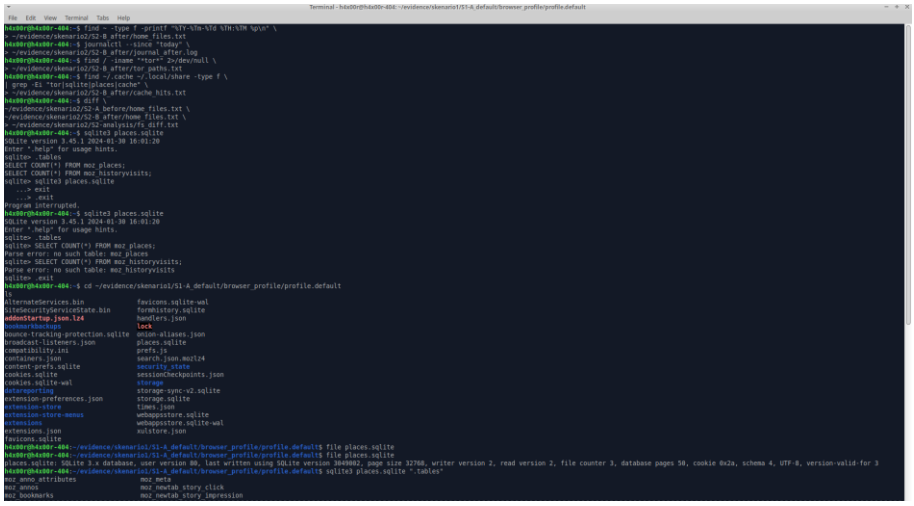
Eksperimen kedua menunjukkan bahwa residu data masih dapat ditemukan setelah *Tor Browser* ditutup dan sistem direstart. Artefak berupa file cache, *journal SQLite*, dan *temporary metadata* masih tersimpan pada direktori sistem. Analisis menggunakan *Autopsy* memperlihatkan keberadaan *timestamp* aktivitas yang tetap dapat dikorelasikan dengan sesi penggunaan sebelumnya.

Klaim *"no trace browsing"* pada *Tor Browser* tidak sepenuhnya berlaku dalam konteks *host-based digital forensics*. Walaupun Tor mampu menyembunyikan identitas jaringan pengguna, beberapa residu lokal tetap dapat diidentifikasi melalui pendekatan forensik digital. Temuan Persistensi Sesi dan Residu Data seperti pada tabel 3.

Tabel 3. Temuan *Persistensi Sesi dan Residu Data*

Temuan	Keterangan
File cache masih tersimpan	Residu data tetap ditemukan setelah browser ditutup
Journal SQLite teridentifikasi	Aktivitas sesi sebelumnya masih dapat dianalisis
Timestamp aktivitas masih tersedia	Waktu penggunaan masih dapat direkonstruksi
Metadata sementara masih ditemukan	Sistem host tetap menyimpan sebagian artefak lokal

Artefak browser seperti file cache dan journal SQLite masih tersimpan setelah Tor Browser ditutup dan sistem direstart. Adanya persistensi data lokal yang dapat dimanfaatkan dalam proses investigasi forensik digital. Artefak Cache dan Journal SQLite yang ditemukan seperti pada gambar 3.



Gambar 3. Artefak Cache dan Journal SQLite yang Masih Tersimpan Setelah Sistem Direstart

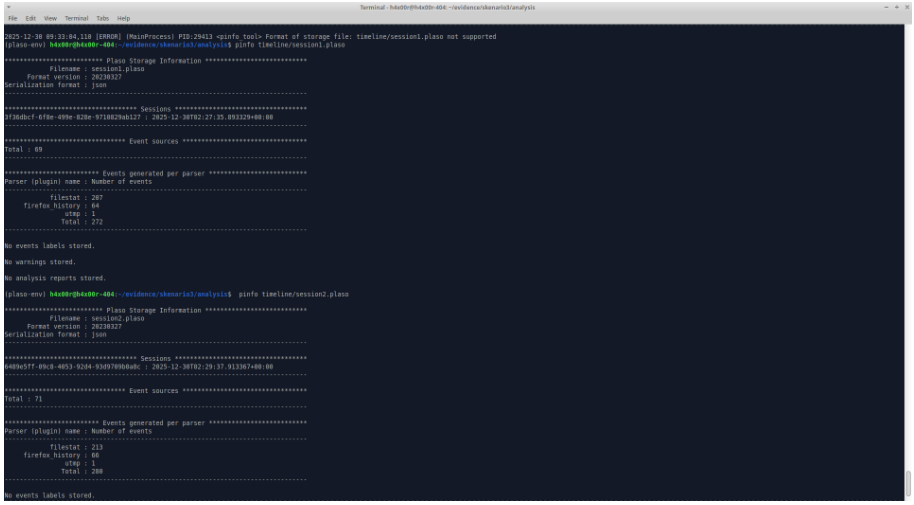
4.2.3 Korelasi Multi-Sesi *(Cross-Session Correlation)*

