Forensik Digital Artefak *Malware Persistent Glitch* pada Windows Berbasis ISO/IEC 27037 dan ISO/IEC 27042

Aurelia Sandra Darmawan[1)], Geowaldi Nainggolan[2)], Hanif Nur Hidayat[3)], Jeckson Sidabutar[4)], Mahardika Hakim Permana Saputri[5)]

1) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, aurelia.sandra@student.poltekssn.ac.id
2) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, geowaldi.nainggolan@student.poltekssn.ac.id
3) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, hanif.nur@student.poltekssn.ac.id
4) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, jeckson.sidabutar@poltekssn.ac.id
5) Otoritas Bandara Udara Pangsuma, dkmhrr@gmail.com

Riwayat Artikel

Dikirim 24 Apr 2026
Diterima 16 Jul 2026
Diterbitkan 26 Agu 2026

Kata kunci:

Forensik Digital
ISO/IEC 27037
ISO/IEC 27042
Malware
Windows

Abstrak

Penelitian menyajikan hasil investigasi forensik digital terhadap indikasi kompromi keamanan pada infrastruktur Windows Server 2025. Insiden melibatkan *Persistent Windows Server Glitch Malware* yang menyebabkan gangguan visual dan operasional server. Penelitian ini menerapkan pendekatan *Live Forensics* untuk mengamankan data volatil pada memori (RAM) serta analisis *Dead Forensics* pada *disk* penyimpanan. Seluruh proses akuisisi bukti digital dan analisis interpretatif dilaksanakan dengan mematuhi standar ISO/IEC 27037 untuk penanganan bukti dan ISO/IEC 27042 untuk analisis guna menjamin integritas temuan. Hasil analisis menemukan artefak kunci berupa file eksekusi berbahaya *setup.exe* serta jejak eksekusi skrip PowerShell di memori yang menyebabkan anomali visual persisten. Investigasi membuktikan bahwa sistem terkompromi melalui metode *social engineering* (*phishing*) yang menyamar sebagai pembaruan Windows.

Keyword:

Digital Forensics
ISO/IEC 27037
ISO/IEC 27042
Malware
Windows

Abstract

The study presents the results of a digital forensics investigation into indications of security compromise on a Windows Server 2025 infrastructure. The incident involved a Persistent Windows Server Glitch Malware that caused visual and operational server disruptions. The study applied a Live Forensics approach to secure volatile data in memory (RAM) and Dead Forensics analysis on disk storage. The entire digital evidence acquisition and interpretive analysis process was carried out in compliance with ISO/IEC 27037 standards for evidence handling and ISO/IEC 27042 for analysis to ensure the integrity of the findings. The analysis found key artifacts in the form of a malicious executable file setup.exe and traces of PowerShell script execution in memory that caused persistent visual anomalies. The investigation proved that the system was compromised through social engineering (phishing) methods disguised as Windows updates.

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah meningkatkan kompleksitas ancaman siber, khususnya pada sistem operasi server modern seperti Windows Server 2025. Serangan berbasis *social engineering* melalui email menjadi salah satu vektor utama penyebaran *malware*, di mana pengguna sering kali menjadi target manipulasi untuk mengunduh dan mengeksekusi aplikasi berbahaya [1]. Studi terdahulu menunjukkan bahwa *malware* dengan mekanisme persisten mampu bertahan dalam sistem dan menimbulkan gangguan operasional yang signifikan [2]. Dalam konteks forensik digital, standar internasional ISO/IEC 27037 memberikan pedoman terkait akuisisi bukti digital, sedangkan ISO/IEC 27042 mengatur metodologi analisis yang terstruktur. Penerapan kedua standar ini penting untuk memastikan integritas dan validitas bukti yang diperoleh, sehingga hasil investigasi dapat dipertanggungjawabkan secara hukum maupun akademik.

