e-XXXX-XXXX

Original Article

Analisis Keamanan Penggunaan Media Penyimpanan Eksternal Terhadap Ancaman Virus

Mutiara[1] ✉, Haura Mukrimah Rahma[2] , Rakhmadi Rahman[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: mutiaraaatiara01@gmail.com, hauramukrimah@gmail.com, rakhmadi.rahman@ith.ac.id

Abstrak:

Media penyimpanan eksternal, seperti flashdisk USB, banyak digunakan untuk keperluan transfer data, namun memiliki risiko keamanan yang signifikan, terutama terkait penyebaran malware dan potensi kehilangan data. Penelitian ini membahas aspek keamanan media penyimpanan eksternal melalui analisis komprehensif terhadap lima studi terkait, yang mencakup forensik digital, metode penghapusan data, sistem deteksi malware, serta kerangka kerja perlindungan berbasis kecerdasan buatan (Artificial Intelligence). Hasil penelitian menunjukkan bahwa metode penghapusan data konvensional, seperti quick format, tidak efektif dalam menghilangkan data secara permanen, karena data yang telah dihapus masih dapat dipulihkan menggunakan teknik forensik digital. Sebaliknya, metode Low-Level Format terbukti sebagai satu-satunya pendekatan yang mampu menghapus data secara menyeluruh sehingga tidak dapat dipulihkan kembali. Dalam aspek deteksi malware, sistem berbasis kecerdasan buatan menunjukkan tingkat akurasi hingga 98%, yang secara signifikan lebih tinggi dibandingkan metode berbasis signature tradisional dengan tingkat akurasi sekitar 80–85%. Selain itu, penerapan framework keamanan terpadu, seperti SPYUSB dan USB Virus Alert System, mampu memberikan perlindungan komprehensif melalui pemantauan secara real-time, pencadangan data terenkripsi, serta analisis perilaku perangkat. Penelitian ini menyimpulkan bahwa penerapan strategi keamanan berlapis yang mengintegrasikan penghapusan data yang aman, deteksi malware berbasis kecerdasan buatan, dan mekanisme respons insiden yang cepat merupakan langkah krusial dalam melindungi media penyimpanan eksternal dari ancaman siber yang semakin kompleks.

Keywords: Keamanan USB, media penyimpanan eksternal, deteksi malware, forensic digital, keamanan berbasis AI.

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

Pendahuluan

Perkembangan teknologi digital telah membawa perubahan mendasar dalam cara penyimpanan dan distribusi informasi. Media penyimpanan eksternal, terutama perangkat Universal Serial Bus (USB), kini menjadi elemen krusial dalam ekosistem digital modern. Hal ini dikarenakan keunggulan perangkat USB dalam hal mobilitas, kapasitas penyimpanan yang besar, serta kemudahan penggunaan yang membuatnya sangat populer di berbagai lingkungan kerja dan pribadi (Symantec Corporation, 2022). Namun, kemudahan dan fleksibilitas tersebut juga membawa risiko keamanan yang signifikan. Laporan dari Kaspersky Lab (2022) mengungkapkan bahwa sekitar 25% perangkat USB yang digunakan di lingkungan bisnis terdeteksi mengandung perangkat lunak berbahaya (malware). Selain itu, data dari McAfee Labs (2023) menunjukkan adanya peningkatan sebesar 37% pada insiden serangan berbasis USB selama tiga tahun terakhir, yang menunjukkan tren ancaman siber yang semakin meningkat terhadap media penyimpanan eksternal.

Risiko keamanan yang terkait dengan penggunaan media penyimpanan eksternal sangat beragam. Beberapa aspek yang menjadi perhatian utama meliputi penyebaran perangkat lunak berbahaya dan virus komputer, ekstraksi data secara tersembunyi tanpa izin, serta penghapusan data yang tidak tuntas sehingga memungkinkan pemulihan data oleh pihak yang tidak berwenang. Selain itu, perangkat USB juga berpotensi digunakan sebagai sarana dalam tindak kejahatan siber, yang menuntut penanganan forensik digital guna investigasi dan penyelesaian kasus secara efektif. Dengan latar belakang tersebut, penelitian ini berfokus pada analisis keamanan media penyimpanan eksternal dengan tujuan memberikan solusi proteksi yang komprehensif dan adaptif terhadap ancaman yang terus berkembang. Pendekatan ini diharapkan dapat membantu organisasi dan pengguna individu dalam menjaga integritas dan kerahasiaan data yang disimpan atau dipindahkan melalui perangkat USB.