Pada eksperimen multi-sesi ditemukan bahwa artefak antar-sesi penggunaan masih memiliki pola korelasi tertentu, terutama metadata file, *timestamp*, dan pola akses direktori sistem. Analisis menggunakan *Bulk Extractor dan Plaso* menunjukkan adanya hubungan kronologis antar-sesi *browsing* yang dilakukan dalam waktu berbeda. Aktivitas pengguna dapat direkonstruksi melalui pendekatan korelasi *timeline* meskipun dilakukan menggunakan jaringan anonim. Temuan tersebut penting dalam konteks investigasi forensik karena menunjukkan bahwa pola penggunaan *Tor Browser* masih dapat dianalisis dari sisi sistem lokal pengguna. Temuan Korelasi Multi-Sesi seperti pada tabel 4.

Tabel 4. Temuan Korelasi Multi-Sesi

Temuan	Keterangan
Timestamp antar-sesi berkorelasi	Aktivitas browsing dapat direkonstruksi secara kronologis
Metadata file tetap konsisten	Pola akses direktori masih dapat dianalisis
Timeline aktivitas berhasil dibangun	*Plaso* menunjukkan hubungan antar-sesi penggunaan

Hasil korelasi aktivitas antar sesi penggunaan Tor Browser yang berhasil direkonstruksi menggunakan Plaso berdasarkan timestamp dan metadata sistem seperti pada gambar 4.



Gambar 4. Timeline Aktivitas Multi-Sesi Menggunakan *Plaso*

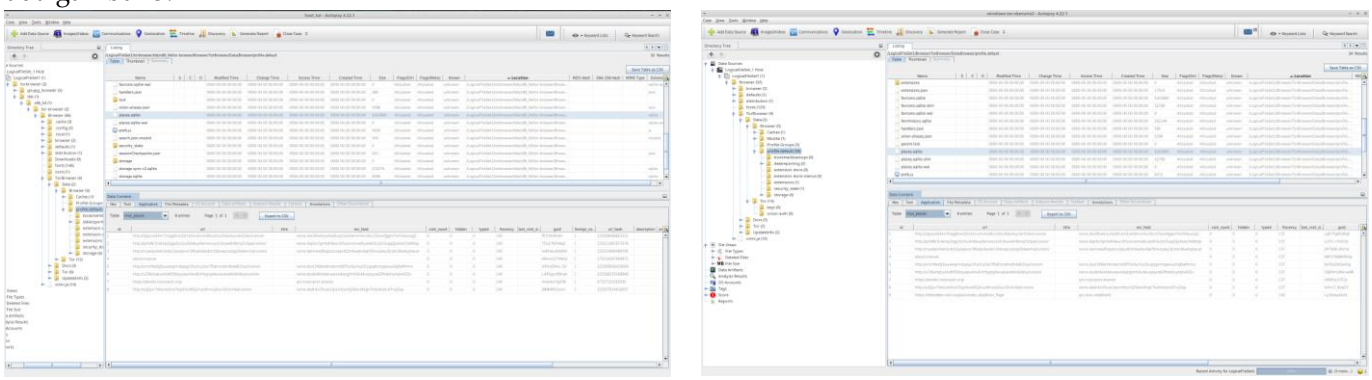
4.2.4 Perbandingan Artefak Host dan Virtualisasi

Skenario keempat menemukan bahwa lingkungan virtualisasi menghasilkan karakteristik artefak yang berbeda dibandingkan sistem *host* langsung [20]. Sistem *guest* berbasis Windows pada *Oracle VirtualBox* menghasilkan jumlah residu file yang lebih sedikit dibandingkan sistem *BackBox Linux* sebagai *host*. Artefak seperti cache, metadata sesi, dan file sementara tetap dapat ditemukan pada kedua lingkungan. Integritas data hasil akuisisi tetap terjaga selama proses analisis berlangsung. Temuan Artefak Host dan Virtualisasi seperti pada tabel 5.