Penelitian ini dilakukan untuk menganalisis artefak *malware* yang menyerang Windows Server 2025 melalui skenario email *phishing*, dengan fokus pada proses akuisisi bukti digital baik secara *live acquisition* maupun *dead acquisition*. Tujuan penelitian adalah mengidentifikasi jejak eksekusi malware, memahami pola persisten, serta mengevaluasi efektivitas penerapan ISO/IEC 27037 dan 27042 dalam investigasi forensik digital. Luaran penelitian berupa dokumentasi artefak digital dari memori dan *disk* yang dianalisis menggunakan DumpIt.exe, Volatility, serta FTK Imager. Manfaat penelitian ini adalah memberikan kontribusi terhadap pengembangan praktik forensik sesuai standar internasional, meningkatkan kesadaran akan ancaman *phishing*, serta memperkuat strategi keamanan sistem informasi di lingkungan organisasi.

2. TINJAUAN PUSTAKA

2.1. Forensik Digital

Forensik digital adalah cabang ilmu yang berfokus pada proses identifikasi, akuisisi, analisis, dan pelaporan bukti elektronik untuk tujuan investigasi [3]. Prinsip utama dalam forensik digital adalah menjaga integritas bukti agar dapat diterima dalam proses hukum maupun penelitian akademik. Dengan meningkatnya ancaman siber, forensik digital menjadi instrumen penting dalam mengungkap serangan *malware*, aktivitas ilegal, serta insiden keamanan informasi.

2.2. ISO/IEC 27037

ISO/IEC 27037 merupakan standar internasional yang memberikan pedoman mengenai proses identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital [4]. Standar ini menekankan pentingnya menjaga integritas bukti agar dapat diterima dalam proses hukum maupun penelitian akademik. Dalam konteks forensik *malware*, ISO/IEC 27037 memastikan bahwa proses akuisisi dilakukan secara sah dan terverifikasi.

2.3. ISO/IEC 27042

ISO/IEC 27042 melengkapi ISO/IEC 27037 dengan menyediakan kerangka metodologi analisis bukti digital [5]. Standar ini mengatur bagaimana bukti yang telah diperoleh dianalisis secara sistematis, termasuk interpretasi artefak, korelasi data, dan pelaporan hasil investigasi. Penerapan ISO/IEC 27042 untuk menjamin bahwa kegiatan analisis dilakukan secara konsisten dan dapat dipertanggungjawabkan.

2.4. *Malware* Mekanisme Persisten

Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem komputer [6]. Salah satu teknik yang sering digunakan adalah persisten, yaitu kemampuan *malware* untuk tetap aktif meskipun sistem *restart*. Persisten biasanya dilakukan melalui modifikasi *registry*, layanan sistem, atau penambahan file eksekusi otomatis. Analisis terhadap mekanisme persisten menjadi krusial untuk memahami dampak dalam jangka panjang serangan.

2.5. FTK Imager

FTK Imager adalah perangkat lunak forensik yang digunakan untuk melakukan *dead acquisition* dengan cara membuat citra *disk* secara *bit-by-bit* [7]. Alat ini memungkinkan penyidik memperoleh salinan lengkap media penyimpanan tanpa mengubah data asli. FTK Imager juga mendukung verifikasi integritas melalui fungsi hash, sehingga hasil akuisisi dapat dipastikan keasliannya.

2.6. Volatility

Volatility merupakan kerangka kerja *open-source* untuk analisis memori (*memory forensics*) [8]. Dengan Volatility, artefak yang tersimpan dalam RAM seperti proses aktif, modul kernel, koneksi jaringan, dan *handles* sistem dapat diidentifikasi. Analisis ini penting dalam *live acquisition* karena *malware* sering kali hanya meninggalkan jejak sementara di memori.