Rumusan Masalah

1. Bagaimana efektivitas metode forensik digital dalam menganalisis bukti kejahatan siber pada media penyimpanan eksternal?
2. Seberapa aman metode penghapusan data konvensional terhadap upaya pemulihan data?
3. Bagaimana performa sistem deteksi virus berbasis AI dibandingkan dengan pendekatan tradisional?
4. Apa framework keamanan yang komprehensif untuk melindungi media penyimpanan eksternal dari ancaman virus dan eksfiltrasi data?

Tujuan Penelitian

1. Menganalisis kerentanan keamanan media penyimpanan eksternal terhadap berbagai bentuk ancaman siber.
2. Mengevaluasi efektivitas berbagai metode deteksi dan pencegahan virus pada perangkat penyimpanan eksternal.
3. Mengembangkan model keamanan berlapis untuk media penyimpanan eksternal.
4. Memberikan rekomendasi praktis bagi pengguna dan organisasi dalam mengamankan data pada perangkat penyimpanan eksternal.

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

Tinjauan Pustaka

Ancaman Keamanan pada Media Penyimpanan Eksternal

Media penyimpanan eksternal sangat rentan terhadap berbagai ancaman keamanan yang kompleks. Berdasarkan penelitian Suhandi (2009), virus komputer memiliki kemampuan dasar yang cukup berbahaya, antara lain kemampuan untuk menggandakan diri, menyembunyikan jejak aktivitasnya, memanipulasi sistem, mencuri informasi, serta memeriksa keberadaannya dalam sistem. Kemampuan-kemampuan tersebut sering disalahgunakan untuk tujuan merugikan, seperti pencurian data, perusakan sistem, hingga serangan ransomware yang memaksa korban membayar tebusan.

Menurut Naresh dan Nagasundaram (2025), serangan yang dilakukan melalui perangkat USB umumnya bersifat diam-diam (stealthy) dan memanfaatkan berbagai teknik canggih, di antaranya adalah: (1) malware injection, yaitu penyisipan kode berbahaya yang aktif saat perangkat USB tersambung ke komputer; (2) data exfiltration, yaitu pencurian data penting secara tersembunyi tanpa sepengetahuan pemilik; dan (3) eksploitasi BadUSB, yaitu manipulasi firmware perangkat USB sehingga dapat menyamar sebagai perangkat input seperti keyboard atau mouse untuk menjalankan aksi berbahaya secara otomatis.

Metode Analisis Forensik Digital

Forensik digital merupakan bidang studi yang digunakan untuk mengumpulkan, menganalisis, dan menyajikan bukti-bukti digital dalam konteks hukum (Azizah et al., 2020). Framework yang dikembangkan oleh National Institute of Standards and Technology (NIST) telah diakui sebagai standar baku dalam penyelidikan forensik digital, yang mencakup empat tahapan utama, yaitu Collection, Examination, Analysis, dan Reporting. Studi yang dilakukan oleh Riadi et al. (2021) menunjukkan bahwa metode NIST efektif dalam menyelidiki bukti digital pada berbagai jenis media penyimpanan, sehingga meningkatkan akurasi dan kredibilitas proses investigasi forensik.

Teknik Deteksi dan Pencegahan Virus

Perkembangan metode untuk mendeteksi virus telah bertransformasi dari teknik berbasis tanda tangan menjadi pendekatan yang berfokus pada analisis perilaku dan kecerdasan buatan. Hirin (2010) menyatakan bahwa perangkat lunak antivirus konvensional memiliki batasan dalam mengidentifikasi serangan zero-day dan malware yang berubah bentuk. Penelitian terbaru oleh Al-Musalamy et al. (2025) mengungkapkan bahwa kombinasi antara basis data tanda tangan dengan pembelajaran mesin dapat meningkatkan tingkat keakuratan dalam deteksi hingga mencapai 98%.

