INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 268-280, ISSN: 3123-5573 (Online)

Analisis Digital Forensik pada Insiden Serangan *Malware* di Sistem Operasi

Rakhmadi Rahman[1], Fatha Mutia Nur Inayah[2], Dea Apriyani[3]
[1,2,3] Information Systems Bacharuddin Jusuf Habibie Institute of Technology Parepare
rakhmadi.rahman@ith.ac.id[1], fathamuthianurinayah.241031083@mahasiswa.ith.ac.id[2],
apriyanidea.241031077@mahasiswa.ith.ac.id[3]

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:
Digital Forensics, Malware, Operating Systems, Cybersecurity

ABSTRACT

Malware attacks are one of the main threats to the security of the Windows operating system because they can cause system damage, data theft, and information technology service disruptions. The complexity of the Windows operating system architecture makes the process of investigating malware incidents require a systematic and structured digital forensic approach. This study aims to analyze the application of digital forensics in identifying, analyzing, and reconstructing malware attack incidents on the Windows operating system through the examination of the resulting digital artifacts. The research method used is an experimental method by simulating malware infection in a controlled Windows environment, then forensic investigation is carried out based on the stages of identification, acquisition, analysis, and reporting. The digital artifacts analyzed include the Windows Registry, Windows Event Log, NTFS file system, and memory (RAM). The results of the study show that the digital forensic approach is able to comprehensively uncover malware activities, ranging from the initial infection process, persistence mechanisms, to hidden activities in memory that are not detected through disk-based analysis. This research is expected to contribute to the development of malware forensic investigation methods and improve the readiness to handle cybersecurity incidents on the Windows operating system.

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
Digital Forensik, Malware, Sistem Operasi, Keamanan siber

ABSTRAK

Serangan malware merupakan salah satu ancaman utama terhadap keamanan sistem operasi Windows karena dapat menyebabkan kerusakan sistem, pencurian data, serta gangguan layanan teknologi informasi. Kompleksitas arsitektur sistem operasi Windows menjadikan proses investigasi insiden malware memerlukan pendekatan digital forensik yang sistematis dan terstruktur. Penelitian ini bertujuan untuk menganalisis penerapan digital forensik dalam mengidentifikasi, menganalisis, dan merekonstruksi insiden serangan malware pada sistem operasi Windows melalui pemeriksaan artefak digital yang dihasilkan. Metode penelitian yang digunakan adalah metode eksperimental dengan melakukan simulasi infeksi malware pada lingkungan Windows yang terkontrol, kemudian dilakukan investigasi forensik berdasarkan tahapan identifikasi, akuisisi, analisis, dan pelaporan. Artefak digital yang dianalisis meliputi Windows Registry, Windows Event Log, sistem file NTFS, serta memory (RAM). Hasil penelitian menunjukkan bahwa pendekatan digital forensik mampu mengungkap aktivitas malware secara komprehensif, mulai dari proses infeksi awal, mekanisme persistensi, hingga aktivitas tersembunyi di dalam memory yang tidak terdeteksi melalui analisis berbasis disk. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan metode investigasi forensik malware serta meningkatkan kesiapan penanganan insiden keamanan siber pada sistem operasi Windows.

INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 268-280, ISSN: 3123-5573 (Online)

Corresponding Author:
Rakhmadi Rahman
Information Systems Bacharuddin Jusuf Habibie Institute of Technology
E-mail: rakhmadi.rahman@ith.ac.id

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong pemanfaatan sistem komputer secara luas di berbagai sektor, seperti pemerintahan, pendidikan, industri, kesehatan, dan layanan publik. Sistem komputer saat ini tidak hanya digunakan sebagai alat bantu kerja, tetapi telah menjadi infrastruktur utama dalam pengelolaan data, pengambilan keputusan, dan penyediaan layanan digital. Dalam ekosistem tersebut, sistem operasi memegang peranan yang sangat penting karena berfungsi sebagai penghubung antara perangkat keras (hardware), perangkat lunak (software), dan pengguna. Sistem operasi mengatur alokasi sumber daya, mengelola proses, serta memastikan aplikasi dapat berjalan secara stabil dan aman.

Microsoft Windows merupakan salah satu sistem operasi yang paling banyak digunakan di dunia, baik pada lingkungan personal maupun organisasi. Popularitas Windows disebabkan oleh kemudahan penggunaan, kompatibilitas perangkat lunak yang luas, serta dukungan ekosistem aplikasi yang sangat besar. Namun, dominasi penggunaan sistem operasi Windows juga menjadikannya target utama berbagai ancaman keamanan siber, khususnya serangan malware. Penyerang sering memanfaatkan celah keamanan pada sistem operasi Windows untuk menyusupkan perangkat lunak berbahaya dengan tujuan mencuri data, merusak sistem, atau mengganggu layanan teknologi informasi.

Malware merupakan salah satu bentuk ancaman keamanan siber yang paling kompleks dan terus berkembang. Malware dirancang untuk beroperasi secara tersembunyi dan sulit terdeteksi oleh pengguna awam. Pada sistem operasi Windows, malware dapat memanfaatkan berbagai mekanisme internal sistem, seperti Windows Registry, layanan sistem, task scheduler, serta memory, untuk mempertahankan persistensi dan menghindari deteksi. Akibatnya, serangan malware tidak hanya menimbulkan kerusakan teknis, tetapi juga berpotensi menyebabkan kerugian finansial, kebocoran data sensitif, serta penurunan kepercayaan terhadap sistem teknologi informasi yang digunakan.