2.7. DumpIt.exe

DumpIt.exe adalah utilitas ringan yang digunakan untuk melakukan akuisisi memori fisik pada sistem Windows. Sebagai perangkat akuisisi RAM terkemuka, yang mirip dengan FTK Imager dan Magnet RAM Capture, DumpIt.exe berperan krusial dalam forensik langsung, memungkinkan penyelidikan mendalam terhadap data volatil guna mengungkap jejak aktivitas berbahaya dan artefak kunci [9]. Alat ini menghasilkan file *dump* RAM yang kemudian dapat dianalisis menggunakan Volatility. DumpIt.exe sering dipilih karena kemudahan penggunaan dan kemampuannya menghasilkan citra memori yang lengkap, sehingga mendukung investigasi forensik terhadap *malware* yang aktif.

2.8. Windows Server 2025

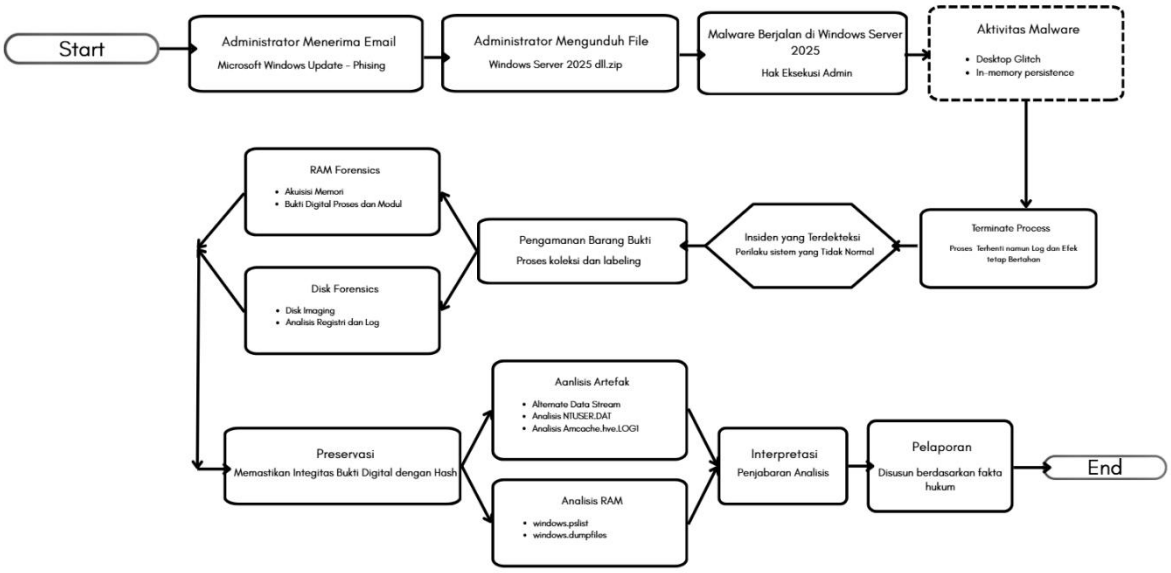
Windows Server 2025 merupakan iterasi terbaru dari sistem operasi server Microsoft yang dirancang khusus untuk mengoptimalkan performa infrastruktur *hybrid cloud* dan keamanan tingkat lanjut [10]. Fokus utama dari pengembangan versi ini adalah peningkatan pada sektor *Active Directory* (AD) dan protokol keamanan data melalui fitur SMB *over* QUIC guna memitigasi risiko akses jarak jauh yang tidak terotorisasi. Salah satu inovasi paling signifikan yang diperkenalkan adalah teknologi *Hotpatching*, yang memungkinkan penerapan pembaruan keamanan secara *real-time* tanpa memerlukan *reboot* sistem, sehingga menjamin ketersediaan layanan yang lebih tinggi. Selain itu, sistem operasi ini menghadirkan optimalisasi performa penyimpanan melalui dukungan NVMe yang lebih luas dan efisiensi *Resilient File System* (ReFS) dalam menangani beban kerja data berskala besar [11]. Dari sisi komputasi modern, Windows Server 2025 memberikan dukungan akselerasi GPU yang ditingkatkan untuk mengakomodasi kebutuhan *artificial intelligence* dan *machine learning* pada lingkungan *on-premises*. Dalam konteks investigasi digital, pembaruan mekanisme *logging* dan audit pada versi ini menjadi komponen krusial bagi tim forensik untuk mengidentifikasi jejak aktivitas *malware* dan persistensi sistem secara lebih akurat.