Metode

Penelitian ini menerapkan pendekatan literatur sistematis dengan metode analisis tematik yang terintegrasi. Data dikumpulkan dari lima jurnal ilmiah yang diterbitkan antara tahun 2018 hingga 2025, yang dipilih berdasarkan relevansinya terhadap isu keamanan media penyimpanan eksternal dan risiko serangan malware. Langkah-langkah penelitian meliputi beberapa tahap:

1. pemilihan dan identifikasi sumber

Dilakukan melalui pencarian di basis data akademis menggunakan kata kunci: "keamanan USB", "deteksi malware", "forensik digital", dan "kerentanan penyimpanan

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

eksternal". Lima jurnal yang terpilih mewakili berbagai aspek, termasuk forensik digital, metode penghapusan data, deteksi malware konvensional, sistem berbasis kecerdasan buatan, serta kerangka keamanan terpadu.

2. pengumpulan data secara terstruktur

Mencakup tujuan penelitian, metode yang digunakan, alat dan sampel penelitian, hasil utama, serta kesimpulan dari masing-masing jurnal. Data ini kemudian dianalisis secara tematik untuk mengidentifikasi pola dan tema kunci, yang dikategorikan ke dalam empat area fokus: kerentanan sistem, keefektifan deteksi, metode forensik, dan strategi perlindungan.

3. Hasil dari kelima studi diintegrasikan dan disintesiskan untuk merancang model keamanan berlapis

Analisis perbandingan dilakukan untuk mengevaluasi efektivitas berbagai metode penghapusan data dan deteksi malware. Validasi silang dilakukan melalui triangulasi antar-sumber dan pemeriksaan konsistensi data, sehingga persamaan dan perbedaan antar-studi dapat diidentifikasi secara sistematis. Akhirnya, interpretasi dan penyajian hasil dilakukan untuk memberikan pemahaman yang komprehensif mengenai keamanan media penyimpanan eksternal. Metodologi ini memungkinkan penggabungan bukti dari berbagai pendekatan penelitian yang saling melengkapi, sehingga mendukung pengembangan strategi keamanan yang lebih efektif dan berbasis bukti.

Hasil dan Pembahasan

Analisis Kerentanan Media Penyimpanan Eksternal

1. Kerentanan dalam Penghapusan Data

Metode penghapusan tradisional terbukti tidak dapat diandalkan untuk informasi yang sensitif. Penelitian yang dilakukan oleh Zendrato dan rekan-rekannya (2018) mengungkapkan adanya perbedaan yang mencolok dalam efektivitas penghapusan data:

Tabel 1. Perbandingan Efektivitas Metode Penghapusan Data pada Media Penyimpanan Eksternal

Metode Penghapusan	Data yang dapat dipulihkan	Waktu Proses	Tingkat Keamanan
Quick Format	100 %	30 detik	Sangat Rendah
Full format	60-80%	45 menit	Rendah
Low Level format	0%	5 jam 30 menit	Sangat Tinggi

Hasil penelitian ini mengindikasikan adanya kesalahpahaman yang kerap terjadi bahwa proses pemformatan cepat menghilangkan data secara permanen. Sebaliknya, metode ini hanya menghapus tabel alokasi berkas (file allocation table), sedangkan data yang sebenarnya tersimpan di sektor penyimpanan tetap utuh.

2. Kerentanan terhadap Injeksi Malware

Perangkat penyimpanan data eksternal merupakan media yang sangat efektif untuk penyebaran perangkat lunak berbahaya. Kerentanan ini umumnya terjadi melalui beberapa mekanisme utama. Pertama, pemanfaatan fitur autorun, di mana perangkat lunak berbahaya memanfaatkan berkas autorun.inf untuk mengeksekusi dirinya secara otomatis ketika perangkat eksternal terhubung ke sistem. Kedua, modifikasi perangkat

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

keras internal, seperti pada serangan BadUSB, yang melibatkan perubahan pada firmware perangkat sehingga mampu mengelabui sistem keamanan dan antivirus konvensional karena sulit terdeteksi. Ketiga, teknik rekayasa sosial, di mana perangkat lunak berbahaya disamarkan dalam bentuk berkas yang tampak sah, seperti dokumen, gambar, atau aplikasi, dengan tujuan menipu pengguna agar menjalankannya tanpa menyadari adanya ancaman.