Dalam banyak kasus insiden keamanan siber, serangan malware tidak langsung terdeteksi pada saat awal infeksi. Malware sering kali bekerja secara pasif dalam jangka waktu tertentu sebelum melakukan aksi utama, seperti eksfiltrasi data atau sabotase sistem. Selama periode tersebut, malware meninggalkan jejak digital dalam bentuk artefak digital yang tersimpan pada sistem operasi. Artefak digital ini dapat berupa log aktivitas sistem, perubahan konfigurasi registry, modifikasi file sistem, serta aktivitas proses yang terekam di dalam memory. Namun, jejak digital tersebut sering kali tersebar di berbagai komponen sistem dan tidak mudah dianalisis tanpa pendekatan yang sistematis.

Digital forensik merupakan disiplin ilmu yang berfokus pada proses identifikasi, pengumpulan, analisis, dan pelaporan bukti digital yang berasal dari perangkat elektronik. Dalam konteks keamanan siber, digital forensik berperan penting dalam investigasi insiden

serangan malware. Pendekatan digital forensik memungkinkan investigator untuk mengungkap aktivitas malware secara teknis, merekonstruksi kronologi serangan, serta mengidentifikasi dampak yang ditimbulkan terhadap sistem. Proses ini sangat penting tidak hanya untuk pemulihan sistem, tetapi juga untuk keperluan pembuktian hukum dan peningkatan strategi keamanan di masa mendatang.

Sistem operasi Windows memiliki karakteristik dan kompleksitas tersendiri yang menjadikan proses investigasi forensik malware sebagai tantangan yang cukup besar. Windows menyimpan berbagai informasi penting dalam struktur internal yang kompleks, seperti registry hive, event log, file system NTFS, dan memory volatile. Setiap komponen tersebut menyimpan artefak digital yang dapat memberikan informasi berharga mengenai aktivitas malware. Namun, tanpa pemahaman yang mendalam mengenai struktur dan mekanisme kerja sistem operasi Windows, artefak digital tersebut sulit untuk diinterpretasikan secara akurat.

Penelitian sebelumnya menunjukkan bahwa pendekatan digital forensik yang terstruktur mampu memberikan gambaran yang jelas mengenai perilaku malware pada sistem operasi Windows. Analisis terhadap Windows Event Log dapat mengungkap aktivitas abnormal yang berkaitan dengan eksekusi program dan perubahan sistem. Pemeriksaan Windows Registry dapat mengidentifikasi mekanisme persistensi malware. Analisis sistem file NTFS dapat menunjukkan perubahan file yang mencurigakan, sedangkan analisis memory forensik mampu mengungkap proses malware yang berjalan secara tersembunyi di dalam RAM. Oleh karena itu, integrasi berbagai teknik forensik menjadi kunci dalam investigasi insiden malware yang efektif.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada analisis digital forensik terhadap insiden serangan malware pada sistem operasi Windows. Penelitian ini bertujuan untuk mengkaji penerapan tahapan digital forensik dalam mengidentifikasi, menganalisis, dan merekonstruksi aktivitas malware melalui pemeriksaan artefak digital utama pada sistem operasi Windows. Metode yang digunakan dalam penelitian ini adalah metode eksperimental dengan melakukan simulasi infeksi malware pada lingkungan Windows yang terkontrol, sehingga perilaku malware dapat diamati dan dianalisis secara mendalam.Kontribusi dari penelitian ini diharapkan dapat memberikan pemahaman teknis yang lebih komprehensif mengenai proses investigasi forensik malware pada sistem operasi Windows. Selain itu, hasil penelitian ini diharapkan dapat menjadi referensi bagi praktisi keamanan siber, peneliti, dan akademisi dalam mengembangkan metode investigasi forensik yang lebih efektif serta meningkatkan kesiapan dalam menghadapi insiden serangan malware di lingkungan sistem operasi Windows.

TINJAUAN PUSTAKA

a. Digital Forensik

Digital forensik merupakan cabang ilmu forensik yang berfokus pada identifikasi, pengumpulan, analisis, dan pelaporan bukti digital yang berasal dari perangkat elektronik. Bukti digital dapat ditemukan pada berbagai media, seperti komputer, perangkat mobile, jaringan, dan sistem penyimpanan digital. Dalam konteks keamanan siber, digital forensik berperan penting dalam menangani insiden serangan siber, termasuk serangan malware,

dengan tujuan mengungkap aktivitas yang terjadi di dalam sistem secara teknis dan terstruktur.

Proses digital forensik harus dilakukan secara sistematis dan mengikuti prosedur yang telah ditetapkan untuk menjaga integritas dan keaslian bukti digital. Setiap tindakan yang dilakukan selama investigasi harus terdokumentasi dengan baik agar hasil analisis dapat dipertanggungjawabkan secara teknis maupun hukum. Hal ini menjadi sangat penting ketika hasil investigasi forensik digunakan sebagai bahan evaluasi keamanan sistem atau sebagai alat bukti dalam proses hukum.