3. METODE PENELITIAN

Objek penelitian yang digunakan adalah sistem operasi Windows Server 2025 yang digunakan oleh seorang pengguna dan menjadi target serangan *malware* melalui skenario *email phishing*. Sistem ini dipilih karena merupakan platform server modern yang rentan terhadap serangan berbasis *social engineering* dan menjadi relevan untuk studi forensik digital. Jenis penelitian yang digunakan adalah kualitatif dengan pendekatan studi kasus. Penelitian ini berfokus pada analisis artefak digital yang dihasilkan dari serangan *malware*, bukan pada pengukuran kuantitatif. Pendekatan kualitatif dipilih untuk menggali secara mendalam jejak eksekusi *malware*, pola persisten, serta efektivitas penerapan standar ISO/IEC 27037 dan 27042.

3.1. Skenario Penelitian

Penelitian ini menggunakan skenario serangan *phishing* terhadap pengguna Windows Server 2025 dengan desain skenario penelitian yang disajikan pada Gambar 1. Korban menerima email melalui Microsoft Outlook dari akun palsu yang menyamar sebagai petugas resmi Microsoft. Email tersebut berisi tautan pembaruan sistem yang sebenarnya adalah file berbahaya bernama *setup.exe*. File tersebut diekstraksi dan file *setup.exe* dieksekusi pada 19 Januari 2026 pukul 20:33 WIB. Hal ini menyebabkan *Desktop Transparency Glitch* yang tidak hilang meskipun proses dimatikan. Setelah dijalankan, file tersebut menanamkan *malware* dengan mekanisme persisten yang menyebabkan sistem mengalami gangguan visual.



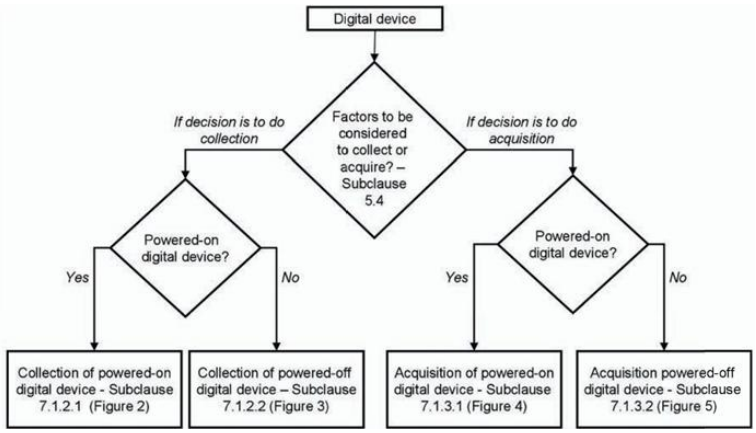
Gambar 1. Desain Skenario Penelitian

Tim forensik melakukan langkah-langkah pasca insiden dengan dua pendekatan:

- *Live acquisition* menggunakan *DumpIt.exe* untuk memperoleh citra RAM, yang kemudian dianalisis dengan *Volatility*.
- *Dead acquisition* menggunakan *FTK Imager* untuk membuat citra *disk* secara bit-by-bit, sehingga artefak *malware* dapat diidentifikasi tanpa mengubah data asli.