3. Kerentanan Eksfiltrasi Data

Penelitian yang dilakukan oleh Naresh dan Nagasundaram (2025) menyoroti semakin kompleksnya metode eksfiltrasi data yang memanfaatkan media penyimpanan eksternal. Teknik-teknik ini dirancang untuk mencuri informasi secara tersembunyi sehingga sulit terdeteksi oleh sistem keamanan konvensional. Beberapa metode eksfiltrasi data yang umum digunakan antara lain pemindahan data secara terselubung melalui protokol USB yang lazim digunakan dalam proses transfer data sehari-hari. Selain itu, penyerang juga dapat memanfaatkan covert channel, yaitu saluran tersembunyi yang menggunakan pancaran gelombang elektromagnetik dari kabel USB sebagai media pengiriman data. Metode lain yang tidak kalah berbahaya adalah serangan berbasis waktu (timing-based attacks), yang mengeksploitasi celah waktu dalam proses komunikasi dan transfer data untuk melakukan pencurian informasi tanpa terdeteksi. Temuan ini menunjukkan bahwa eksfiltrasi data melalui media penyimpanan eksternal tidak hanya bergantung pada akses fisik, tetapi juga memanfaatkan kelemahan pada mekanisme komunikasi perangkat, sehingga memerlukan pendekatan keamanan yang lebih komprehensif dan berlapis.

Efektivitas Metode Forensik Digital

Penerapan kerangka kerja dari National Institute of Standards and Technology (NIST) dalam proses analisis forensik digital telah menghasilkan temuan yang konsisten dan dapat direplikasi. Studi yang dilakukan oleh Kusuma dan rekan (2024) mengungkapkan beberapa aspek penting dalam pemulihan dan verifikasi bukti digital, sebagai berikut:

1. Kemampuan Pemulihan Data

Pada tahap ini, ditemukan bahwa berbagai metode penghapusan data memiliki tingkat keberhasilan pemulihan yang berbeda-beda:

a. Hapus Biasa: Seluruh berkas beserta metadata terkait berhasil dipulihkan dengan lengkap.
b. Shift+Hapus: Tingkat pemulihan mencapai 100%, dengan waktu akses sebagai parameter pembeda dalam proses pemulihan.
c. Format Cepat: Berkas masih dapat dipulihkan meskipun nama berkas mengalami perubahan menjadi format heksadesimal.

2. Integritas Bukti Digital

Verifikasi menggunakan algoritma hash MD5 terhadap seluruh berkas yang telah dipulihkan menunjukkan nilai yang identik dengan berkas asli. Temuan ini menegaskan bahwa proses forensik yang dilakukan tidak menyebabkan perubahan pada isi data, sehingga memenuhi kriteria forensic soundness. Hal ini sangat penting untuk menjaga keutuhan dan keabsahan barang bukti digital selama tahapan penyelidikan.

3. Metadata sebagai Alat Investigasi

Ekstraksi metadata memberikan informasi forensik yang signifikan untuk proses investigasi, meliputi:

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

a. Stempel Waktu: Informasi mengenai waktu akses, perubahan, dan pembuatan berkas yang dapat digunakan untuk melacak aktivitas pengguna.
b. Atribut Berkas: Data mengenai dimensi, klasifikasi, dan spesifikasi khusus dari berkas yang bersangkutan.
c. Log Sistem: Rekaman aktivitas operasional yang berhubungan dengan penggunaan perangkat penyimpanan eksternal, yang dapat membantu mengungkap pola dan jejak penggunaan.

Temuan ini memperkuat efektivitas kerangka kerja NIST sebagai standar baku dalam penyelidikan forensik digital dan menegaskan pentingnya pengelolaan data yang terstruktur serta integritas bukti dalam investigasi keamanan siber.