Secara umum, tahapan digital forensik terdiri dari empat tahap utama, yaitu identifikasi, akuisisi, analisis, dan pelaporan. Tahap identifikasi bertujuan untuk menentukan sistem yang terlibat dalam insiden serta jenis data yang berpotensi mengandung bukti digital. Tahap akuisisi dilakukan untuk mengambil data dari sistem target secara forensik tanpa mengubah kondisi asli data tersebut. Tahap analisis bertujuan untuk menafsirkan bukti digital guna mengungkap aktivitas yang terjadi pada sistem. Tahap terakhir, yaitu pelaporan, bertujuan untuk menyajikan hasil investigasi dalam bentuk laporan yang sistematis, jelas, dan mudah dipahami. Dalam sistem operasi Windows, penerapan digital forensik memiliki tantangan tersendiri karena kompleksitas arsitektur sistem dan banyaknya artefak digital yang tersebar di berbagai komponen. Oleh karena itu, investigator harus memiliki pemahaman yang mendalam mengenai struktur internal sistem operasi Windows agar proses investigasi dapat dilakukan secara efektif dan akurat.

b. Malware

Malware merupakan perangkat lunak berbahaya yang dirancang untuk melakukan aktivitas yang merugikan sistem atau pengguna. Pada sistem operasi Windows, malware dapat hadir dalam berbagai bentuk, seperti virus, worm, trojan, ransomware, spyware, dan adware. Setiap jenis malware memiliki karakteristik dan tujuan yang berbeda, namun secara umum malware dirancang untuk menyusup ke dalam sistem, menyembunyikan keberadaannya, serta menjalankan aktivitas berbahaya tanpa sepengetahuan pengguna.

Sistem operasi Windows sering menjadi target utama serangan malware karena tingkat penggunaannya yang sangat tinggi serta dukungan ekosistem aplikasi yang luas. Malware pada Windows biasanya masuk ke dalam sistem melalui berbagai vektor serangan, seperti email phishing, file unduhan berbahaya, media penyimpanan eksternal, serta eksploitasi celah keamanan pada aplikasi atau sistem operasi. Setelah berhasil masuk ke dalam sistem, malware akan berusaha untuk mempertahankan persistensinya agar tetap aktif meskipun sistem direstart.Untuk mempertahankan persistensi, malware pada Windows sering memanfaatkan mekanisme internal sistem, seperti memodifikasi Windows Registry, menambahkan layanan

sistem, memanfaatkan task scheduler, atau menyisipkan kode berbahaya ke dalam proses yang sah. Selain itu, beberapa malware modern dirancang untuk beroperasi secara fileless, yaitu menjalankan aktivitas berbahaya langsung di memory tanpa meninggalkan file yang jelas pada sistem file. Teknik ini membuat malware semakin sulit dideteksi dan dianalisis.

Aktivitas malware tersebut meninggalkan berbagai jejak digital pada sistem operasi Windows. Jejak ini dapat berupa perubahan konfigurasi sistem, aktivitas proses yang

mencurigakan, serta komunikasi jaringan yang tidak normal. Oleh karena itu, analisis malware tidak dapat dilepaskan dari pendekatan digital forensik yang mampu mengungkap jejak digital tersebut secara sistematis.

c. Artefak Digital

Artefak digital merupakan jejak aktivitas yang ditinggalkan oleh sistem, pengguna, maupun aplikasi selama sistem beroperasi. Pada sistem operasi Windows, artefak digital memiliki peran yang sangat penting dalam investigasi forensik malware karena dapat digunakan untuk mengungkap aktivitas yang dilakukan oleh malware sebelum, selama, dan setelah infeksi.

Salah satu artefak digital utama pada Windows adalah Windows Registry. Registry menyimpan berbagai konfigurasi sistem dan aplikasi, sehingga sering dimanfaatkan oleh malware untuk menyimpan informasi konfigurasi dan mempertahankan persistensi. Analisis terhadap registry dapat mengungkap keberadaan entri mencurigakan yang dibuat oleh malware, seperti autorun key atau layanan sistem palsu.

Artefak digital lainnya adalah Windows Event Log, yang mencatat berbagai aktivitas sistem, aplikasi, dan keamanan. Event log dapat digunakan untuk mengidentifikasi waktu terjadinya aktivitas mencurigakan, seperti eksekusi program yang tidak dikenal, kegagalan login, atau perubahan konfigurasi sistem. Dengan menganalisis event log, investigator dapat merekonstruksi kronologi kejadian yang berkaitan dengan serangan malware.

Selain itu, sistem file NTFS juga menyimpan artefak digital yang penting, seperti metadata file, timestamp, dan struktur direktori. Malware sering memodifikasi atau menyembunyikan file berbahaya dalam sistem file NTFS. Analisis metadata file dapat membantu investigator mengidentifikasi perubahan file yang mencurigakan serta menentukan waktu terjadinya aktivitas malware.