Tabel 5. Temuan Perbandingan Artefak Host dan Virtualisasi

Temuan	Keterangan
Lingkungan virtual menghasilkan residu lebih sedikit	Virtual machine menghasilkan jumlah artefak lebih rendah dibanding host langsung
Cache dan metadata sesi tetap ditemukan	Aktivitas pengguna masih meninggalkan jejak digital pada kedua lingkungan
File sementara masih teridentifikasi	*Temporary files* tetap tersimpan setelah sesi penggunaan
Integritas akuisisi terjaga	Hashdeep menunjukkan data hasil akuisisi tidak mengalami perubahan

Lingkungan virtual menghasilkan jumlah residu artefak yang relatif lebih sedikit dibandingkan host langsung. Perbandingan jumlah artefak yang ditemukan pada lingkungan host *BackBox Linux* dan virtual machine Windows seperti pada gambar 5.



Gambar 5. Perbandingan Artefak pada Lingkungan Host dan Virtual Machine

4.2.5 Analisis Jejak Memori *(Memory Footprint Analysis)*

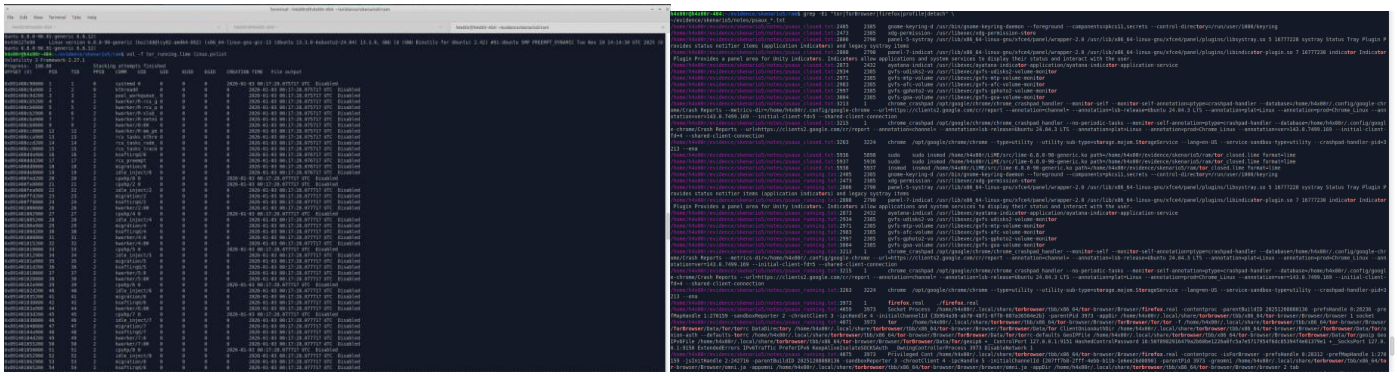
Analisis memori menunjukkan bahwa residu data volatil masih dapat ditemukan pada RAM meskipun *Tor Browser* telah ditutup. *Volatility* berhasil mengidentifikasi proses terkait Tor, koneksi jaringan aktif, serta potongan URL yang masih tersimpan pada area memori tertentu [21]. *Bulk Extractor* menemukan beberapa *string* dan metadata sementara yang berkaitan dengan aktivitas *browsing*. Memori volatil memiliki potensi besar sebagai sumber bukti digital dalam investigasi penggunaan browser anonim[22]. Temuan analisis jejak memori seperti pada tabel 6

Tabel 6. Temuan Analisis Jejak Memori

Temuan	Keterangan
Proses Tor masih ditemukan pada RAM	*Volatility* berhasil mengidentifikasi proses *tor.real dan firefox.real*
URL sementara masih tersimpan	Sebagian aktivitas browsing masih berada pada memori volatil
Metadata sesi ditemukan di RAM	Informasi sementara tetap dapat dianalisis setelah aplikasi ditutup

Data volatil memiliki nilai forensik tinggi	Memori menjadi sumber bukti penting dalam investigasi digital

Proses Tor Browser yang masih dapat diidentifikasi pada memori volatil menggunakan *Volatility* meskipun aplikasi telah ditutup. Hasil analisis ram dump menggunakan *volatility* seperti pada gambar 6