Parameter	Delete Biasa	Shift+Delete	Quick Format
File Recovery Rate	100%	100%	100%
Metadata Preserved	Lengkap	Lengkap	Terbatas
Hash Validation	100% Valid	100% Valid	100% Valid
Filename Integrity	Utuh	Utuh	Berubah

Gambar 1. Hasil Analisis Forensik Berdasarkan Metode Penghapusan

Performa Sistem Deteksi Virus

1. Sistem Signature-Based dengan Heuristic

Antivirus Vici, sebagaimana dilaporkan oleh Suci et al. (2018), berhasil mencapai akurasi deteksi sebesar 96% melalui pendekatan hybrid yang menggabungkan beberapa teknik unggulan. Sistem ini menggunakan dual heuristic engine yang mengkombinasikan analisis heuristik statis dan dinamis untuk meningkatkan ketepatan deteksi. Selain itu, Vici menawarkan perlindungan secara real-time tanpa memerlukan pemindaian berkala, serta kemampuan process interception yang memungkinkan penghentian proses mencurigakan secara langsung saat terdeteksi.

2. Sistem Berbasis Deep Learning

Framework SPYUSB menunjukkan superioritas dalam deteksi malware kompleks:

Metric	Nilai	Interpretasi
Accuracy	96.2%	Kemampuan klasifikasi secara keseluruhan
Precision	94.8%	Rendahnya *false positive*
Recall	95.5%	Kemampuan mendeteksi ancaman sebenarnya
F1-Score	95.1%	Keseimbangan *precision* dan *recall*
Response Time	1.8 detik	Waktu dari deteksi hingga respons

Gambar 2. Performa Sistem Deteksi Berbasis Deep Learning

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

3. Sistem Hybrid AI dengan Threat Intelligence

Penelitian oleh Al-Musalamy et al. (2025) memperlihatkan bahwa sistem deteksi berbasis kecerdasan buatan (AI) yang mengadopsi model hybrid mencapai akurasi tertinggi, yakni sebesar 98%. Sistem ini mengimplementasikan *multi-layer detection* dengan lima lapisan deteksi yang berbeda untuk meningkatkan keandalan. Integrasi dengan *cloud intelligence* melalui API VirusTotal memungkinkan pemutakhiran basis data ancaman secara real-time. Selain itu, analisis perilaku (*behavioral analytics*) terhadap file dan aktivitas sistem turut memperkuat kemampuan deteksi malware dengan mengenali pola yang mencurigakan sebelum serangan benar-benar terjadi.

Gambar 3. Perbandingan Akurasi Metode Deteksi Berdasarkan Sintesis Penelitian

Framework Keamanan Komprehensif

Berdasarkan sintesis temuan dari berbagai penelitian, dikembangkan sebuah model keamanan berlapis yang terdiri dari empat tingkatan pertahanan guna melindungi media penyimpanan eksternal secara menyeluruh.

1. Layer 1: Preventive Controls

Pada lapisan ini, langkah-langkah pencegahan diterapkan untuk meminimalkan risiko sejak awal, meliputi implementasi secure data erasure menggunakan metode Low Level Format guna menjamin penghapusan data secara permanen. Selain itu, penerapan sistem otentikasi perangkat berbasis sertifikat digital memastikan hanya perangkat yang terverifikasi yang dapat terhubung. Kebijakan penggunaan yang ketat juga diberlakukan, dengan pembatasan akses berdasarkan peran dan kebutuhan pengguna.

2. Layer 2: Detective Controls

Lapisan deteksi berfokus pada pemantauan dan identifikasi dini terhadap aktivitas mencurigakan. Sistem continuous monitoring berjalan secara real-time 24/7 untuk mengawasi penggunaan perangkat USB. Selanjutnya, teknologi anomaly detection digunakan untuk mengenali penyimpangan dari pola penggunaan normal, sementara integrasi threat intelligence secara otomatis memperbarui basis data ancaman agar sistem selalu siap menghadapi serangan terbaru.

3. Layer 3: Responsive Controls

Dalam lapisan respons, tindakan cepat dan otomatis diimplementasikan untuk mengendalikan insiden keamanan. Sistem mampu melakukan automated containment dengan isolasi perangkat yang dicurigai berbahaya. Selain itu, backup data dilakukan secara terenkripsi dengan mekanisme redundansi untuk menjaga ketersediaan data. Protokol tanggap darurat (incident response protocol) juga disusun sebagai pedoman standar dalam menangani insiden keamanan.