Artefak digital yang bersifat volatile, seperti memory (RAM), juga sangat penting dalam investigasi malware. Beberapa malware dirancang untuk berjalan secara tersembunyi di memory tanpa meninggalkan jejak yang jelas pada disk. Oleh karena itu, analisis memory forensik menjadi kunci dalam mengungkap proses malware yang aktif, koneksi jaringan tersembunyi, serta teknik injeksi proses yang digunakan oleh malware.

d. Forensik Memory

Forensik memory merupakan bagian dari digital forensik yang berfokus pada analisis data volatile yang tersimpan di dalam memory (RAM). Pada sistem operasi Windows, memory menyimpan berbagai informasi penting, seperti proses yang sedang berjalan, modul yang dimuat, koneksi jaringan aktif, serta data sementara aplikasi. Informasi ini sangat berharga dalam investigasi malware karena banyak malware modern beroperasi secara langsung di memory.

Akuisisi memory harus dilakukan dengan hati-hati karena data volatile akan hilang ketika sistem dimatikan. Oleh karena itu, proses pengambilan memory biasanya dilakukan saat sistem masih dalam keadaan aktif. Data memory yang telah diakuisisi kemudian dianalisis menggunakan tools forensik untuk mengidentifikasi aktivitas mencurigakan yang tidak terlihat pada sistem file.Analisis memory memungkinkan investigator untuk mengungkap malware yang menggunakan teknik stealth, seperti process injection atau reflective DLL injection.

Teknik ini sering digunakan oleh malware untuk menyembunyikan prosesnya di dalam proses yang sah, sehingga sulit terdeteksi oleh mekanisme keamanan konvensional. Dengan demikian, forensik memory menjadi komponen penting dalam investigasi insiden malware pada sistem operasi Windows.

e. Penelitian Terkait Digital Forensik Malware

Beberapa penelitian sebelumnya menunjukkan bahwa pendekatan digital forensik mampu mengungkap aktivitas malware secara detail pada sistem operasi Windows. Penelitian-penelitian tersebut menekankan pentingnya analisis artefak digital, seperti registry, event log, sistem file, dan memory, dalam merekonstruksi kronologi serangan malware. Hasil penelitian menunjukkan bahwa kombinasi analisis artefak digital statis dan volatile memberikan gambaran yang lebih komprehensif mengenai perilaku malware.

Namun, masih terdapat tantangan dalam penerapan digital forensik malware, terutama terkait dengan teknik anti-forensik yang digunakan oleh malware modern. Oleh karena itu, penelitian ini berupaya untuk memperkuat pemahaman mengenai penerapan digital forensik dalam konteks serangan malware pada sistem operasi Windows melalui pendekatan eksperimental yang terstruktur.

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimental dengan pendekatan digital forensik untuk menganalisis insiden serangan malware pada sistem operasi Windows. Metode eksperimental dipilih karena memungkinkan peneliti untuk melakukan simulasi serangan malware dalam lingkungan yang terkontrol, sehingga perilaku malware dan dampaknya terhadap sistem dapat diamati secara sistematis. Pendekatan ini juga memungkinkan proses investigasi forensik dilakukan secara menyeluruh terhadap artefak digital yang dihasilkan selama insiden berlangsung.

Kerangka kerja penelitian ini mengacu pada tahapan standar digital forensik, yaitu identifikasi, akuisisi, analisis, dan pelaporan. Setiap tahapan dilakukan secara berurutan untuk memastikan integritas bukti digital tetap terjaga dan hasil investigasi dapat dipertanggungjawabkan secara ilmiah.

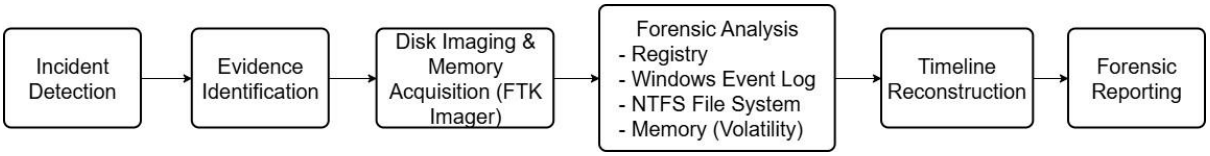
a. Lingkungan dan Skenario Penelitian

Penelitian dilakukan pada sistem operasi Microsoft Windows yang digunakan sebagai objek uji. Lingkungan pengujian dirancang sedemikian rupa agar menyerupai kondisi sistem nyata yang umum digunakan oleh pengguna. Sistem Windows yang digunakan dikonfigurasikan dengan aplikasi standar dan layanan sistem aktif, sehingga memungkinkan malware beroperasi secara normal seperti pada lingkungan produksi.

Skenario penelitian dimulai dengan kondisi sistem Windows yang bersih, kemudian dilakukan simulasi infeksi malware. Setelah malware berhasil dieksekusi, sistem dibiarkan berjalan dalam periode tertentu untuk memungkinkan malware melakukan aktivitasnya, seperti modifikasi sistem, eksekusi proses, dan komunikasi internal. Selama periode tersebut, sistem akan menghasilkan berbagai artefak digital yang kemudian dianalisis menggunakan pendekatan digital forensik.

b. Tahapan Proses Digital Forensik

Tahapan proses digital forensik dalam penelitian ini terdiri dari empat tahap utama, yaitu identifikasi, akuisisi, analisis, dan pelaporan. Alur proses ini dirancang untuk **memastikan investigasi dilakukan secara sistematis dan terstruktur.**



Gambar 1. Diagram teknis proses digital forensik pada sistem operasi Windows

1. Tahap Identifikasi

Tahap identifikasi merupakan tahap awal dalam proses investigasi forensik. Pada tahap ini, dilakukan penentuan sistem yang terindikasi terinfeksi malware serta ruang lingkup investigasi. Identifikasi mencakup penentuan komponen sistem yang akan dianalisis, seperti Windows Registry, Windows Event Log, sistem file NTFS, dan memory (RAM).