Gambar 6. Hasil Analisis RAM Dump Menggunakan *Volatility*

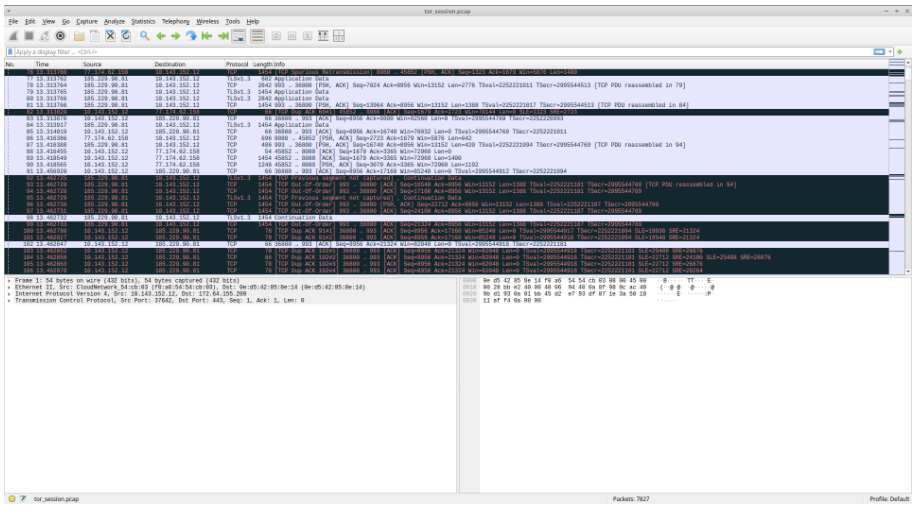
4.2.6 Analisis Pola Trafik Jaringan

Analisis menggunakan Wireshark menunjukkan adanya pola trafik yang konsisten selama penggunaan *Tor Browser*. Walaupun isi paket tidak dapat dibaca karena mekanisme enkripsi Tor, pola ukuran paket, interval transmisi, dan *burst traffic* tetap dapat diamati. Beberapa sesi menunjukkan pola komunikasi yang serupa ketika pengguna mengakses layanan *onion*, terutama pada frekuensi koneksi dan distribusi ukuran paket. *Network traffic analysis* masih memiliki potensi untuk mengidentifikasi karakteristik penggunaan Tor tanpa perlu melakukan dekripsi isi komunikasi [23];[24]. Temuan analisis pola trafik jaringan seperti pada tabel 7.

Tabel 7. Temuan Analisis Pola Trafik Jaringan

Temuan	Keterangan
Pola trafik Tor bersifat konsisten	Distribusi ukuran paket menunjukkan karakteristik tertentu
Burst traffic dapat diamati	Aktivitas komunikasi Tor menghasilkan pola transmisi berulang
Interval paket dapat dianalisis	Wireshark mampu merekam pola komunikasi jaringan
Isi komunikasi tetap terenkripsi	Analisis hanya dilakukan pada pola trafik tanpa dekripsi paket

Pola komunikasi jaringan Tor yang direkam menggunakan *Wireshark*. Walaupun isi komunikasi terenkripsi, ukuran paket dan pola *burst traffic* masih dapat diamati. Capture pola trafik tor menggunakan *wireshark* seperti pada gambar 7.



Gambar 7. Capture Pola Trafik Tor Menggunakan *Wireshark*

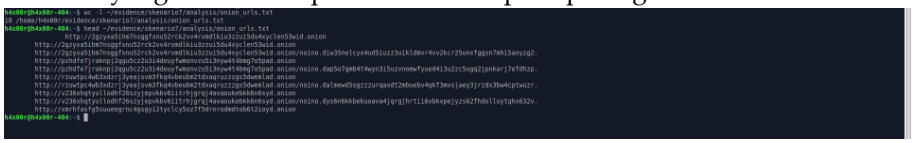
4.2.7 Observasi Dark Web (*Passive Onion Observation)*

Hasil observasi layanan *onion* menemukan bahwa akses pasif tanpa login maupun interaksi aktif tetap menghasilkan artefak lokal pada sistem pengguna. Artefak tersebut meliputi URL *onion*, file sementara, cache, dan metadata sesi. Walaupun tidak ditemukan data kredensial atau isi komunikasi, keberadaan artefak akses menunjukkan bahwa aktivitas kunjungan terhadap *dark web* masih dapat diidentifikasi melalui pendekatan *host-based forensics* [23]. Temuan *Observasi Dark Web* (Passive Onion Observation) seperpti pada tabel 8

Tabel 8. Temuan *Observasi Dark Web (Passive Onion Observation)*

Temuan	Keterangan
URL onion masih dapat ditemukan	Aktivitas akses layanan dark web meninggalkan artefak lokal
Cache dan metadata sesi tersimpan	Sistem host masih menyimpan residu aktivitas pengguna
File sementara berhasil diidentifikasi	*Temporary files* menunjukkan adanya aktivitas browsing
Aktivitas dark web masih dapat dianalisis	*Host-based forensics* tetap efektif untuk investigasi layanan onion

Artefak URL layanan onion yang masih tersimpan pada sistem setelah aktivitas observasi pasif dilakukan melalui Tor Browser. Artefak URL Onion yang ditemukan pada browser seperti pada gambar 8.