3.2. ISO/IEC 27037

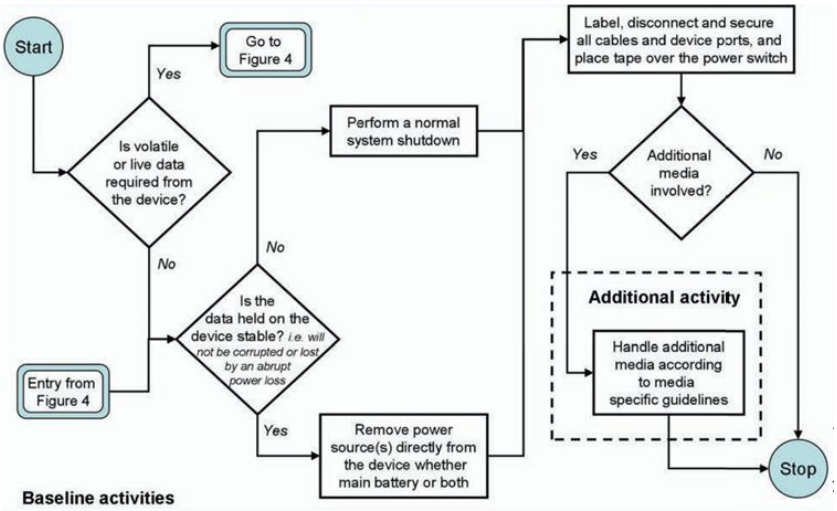
Secara keseluruhan, alur kerja investigasi forensik digital pada penelitian ini divisualisasikan dengan mengadaptasi kerangka kerja internasional ISO/IEC 27037 untuk fase penanganan awal bukti digital, yang kemudian disubstitusikan ke dalam kerangka ISO/IEC 27042 untuk fase analisis dan interpretasi. Langkah pertama yang dilakukan oleh investigator saat menghadapi insiden adalah menentukan strategi penanganan berdasarkan kondisi operasional perangkat target. Proses pengambilan keputusan merujuk pada standar ISO/IEC 27037 yang digambarkan pada Gambar 2.



Gambar 2. Diagram Pengambilan Keputusan Bukti Digital pada ISO/IEC 27037

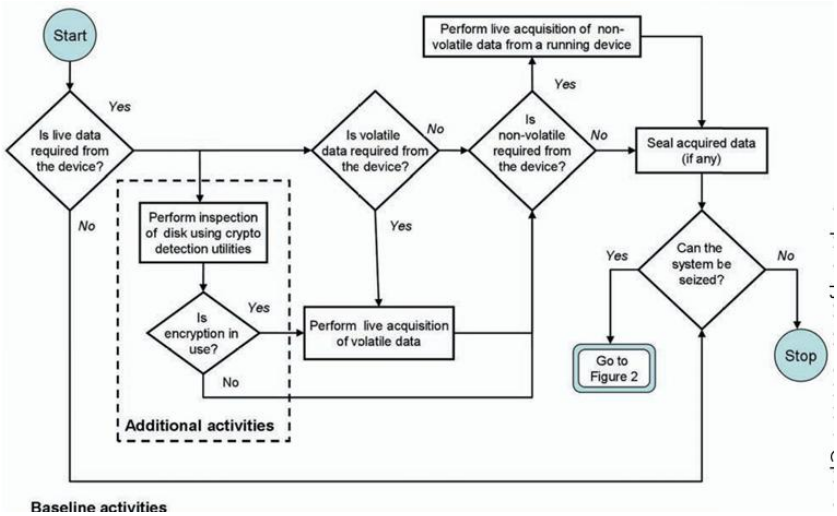
Tahap identifikasi merupakan langkah awal krusial di mana investigator melakukan pengenalan dan pencarian terhadap potensi bukti digital yang relevan dengan insiden keamanan pada sistem operasi Windows Server 2025. Karena sistem target berupa Windows Server 2025 ditemukan dalam keadaan menyala (*power on*) dan terdapat kebutuhan kritis untuk menyelamatkan data volatil yang rentan hilang, investigator memutuskan untuk melakukan penanganan langsung

(*live forensics*) melalui aktivitas koleksi dan akuisisi data volatil terlebih dahulu, sebelum beralih ke data non-volatil dengan proses yang disajikan pada Gambar 3. Proses identifikasi dimulai dengan memverifikasi laporan pengguna terkait adanya anomali sistem pasca-interaksi dengan email yang mengatasnamakan petugas Microsoft via Outlook. Investigator memprioritaskan identifikasi pada data volatil yang berada di *Random Access Memory* (RAM) karena adanya indikasi *malware* yang sedang berjalan (*running process*) serta data non-volatil pada penyimpanan sekunder (*hard disk*) untuk menelusuri jejak persistensi *file* berbahaya (*setup.exe*).