Tujuan utama tahap identifikasi adalah untuk memastikan bahwa proses investigasi difokuskan pada sumber data yang relevan dan berpotensi mengandung bukti digital terkait aktivitas malware. Tahap ini juga mencakup pencatatan kondisi awal sistem sebagai referensi sebelum dilakukan proses akuisisi data.

2. Tahap Akuisisi

Tahap akuisisi bertujuan untuk mengambil data dari sistem target secara forensik tanpa mengubah kondisi asli data. Pada penelitian ini, akuisisi dilakukan terhadap media penyimpanan dan memory sistem Windows. Akuisisi disk dilakukan untuk memperoleh salinan data sistem file, registry, dan event log, sedangkan akuisisi memory dilakukan untuk menangkap data volatile yang tersimpan di dalam RAM.

Proses akuisisi dilakukan dengan prinsip forensic soundness, yaitu memastikan bahwa data yang diambil tetap utuh dan tidak mengalami perubahan. Seluruh proses akuisisi dicatat secara rinci untuk menjaga integritas bukti digital dan mendukung proses analisis selanjutnya.

3. Tahap Analisis

Tahap analisis merupakan tahap inti dalam penelitian ini karena pada tahap inilah seluruh data hasil akuisisi forensik diperiksa dan diinterpretasikan untuk mengidentifikasi aktivitas malware serta dampaknya terhadap sistem operasi Windows. Analisis dilakukan secara sistematis dengan memeriksa berbagai artefak digital utama yang dihasilkan selama sistem beroperasi dalam kondisi terinfeksi malware.

Analisis Windows Registry dilakukan untuk mengidentifikasi perubahan konfigurasi sistem yang mencurigakan akibat aktivitas malware. Pemeriksaan registry difokuskan pada lokasi-lokasi yang umum dimanfaatkan malware untuk mempertahankan persistensi, seperti entri autorun, layanan sistem, dan konfigurasi aplikasi. Melalui analisis ini, investigator dapat mengidentifikasi adanya penambahan atau modifikasi entri registry yang tidak sesuai dengan konfigurasi sistem normal.

Selanjutnya, analisis Windows Event Log dilakukan untuk mengidentifikasi aktivitas sistem dan keamanan yang tidak normal. Event log menyediakan informasi penting terkait waktu kejadian, jenis aktivitas, serta sumber kejadian yang terjadi pada sistem. Dengan menganalisis event log, investigator dapat mengidentifikasi indikasi eksekusi program mencurigakan, perubahan kebijakan sistem, maupun aktivitas lain yang berkaitan dengan serangan malware. Informasi waktu pada event log juga digunakan untuk membantu merekonstruksi kronologi kejadian secara lebih akurat.

Analisis sistem file NTFS dilakukan untuk memeriksa perubahan file dan metadata yang dihasilkan oleh aktivitas malware. Pemeriksaan difokuskan pada keberadaan file mencurigakan, perubahan timestamp, serta struktur direktori yang tidak wajar. Metadata file pada sistem file NTFS memberikan informasi penting mengenai waktu pembuatan, modifikasi, dan akses file, yang dapat digunakan untuk mengidentifikasi periode aktivitas malware pada sistem.Selain analisis artefak statis, dilakukan pula analisis memory forensik untuk mengidentifikasi proses malware yang berjalan secara tersembunyi di dalam RAM.

Analisis memory memungkinkan investigator untuk mendeteksi malware yang menggunakan teknik stealth, seperti injeksi proses atau eksekusi fileless, yang tidak selalu meninggalkan jejak yang jelas pada sistem file. Melalui pemeriksaan memory, proses mencurigakan, modul yang dimuat, serta aktivitas internal sistem dapat diidentifikasi secara lebih mendalam.

Seluruh hasil analisis artefak digital tersebut kemudian dikorelasikan untuk memperoleh gambaran menyeluruh mengenai aktivitas malware. Pendekatan korelasi ini memungkinkan investigator untuk merekonstruksi alur serangan malware, mulai dari proses infeksi awal, mekanisme persistensi, hingga dampak yang ditimbulkan terhadap sistem operasi Windows.

4. Tahap Pelaporan

Tahap pelaporan merupakan tahap akhir dalam proses digital forensik. Pada tahap ini, seluruh hasil analisis disusun dalam bentuk laporan yang sistematis dan terstruktur. Laporan mencakup deskripsi temuan forensik, interpretasi hasil analisis, serta rekonstruksi kronologi serangan malware.