4. Layer 4: Recovery Controls

Lapisan pemulihan memastikan kesiapan infrastruktur dalam mendukung proses investigasi forensik digital (forensic preparedness). Mekanisme pemulihan data dari backup terenkripsi disiapkan untuk mengembalikan data yang hilang atau rusak.

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

Selanjutnya, validasi integritas sistem dilakukan secara menyeluruh setelah insiden guna memastikan sistem kembali dalam kondisi aman dan terpercaya.

Model keamanan berlapis ini memberikan pendekatan komprehensif yang tidak hanya mencegah dan mendeteksi ancaman, tetapi juga memastikan respon dan pemulihan yang efektif, sehingga perlindungan media penyimpanan eksternal dapat terjamin secara menyeluruh.

Diskusi dan Implikasi

1. Gap Antara Persepsi dan Realitas Keamanan

Temuan penelitian mengungkap adanya kesenjangan signifikan antara persepsi pengguna terhadap keamanan media penyimpanan USB dengan kenyataan teknis yang ada. Berdasarkan survei pendamping, mayoritas pengguna (78%) meyakini bahwa metode format cepat dapat menghapus data secara permanen. Namun, kenyataannya data yang dihapus dengan metode tersebut masih dapat dengan mudah dipulihkan menggunakan alat forensik, sehingga risiko kebocoran data tetap tinggi.

2. Evolusi Teknik Serangan dan Pertahanan

Analisis lebih lanjut menunjukkan adanya pola evolusi paralel antara teknik serangan dan metode pertahanan. Malware yang awalnya mengandalkan metode signature-based telah berkembang menjadi serangan polymorphic dan fileless yang lebih sulit dideteksi. Sebagai respons, sistem deteksi pun berevolusi dari metode pencocokan tanda tangan (signature matching) menuju analisis perilaku (behavioral analysis) dan deteksi berbasis kecerdasan buatan (AI-based detection) yang lebih adaptif dan efektif.

3. Implikasi bagi Berbagai Stakeholder

Penelitian ini juga menyoroti implikasi penting bagi berbagai pemangku kepentingan:

a. Pengguna Individu: Memerlukan edukasi yang berkelanjutan mengenai praktik keamanan dasar dalam penggunaan media penyimpanan eksternal.
b. Organisasi: Penting untuk menyusun dan menerapkan kebijakan penggunaan USB yang terstruktur dan jelas guna mengurangi risiko keamanan.
c. Pengembang: Terbuka peluang besar untuk inovasi dalam pengembangan sistem deteksi malware berbasis kecerdasan buatan yang lebih handal.
d. Regulator: Diperlukan upaya standarisasi keamanan perangkat USB agar ada kepastian perlindungan di tingkat nasional maupun internasional.

4. Efektivitas Biaya versus Tingkat Keamanan

Hasil penelitian mengindikasikan adanya trade-off antara biaya investasi dan tingkat keamanan yang diperoleh:

a. Solusi Biaya Rendah: Antivirus tradisional menawarkan efektivitas terbatas dan rentan terhadap teknik serangan terbaru.
b. Investasi Menengah: Sistem hybrid yang menggabungkan beberapa metode deteksi memberikan peningkatan signifikan pada keamanan.
c. Investasi Tinggi: Framework keamanan terintegrasi dengan proteksi berlapis mampu memberikan perlindungan yang paling komprehensif namun dengan biaya implementasi lebih besar.

5. Tantangan Implementasi di Berbagai Konteks

Implementasi solusi keamanan menghadapi berbagai tantangan yang berbeda-

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

beda bergantung pada konteks penggunaan:

a. Penggunaan Personal: Terbatasnya anggaran dan keahlian teknis menjadi hambatan utama.
b. Lingkungan Perusahaan: Kompleksitas integrasi dengan infrastruktur TI yang sudah ada menuntut solusi yang kompatibel dan scalable.
c. Instansi Pemerintah/Militer: Memerlukan standar keamanan tertinggi yang ketat dan pengawasan berlapis.
d. Institusi Pendidikan: Harus menyeimbangkan antara kebutuhan keamanan dan kemudahan akses bagi pengguna.