Gambar 8. Artefak URL Onion yang Ditemukan pada Browser

4.2.8 Implikasi dan Keterbatasan Penelitian

Hasil penelitian menunjukkan bahwa *Tor Browser* tidak sepenuhnya mampu menghilangkan residu aktivitas digital pada sisi sistem pengguna. Artefak lokal masih dapat ditemukan melalui analisis media penyimpanan, memori, maupun pola jaringan. Pendekatan *host-based digital forensics* tetap efektif digunakan dalam investigasi aktivitas anonim berbasis Tor.

Penelitian ini memiliki beberapa keterbatasan, yaitu eksperimen hanya dilakukan pada lingkungan *BackBox Linux* dan sebagian pengujian virtualisasi berbasis Windows sehingga hasil penelitian belum dapat digeneralisasikan pada

seluruh distribusi Linux atau sistem operasi lainnya. Selain itu, penelitian belum mencakup teknik *live deanonymization* maupun analisis tingkat lanjut terhadap node jaringan Tor [14].

4.2.9 Kontribusi dan Kebaruan Penelitian

Penelitian ini memiliki beberapa unsur kebaruan dibandingkan penelitian forensik digital sebelumnya. Pertama, berfokus pada pendekatan *host-based digital forensics* terhadap *Tor Browser* pada sistem operasi *BackBox Linux* yang masih relatif jarang dibahas. Kedua, menggunakan tujuh skenario eksperimen berbeda untuk mengevaluasi variasi artefak digital berdasarkan perilaku pengguna, persistensi sesi, virtualisasi, dan pola komunikasi jaringan. Ketiga, mengintegrasikan pendekatan *disk forensics*, *memory forensics*, dan *network forensics* dalam satu kerangka analisis menggunakan *Autopsy, Volatility, Plaso, Hindsight, dan Wireshark* sebagaimana direkomendasikan dalam penelitian browser forensics modern [15].

4.2.10 Tabel Hasil Penelitian

Berdasarkan hasil penelitian yang telah dilakukan, ditemukan berbagai artefak digital yang menunjukkan bahwa penggunaan Tor Browser masih meninggalkan jejak aktivitas pada sisi host. Artefak tersebut mencakup basis data SQLite, cache browser, metadata sesi, residu memori volatil, hingga pola komunikasi jaringan. Hasil analisis juga menunjukkan bahwa pendekatan *host-based digital forensics* mampu mengidentifikasi dan merekonstruksi aktivitas pengguna melalui integrasi *disk forensics, memory forensics, dan network forensics.* Ringkasan hasil analisis pada setiap skenario penelitian disajikan pada Tabel 9.

Tabel 9. Hasil Analisis Artefak Digital pada Setiap Skenario

Skenario	Artefak Ditemukan	Tools Analisis	Hasil Utama
Behavioral Forensic Leakage	*SQLite database*, cache, metadata	*Hindsight*, *Plaso*	Perubahan perilaku pengguna meningkatkan jumlah artefak lokal
Session Persistence	*Cache residual*,*journal SQLite*	*Autopsy*, *Hindsight*	Residu data tetap ditemukan setelah browser ditutup
Cross-Session Correlation	*Timestamp*, metadata sesi	*Bulk Extractor*, *Plaso*	Aktivitas antar sesi masih dapat dikorelasikan
Host vs Virtualization	*Temporary files*, cache	*Autopsy*, *Hashdeep*	Lingkungan virtual menghasilkan residu lebih sedikit
Memory Footprint Analysis	URL sementara, proses aktif	*LiME*, *Volatility*	RAM masih menyimpan artefak setelah browser ditutup
Network Pattern Consistency	Pola paket dan *burst traffic*	*Wireshark*	Trafik *Tor* memiliki pola komunikasi yang konsisten
Passive Onion Observation	URL *onion*, metadata akses	*Autopsy*, *Hindsight*	Akses pasif tetap meninggalkan artefak lokal