Pelaporan dilakukan dengan bahasa yang jelas dan objektif agar hasil investigasi dapat dipahami oleh pihak teknis maupun non-teknis. Tahap ini sangat penting karena laporan forensik dapat digunakan sebagai bahan evaluasi keamanan sistem maupun sebagai dokumentasi pendukung dalam penanganan insiden keamanan siber.

5. Teknik Analisis Data

Teknik analisis data dalam penelitian ini dilakukan secara kualitatif dengan pendekatan teknis. Data yang diperoleh dari hasil akuisisi dianalisis untuk mengidentifikasi pola aktivitas malware dan hubungan antar artefak digital. Analisis dilakukan dengan mengkorelasikan temuan dari registry, event log, sistem file, dan memory untuk merekonstruksi kronologi serangan malware secara menyeluruh.

Pendekatan korelasi artefak digital ini memungkinkan investigator untuk memperoleh gambaran yang lebih komprehensif mengenai aktivitas malware, mulai dari proses infeksi awal, mekanisme persistensi, hingga dampak yang ditimbulkan terhadap sistem operasi Windows.

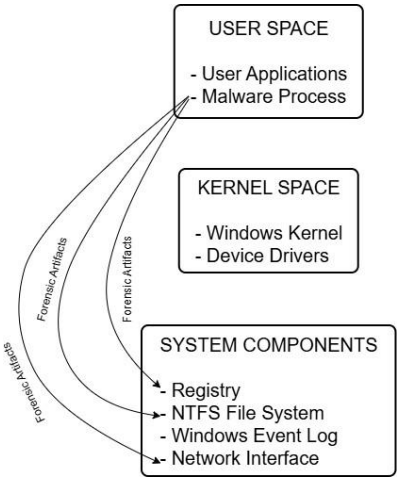
HASIL DAN PEMBAHASAN

Bab ini membahas hasil penelitian yang diperoleh dari penerapan digital forensik pada insiden serangan malware di sistem operasi Windows. Hasil analisis diperoleh melalui pemeriksaan artefak digital utama, yaitu arsitektur sistem Windows, Windows Event Log, dan memory (RAM). Pembahasan difokuskan pada pengungkapan aktivitas malware, mekanisme operasionalnya, serta dampak yang ditimbulkan terhadap sistem.

a. Analisis Arsitektur Sistem Windows Terinfeksi Malware

Analisis arsitektur sistem operasi Windows dilakukan untuk memahami bagaimana malware berinteraksi dengan komponen sistem. Hasil pengamatan menunjukkan bahwa malware beroperasi pada lapisan user space dan memanfaatkan layanan sistem untuk menjalankan proses berbahaya secara tersembunyi. Malware tidak hanya mengeksekusi file berbahaya, tetapi juga memanfaatkan mekanisme sistem yang sah untuk menghindari deteksi oleh pengguna.

Malware teridentifikasi menggunakan proses sistem sebagai media untuk menyamarkan aktivitasnya. Dengan cara ini, aktivitas malware sulit dibedakan dari proses normal sistem operasi. Interaksi malware dengan komponen sistem, seperti registry dan layanan sistem, menghasilkan artefak digital yang dapat dianalisis untuk mengungkap keberadaannya.



Gambar 2. Arsitektur teknis sistem operasi Windows yang terinfeksi malware

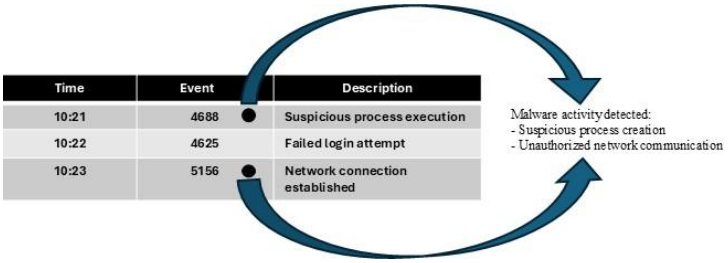
Gambar tersebut menggambarkan hubungan antara malware dengan komponen utama sistem operasi Windows, termasuk interaksi dengan user space, layanan sistem, dan artefak digital yang dihasilkan. Dari analisis ini, dapat disimpulkan bahwa pemahaman terhadap arsitektur sistem Windows sangat penting dalam investigasi forensik malware karena membantu investigator menentukan lokasi artefak digital yang relevan.

b. Analisis Windows Event Log pada Aktivitas Malware

Windows Event Log merupakan salah satu sumber artefak digital yang sangat penting dalam investigasi forensik. Event log mencatat berbagai aktivitas sistem, aplikasi, dan keamanan yang terjadi pada sistem operasi Windows. Dalam penelitian ini, analisis event log dilakukan untuk mengidentifikasi aktivitas abnormal yang berkaitan dengan eksekusi malware.

Hasil analisis menunjukkan adanya beberapa event yang mengindikasikan aktivitas

mencurigakan, seperti eksekusi program yang tidak dikenal dan perubahan status layanan sistem. Event tersebut tercatat dengan informasi waktu kejadian, sumber event, dan jenis aktivitas yang dilakukan. Dengan menganalisis informasi tersebut, investigator dapat mengidentifikasi waktu awal terjadinya infeksi malware serta aktivitas lanjutan yang dilakukan oleh malware.