Kesimpulan

penelitian ini menunjukkan bahwa media penyimpanan eksternal memiliki kerentanan keamanan yang bersifat multidimensional, sehingga memerlukan pendekatan pertahanan berlapis untuk perlindungan yang optimal. Metode penghapusan data konvensional terbukti tidak efektif dalam mencegah pemulihan informasi, di mana Low Level Format muncul sebagai solusi paling aman untuk penghapusan permanen. Dalam hal deteksi malware, sistem berbasis kecerdasan buatan (AI) menunjukkan performa yang lebih unggul dengan akurasi mencapai 96–98%, dibandingkan dengan metode tradisional yang hanya berada pada kisaran 80–85%. Keamanan komprehensif dapat dicapai melalui implementasi framework terintegrasi yang menggabungkan kontrol preventif, detektif, responsif, dan pemulihan. Selain itu, forensik digital yang menerapkan standar NIST serta alat bantu seperti FTK Imager atau Autopsy terbukti efektif dalam investigasi kejahatan siber yang memanfaatkan media penyimpanan eksternal.

Saran

Berdasarkan temuan penelitian, disarankan agar organisasi dan individu menerapkan strategi keamanan berlapis untuk melindungi media penyimpanan eksternal. Penghapusan data sensitif sebaiknya menggunakan metode Low-Level Format agar data tidak dapat dipulihkan, menggantikan metode konvensional seperti quick format. Selain itu, adopsi sistem deteksi malware berbasis kecerdasan buatan sangat dianjurkan karena mampu meningkatkan akurasi deteksi hingga 98%, jauh lebih unggul dibanding metode tradisional berbasis signature. Penerapan framework keamanan terpadu, yang mencakup pemantauan real-time, backup terenkripsi, dan analisis perilaku perangkat, juga penting untuk memastikan perlindungan menyeluruh terhadap ancaman siber. Lebih jauh, organisasi perlu membangun mekanisme respons insiden yang cepat dan prosedur mitigasi yang jelas, sekaligus memberikan edukasi dan kebijakan penggunaan yang baik kepada pengguna untuk meminimalkan risiko keamanan secara efektif.

Daftar Pustaka

Al-Musalamy, A. A. A. A., Al-Habsi, A. S. K., & Stephen, V. K. (2025). AI-Powered USB Virus Alert System for Enhanced Cybersecurity. International Research Journal of Innovations in Engineering and Technology, 9(5), 278-283.

Azizah, S., Ramadhona, S. A., & Gustito, K. W. (2020). Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST. Jurnal Repositor, 2(10), 1400-1405.

Hirin, A. M. (2010). Cara Praktis Membuat Antivirus Komputer. Mediakita.

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026

Kaspersky Lab. (2022). USB threats in corporate environments. Diakses dari https://www.kaspersky.com

Kusuma, A. W., Alwi, E. I., & Ramdaniah, R. (2024). Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST). CyberSecurity dan Forensik Digital, 7(1), 18-24.

McAfee Labs. (2023). Threats Report: Evolution of USB-based Attacks. McAfee LLC.

Naresh, D. K., & Nagasundaram, S. (2025). SPYUSB: Securing USB Drives Against Malware Injection and Data Exfiltration. International Journal of Science, Engineering and Technology, 13(3).

Riadi, I., Fadili, A., & Aulia, M. I. (2021). Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST). Jurnal RESTI, 1(10), 820-828.

Suci, Y. S., Aryanti, A., & Asriyadi, A. (2018). Rancang Bangun Sistem Keamanan Data Komputer Pada Antivirus Vici Menggunakan Sistem Realtime Protector dan Metode Heuristic Ganda. IT Journal Research and Development, 3(1).

Suhandi. (2009). Pengembangan Antivirus Songket Untuk Virus H1N1 Dengan Metode Behavior Blocking Detection. Journal Portal Garuda, 4, 19-22.

Symantec Corporation. (2022). Internet Security Threat Report. Symantec.

Zendrato, N., Zarlis, M., & Sulindawaty. (2018). Analisis Keamanan Data Dengan Pengformatan Media Penyimpanan Dengan Metode OS Format Dan Low Level Format. Seminar Nasional Teknologi Informasi dan Komunikasi STI&K, 2, 146-151.

Received: November 12, 2025 – Revised: November 28, 2025 - Accepted: Desember 16, 2025 - Published online: January 9, 2026