4.2.11 Hasil Teknis Analisis Artefak

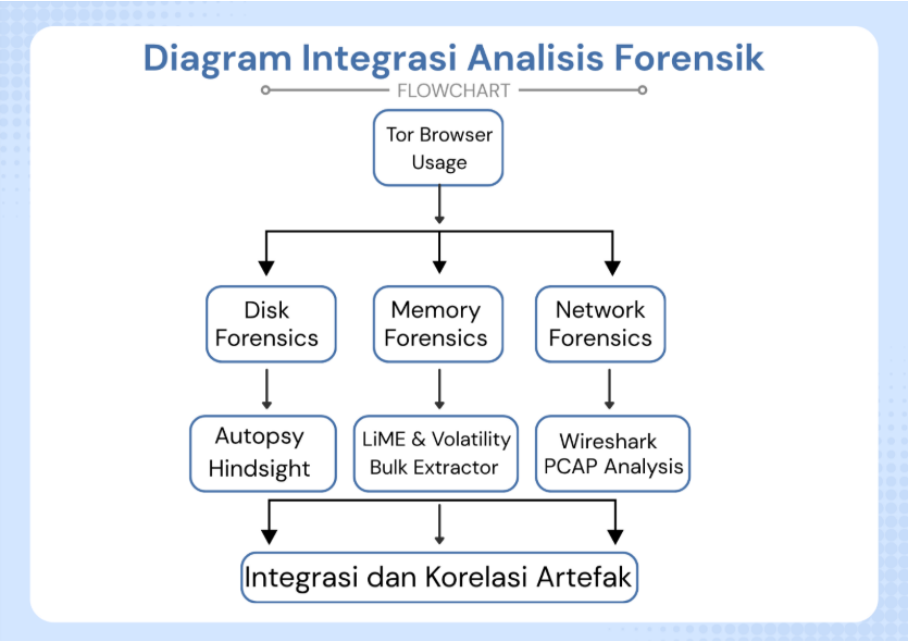
Hasil analisis menunjukkan bahwa beberapa artefak spesifik masih dapat ditemukan pada sistem setelah penggunaan *Tor Browser* [14];[15]. Analisis media penyimpanan ditemukan file seperti *places.sqlite*, *cookies.sqlite*, *sessionstore.jsonlz4*, direktori *cache browser*, dan file log sementara yang tersimpan pada direktori */home/user/.tor-browser/*. Analisis menggunakan Volatility menunjukkan keberadaan proses *tor.real* dan *firefox.real*. Selain itu, beberapa *string* URL dan metadata sesi masih ditemukan pada area memori volatil meskipun aplikasi telah ditutup.

Analisis jaringan menggunakan Wireshark, komunikasi Tor menemukan pola koneksi terenkripsi berbasis protokol TCP dengan distribusi ukuran paket yang relatif konsisten pada beberapa sesi eksperimen. Walaupun isi komunikasi tidak dapat didekripsi, pola *burst traffic* masih dapat diamati dan digunakan sebagai indikator aktivitas jaringan Tor.

4.2.13 Diagram Integrasi Analisis Forensik

Proses investigasi dimulai dari penggunaan Tor Browser yang kemudian dianalisis melalui tiga pendekatan utama, yaitu *disk forensics, memory forensics, dan network forensics.* Pada sisi *disk forensics*, analisis dilakukan menggunakan *Autopsy* dan *Hindsight* untuk mengidentifikasi artefak seperti cache browser, basis data *SQLite*, dan metadata sistem. Pada *memory forensics*, proses akuisisi dan analisis memori dilakukan menggunakan *LiME, Volatility*, dan *Bulk Extractor* untuk menemukan residu data volatil, proses aktif, serta potongan URL sementara. Sementara itu, *network forensics* dilakukan menggunakan *Wireshark* melalui analisis file *PCAP* untuk mengamati pola komunikasi jaringan Tor.

Seluruh hasil analisis kemudian diintegrasikan untuk melakukan korelasi artefak digital dari berbagai sumber data sehingga aktivitas penggunaan *Tor Browser* dapat direkonstruksi secara lebih komprehensif. Hubungan antar pendekatan *host-based digital forensics* yang digunakan dalam penelitian seperti pada gambar 2.