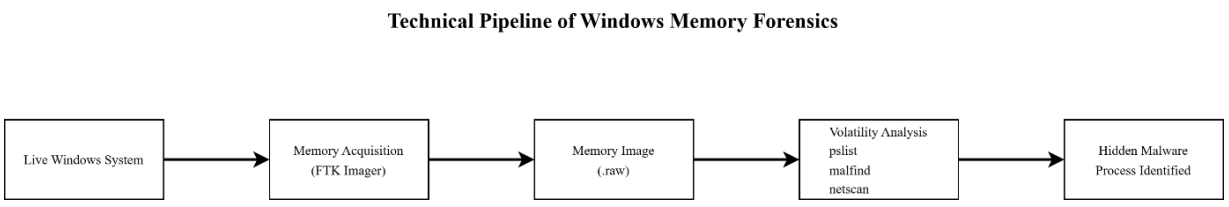
Gambar 3. Analisis Windows Event Log pada aktivitas malware

Gambar ini menunjukkan contoh log kejadian yang mencerminkan aktivitas malware pada sistem operasi Windows. Melalui korelasi antara event log dan artefak digital lainnya, investigator dapat merekonstruksi kronologi serangan malware secara lebih akurat. Hasil ini menegaskan bahwa Windows Event Log memiliki peran penting dalam mengungkap aktivitas malware yang tidak terlihat secara langsung oleh pengguna.

c. Analisis Memory Forensik Windows

Analisis memory forensik dilakukan untuk mengidentifikasi aktivitas malware yang berjalan secara tersembunyi di dalam memory (RAM). Hasil analisis menunjukkan bahwa beberapa proses malware tidak meninggalkan jejak yang jelas pada sistem file, tetapi dapat diidentifikasi melalui pemeriksaan data memory. Malware terdeteksi menggunakan teknik penyamaran proses untuk beroperasi di dalam sistem tanpa terdeteksi oleh mekanisme keamanan konvensional.

Data memory yang dianalisis menunjukkan adanya proses yang tidak terdaftar secara normal dalam sistem, serta aktivitas koneksi internal yang mencurigakan. Informasi ini sangat penting karena memberikan bukti keberadaan malware yang tidak dapat diidentifikasi melalui analisis statis pada disk. Dengan demikian, analisis memory forensik menjadi tahap yang krusial dalam investigasi insiden malware.



Gambar 4. Diagram teknis analisis memory forensik pada sistem operasi Windows

Gambar ini menggambarkan hasil analisis memory yang menunjukkan keberadaan proses malware di dalam RAM. Hasil ini menegaskan bahwa pendekatan digital forensik

yang mencakup analisis artefak volatile sangat diperlukan untuk mengungkap malware modern yang menggunakan teknik stealth.

d. Pembahasan Hasil Penelitian

Berdasarkan hasil analisis yang telah dilakukan, dapat disimpulkan bahwa pendekatan digital forensik mampu mengungkap aktivitas malware secara komprehensif pada sistem operasi Windows. Kombinasi analisis arsitektur sistem, Windows Event Log, dan memory forensik memberikan gambaran yang jelas mengenai cara kerja malware, mulai dari proses eksekusi awal hingga aktivitas tersembunyi di dalam sistem.

Hasil penelitian ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa analisis artefak digital Windows merupakan metode yang efektif dalam investigasi malware. Selain itu, penelitian ini menunjukkan bahwa analisis memory forensik memiliki peran yang sangat penting dalam mengungkap malware yang dirancang untuk menghindari deteksi berbasis disk. Pendekatan yang digunakan dalam penelitian ini juga menegaskan pentingnya korelasi antar artefak digital dalam merekonstruksi kronologi serangan malware. Dengan menggabungkan hasil analisis dari berbagai sumber artefak, investigator dapat memperoleh pemahaman yang lebih menyeluruh mengenai insiden yang terjadi dan dampaknya terhadap sistem operasi Windows.

e. Implikasi Keamanan Sistem Operasi Windows

Hasil penelitian ini menunjukkan bahwa serangan malware pada sistem operasi Windows memiliki implikasi yang signifikan terhadap aspek keamanan sistem secara menyeluruh. Temuan forensik yang diperoleh dari analisis arsitektur sistem, Windows Event Log, dan memory forensik mengindikasikan bahwa malware mampu memanfaatkan mekanisme internal sistem untuk menjalankan aktivitas berbahaya secara tersembunyi dan sulit terdeteksi oleh pengguna.

Salah satu implikasi utama yang dapat diidentifikasi adalah meningkatnya risiko kompromi sistem akibat keterlambatan deteksi serangan malware. Malware yang beroperasi secara stealth, khususnya yang berjalan di dalam memory, menunjukkan bahwa mekanisme keamanan berbasis deteksi file belum sepenuhnya efektif dalam menghadapi ancaman malware modern. Oleh karena itu, diperlukan pendekatan keamanan yang lebih komprehensif dengan mengintegrasikan analisis artefak volatile ke dalam proses deteksi dan respons insiden.