Gambar 3. Integrasi *Host-Based Digital Forensics*

5. Kesimpulan

Penelitian ini berhasil menunjukkan bahwa penggunaan *Tor Browser* pada sistem operasi *BackBox Linux* masih meninggalkan berbagai artefak digital yang dapat dianalisis melalui pendekatan *host-based digital forensics*. Artefak ditemukan pada media penyimpanan, memori volatil, maupun lalu lintas jaringan meskipun *Tor* dirancang untuk mendukung anonimitas pengguna. Hasil penelitian menunjukkan bahwa perubahan perilaku pengguna dapat meningkatkan jumlah artefak lokal yang tersimpan pada sistem. Selain itu, residu data seperti *SQLite database*, *cache browser*, metadata sesi, dan jejak memori masih dapat ditemukan setelah aplikasi ditutup maupun sistem direstart. Analisis lintas sesi juga menunjukkan adanya kemungkinan korelasi aktivitas pengguna melalui pendekatan *timeline analysis*. Analisis pada sisi jaringan, pola komunikasi *Tor network* memperlihatkan karakteristik trafik yang relatif konsisten walaupun isi komunikasi tetap terenkripsi [24]. Sementara itu, pengujian pada lingkungan virtualisasi menunjukkan bahwa penggunaan *virtual machine* dapat mengurangi jumlah residu artefak, namun tidak sepenuhnya menghilangkan jejak aktivitas digital pengguna.

Penelitian ini memberikan kontribusi dalam pengembangan studi forensik digital berbasis host terhadap browser anonim pada lingkungan Linux melalui integrasi pendekatan *disk forensics*, *memory forensics*, dan *network forensics*. Pendekatan tersebut memungkinkan proses identifikasi artefak dilakukan secara lebih komprehensif pada penggunaan *Tor Browser* sejalan dengan perkembangan penelitian *browser forensics* dan *Tor artifact* analysis terkini [14];[15].
Penelitian selanjutnya disarankan untuk mengembangkan pengujian pada distribusi Linux lainnya, menerapkan pendekatan *live network analysis*, serta mengevaluasi teknik *deanonymization* yang lebih kompleks pada jaringan *Tor*.

Daftar Pustaka

[1] H. F. Nugranto and M. Koprawi, "Investigasi Kejahatan Siber pada Surface Web dan Deep Web Menggunakan Metode NIST," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 11, No.1, no. https://jurnal.mdp.ac.id/index.php/jatisi/article/view/3245, pp. 1–5, Mar. 2024, doi: https://doi.org/10.35957/jatisi.v11i1.3245.

[2] G. Z. Muflih, I. Riadi, A. Yudhana, and H. I. Azmi, "Comparison of Forensic Tools on Social Media Services Using the Digital Forensic Research Workshop Method," *J. Inform. dan Komputer) Accredit. KEMENDIKBUD RISTEK*, vol. 6, no. 1, 2023, doi: 10.33387/jiko.v6i1.5872.

[3] I. Sihaloho, A. Widjajarto, and M. T. Kurniawan, "Analisis Penilaian Metrik Anonymity dan Privacy pada Kodachi Linux," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 10, no. 3, pp. 2355–2365, Aug. 2025, doi: 10.29100/jipi.v10i3.6437.

[4] J. Saleem, R. Islam, and M. A. Kabir, "The Anonymity of the Dark Web: A Survey," *IEEE Access*, vol. 10, pp. 33628–33660, 2022, doi: 10.1109/ACCESS.2022.3161547.

[5] H. Hariani, "Eksplorasi Web Browser Dalam Pencarian Bukti Digital Menggunakan Sqlite Hariani 1," *J. INSTEK (Informatika Sains Dan Teknol.*, vol. 6, no. https://journal.uin-alauddin.ac.id/index.php/instek/issue/view/1321, pp. 66–74, Jan. 2021, doi: https://doi.org/10.24252/instek.v6i1.18638.

[6] M. Syukri, I. Riadi, and T. Sutikno, "Validation and Evaluation of Browser Forensics Using Digital Forensic Approach Based on the National Institute of Standards and Technology (NIST) Framework," *J. Tek. Inform.*, vol. 6, no. 4, pp. 2516–2529, Sep. 2025, doi: 10.52436/1.jutif.2025.6.4.4977.

[7] H. Idhofi and G. Zaida Muflih, "Akuisisi Barang Bukti Digital pada Media Penyimpanan Flashdisk Menggunakan Framework National Institute of Justice (NIJ)," 2025.

[8] A. Tofik and G. Zaida Muflih, "Akuisisi Barang Bukti Digital pada Aplikasi Discord Menggunakan Metode ACPO," 2024.

[9] W. Sanjaya, B. Sugiantoro, and Y. Prayudi, "A Metode Offline Forensik Untuk Analisis Digital Artefak Pada TOR Browser Di Sistem Operasi Linux," *JITU J. Inform. Technol. Commun.*, vol. 4, no. 2, pp. 41–51, Jun. 2020, doi: 10.36596/jitu.v4i2.345.

[10] A. Fitriani Shabira and F. Fachri, "Analisis Forensik Digital Pada File Steganografi Menggunakan Ftk Imager Dan Winhex Dalam Kasus Peredaran Narkoba Dengan Live Forensic," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 10, no. 2, pp. 228–240, Jul. 2025, doi: 10.36341/rabit.v10i2.6020.

[11] 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, Apr. 2023, doi: https://doi.org/10.32493/jtsi.v6i2.31535.

[12] A. S. Rido and F. Fachri, "Identifikasi Bukti Digital Whatsapp pada Sistem Operasi Propietary Menggunakan Live Forensics," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 2, pp. 1043–1051, Jun. 2024, doi: 10.29100/jipi.v9i2.5238.

[13] M. N. Bahreisy, R. Rahmadi, and Y. Prayudi, "Analisis Halaman Darkweb Untuk Mendukung Investigasi Kejahatan," *J. Inform. dan Komputer) Akreditasi KEMENRISTEKDIKTI*, vol. 4, no. 1, pp. 2614–8897, 2021, doi: 10.33387/jiko.

[14] M. S. Javed *et al.*, "Analyzing Tor Browser Artifacts for Enhanced Web Forensics, Anonymity, Cybersecurity, and Privacy in Windows-Based Systems," *Inf.*, vol. 15, no. 8, Aug. 2024, doi: 10.3390/info15080495.

[15] R. R. Chand, N. A. Sharma, and M. A. Kabir, "Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques," Oct. 2024, [Online]. Available: http://arxiv.org/abs/2410.12605

[16] F. G. P. Zamsari and T. Wahyono, "Forensic Investigation of Digital Evidence on Flash Disk with Forensic Process Method Based on NIST," *J. Ecotipe (Electronic, Control. Telecommun. Information, Power Eng.*, vol. 11, no. 1, pp. 88–96, Apr. 2024, doi: 10.33019/jurnalecotipe.v11i1.4489.

[17] A. R. Triyanto and F. Fachri, "Analisis Forensik Bukti Digital pada Kejahatan Pembunuhan Berencana Menggunakan Metode National Institute of Justice," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 2, pp. 1031–1042, Jun. 2024, doi: 10.29100/jipi.v9i2.5558.

[18] 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.

[19] E. Daraghmi, Z. Qaroush, M. Hamdi, and O. Cheikhrouhou, "Forensic Operations for Recognizing SQLite Content (FORC): An Automated Forensic Tool for Efficient SQLite Evidence Extraction on Android Devices," *Appl. Sci.*, vol. 13, no. 19, Oct. 2023, doi: 10.3390/app131910736.

[20] M. C. Ghanem, E. Almeida Palmieri, W. Sowinski-Mydlarz, S. Al-Sudani, and D. Dunsin, "Weaponized IoT: A Comprehensive Comparative Forensic Analysis of Hacker Raspberry Pi and PC Kali Linux Machine," *Internet of Things*, vol. 6, no. 1, Mar. 2025, doi: 10.3390/iot6010018.

[21] G. Choi, J. Bang, S. Lee, and J. Park, "Chracer: Memory analysis of Chromium-based browsers," *Forensic Sci. Int. Digit. Investig.*, vol. 46, Oct. 2023, doi: 10.1016/j.fsidi.2023.301613.

[22] I. Hamid and M. M. H. Rahman, "A Comprehensive Literature Review on Volatile Memory Forensics," Aug. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/electronics13153026.

[23] J. Bergman and O. B. Popov, "Recognition of tor malware and onion services," *J. Comput. Virol. Hacking Tech.*, vol. 20, no. 2, pp. 261–275, Jun. 2024, doi: 10.1007/s11416-023-00476-z.

[24] P. Choorod, T. J. Bauer, and A. Aßmuth, "Distinguishing Tor From Other Encrypted Network Traffic Through Character Analysis," May 2024, [Online]. Available: http://arxiv.org/abs/2405.09412