Implikasi lainnya berkaitan dengan pentingnya penerapan pemantauan sistem secara berkelanjutan. Hasil analisis Windows Event Log dalam penelitian ini membuktikan bahwa log aktivitas sistem dan keamanan dapat menjadi sumber informasi yang sangat penting dalam mengidentifikasi indikasi awal serangan malware. Dengan pemantauan log yang konsisten, potensi serangan dapat dideteksi lebih dini sebelum menimbulkan dampak yang lebih besar terhadap sistem.

Selain itu, hasil penelitian ini juga menegaskan pentingnya kesiapan respons insiden dalam lingkungan sistem operasi Windows. Pemahaman terhadap artefak digital yang dihasilkan oleh malware dapat membantu organisasi dalam menyusun prosedur respons insiden yang lebih efektif dan terstruktur. Digital forensik tidak hanya berperan dalam investigasi pasca-insiden, tetapi juga menjadi bagian penting dalam strategi peningkatan

keamanan sistem.

Secara keseluruhan, implikasi keamanan yang diidentifikasi dalam penelitian ini menunjukkan bahwa penerapan digital forensik memiliki peran strategis dalam mendukung keamanan sistem operasi Windows. Integrasi antara pendekatan forensik dan mekanisme keamanan preventif diharapkan dapat meningkatkan kemampuan sistem dalam mendeteksi, menganalisis, dan merespons serangan malware secara lebih efektif.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa pendekatan digital forensik merupakan metode yang efektif dalam menangani dan menganalisis insiden serangan malware pada sistem operasi Windows. Melalui penerapan tahapan digital forensik yang sistematis, yaitu identifikasi, akuisisi, analisis, dan pelaporan, aktivitas malware dapat diungkap secara terstruktur dan komprehensif. Pendekatan ini memungkinkan investigator untuk memperoleh gambaran teknis mengenai perilaku malware serta dampak yang ditimbulkannya terhadap sistem operasi.

Hasil analisis menunjukkan bahwa malware pada sistem operasi Windows memanfaatkan mekanisme internal sistem untuk menjalankan aktivitas berbahaya dan mempertahankan persistensinya. Analisis terhadap arsitektur sistem Windows memberikan pemahaman awal mengenai bagaimana malware berinteraksi dengan komponen sistem. Pemeriksaan Windows Event Log mampu mengungkap aktivitas abnormal yang berkaitan dengan eksekusi malware dan perubahan sistem, sedangkan analisis memory forensik terbukti sangat penting dalam mengidentifikasi proses malware yang berjalan secara tersembunyi di dalam RAM dan tidak meninggalkan jejak yang jelas pada sistem file.

Penelitian ini juga menunjukkan bahwa analisis artefak digital secara terpisah tidak cukup untuk mengungkap insiden malware secara menyeluruh. Diperlukan korelasi antara berbagai artefak digital, seperti registry, event log, sistem file NTFS, dan memory, untuk merekonstruksi kronologi serangan malware secara akurat. Dengan melakukan korelasi tersebut, investigator dapat mengidentifikasi tahapan infeksi, aktivitas malware selama berada di dalam sistem, serta dampak yang ditimbulkan terhadap sistem operasi Windows.

Dengan demikian, dapat disimpulkan bahwa digital forensik memiliki peran yang sangat penting dalam penanganan insiden keamanan siber, khususnya serangan malware pada sistem operasi Windows. Pendekatan yang digunakan dalam penelitian ini diharapkan dapat menjadi referensi teknis bagi praktisi keamanan siber, akademisi, dan peneliti dalam melakukan investigasi forensik malware secara lebih efektif. Selain itu, hasil penelitian ini juga diharapkan dapat berkontribusi dalam meningkatkan kesiapan dan kesadaran terhadap pentingnya penerapan digital forensik dalam menjaga keamanan sistem operasi Windows.

DAFTAR PUSTAKA

Dolan-Gavitt, B., "Analisis forensik registri Windows dalam memori", Investigasi Digital, vol. 5, no. 3, hlm. S26-S32, 2008.

Ali, M., Shiaeles, S., Clarke, N., & Kontogeorgis, D., "Pendekatan identifikasi perangkat lunak berbahaya proaktif untuk pemeriksa forensik digital", arXiv:2109.09567, 2021.

D4I – Kerangka Kerja Forensik Digital untuk Meninjau dan Menyelidiki Serangan Siber, Athanasios Dimitriadis, Pusat Informasi Bioteknologi Nasional, 2022.

Forensik memori Windows: Identifikasi modifikasi (berbahaya) dalam file gambar yang dipetakan memori, Forensic Science International: Digital Investigation, 2023.

Patil, D., & Prabhu, A., *Deteksi Malware Melalui Forensik Memori dan Analisis Log Peristiwa Windows*, *Jurnal Teknologi Informasi Arab Internasional*, 2025.

Analisis Forensik Langsung Kejahatan Email yang Diidentifikasi Malware, *Zona Digital: Jurnal Teknologi Informasi dan Komunikasi*, 2022.

"Analisis Malware dengan metode Surface dan Runtime Analysis", *Jurnal Ilmiah Matrik*, 2021.

"Analisis Perilaku Malware Menggunakan Pendekatan Statis dan Dinamis", *Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi*, 2025.

Forensik Volatile Memori untuk Deteksi Malware menggunakan ML, Jurnal Teknik Informatika dan Sistem Informasi, (Tasikmalaya), 2018.