Gambar 3. Proses Koleksi ketika *Device* dalam Keadaan Menyala pada ISO/IEC 27037

Selanjutnya, proses koleksi dilakukan dengan strategi *order of volatility*, yaitu mengamankan data yang paling mudah berubah terlebih dahulu. Investigator mengumpulkan data volatil dari sistem yang masih menyala (*live system*) guna menghindari hilangnya informasi enkripsi atau koneksi jaringan yang aktif pada proses akuisisi yang disajikan pada Gambar 4. Setelah data volatil diamankan, sistem dimatikan melalui prosedur *normal shutdown* atau pencabutan daya (sesuai kondisi) untuk melanjutkan koleksi data non-volatil dari *hard disk*, memastikan seluruh artefak digital pada perangkat korban berada dalam penguasaan investigator.



Gambar 4. Proses Akuisisi ketika *Device* dalam Keadaan Menyala pada ISO/IEC 27037

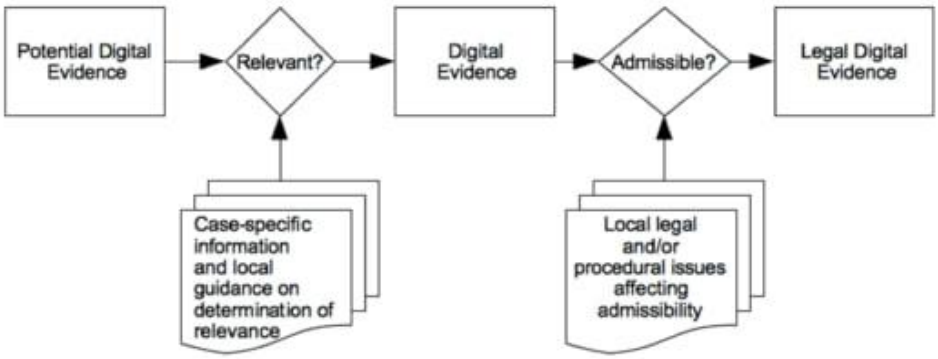
Akuisisi bukti digital dilaksanakan dalam dua tahap utama. Pertama, *live acquisition* menggunakan DumpIt.exe untuk menyalin isi RAM ke format .dmp. Kedua, *dead acquisition* dilakukan pada *hard disk* menggunakan perangkat lunak FTK Imager (versi 4.7.1.2). Metode yang

digunakan adalah pencitraan fisik (*physical imaging*) untuk membuat salinan *bit-by-bit* yang presisi dari seluruh partisi *disk*. Hasil akuisisi *disk* disimpan dalam format E01 (*EnCase Image File*) yang terpecah menjadi beberapa segmen (misalnya E01-Clone001_001.E01 hingga .E10) untuk memudahkan manajemen penyimpanan dan integritas data.

Selanjutnya yakni tahap preservasi. Preservasi bertujuan menjamin keaslian dan integritas bukti digital agar dapat dipertanggungjawabkan secara hukum (*admissible*). Seluruh hasil akuisisi, baik *memory dump* maupun *disk image* E01, diverifikasi integritasnya menggunakan algoritma *hashing* (MD5 dan SHA-1) yang dihasilkan secara otomatis oleh FTK Imager dan DumpIt.exe. Bukti asli disimpan dalam media penyimpanan yang aman, sementara analisis dilakukan hanya pada salinan (*clone*) bukti tersebut untuk mencegah kontaminasi atau perubahan data yang tidak disengaja selama proses investigasi berlangsung.

3.3. ISO/IEC 27042

Fase analisis dan interpretasi dalam penelitian ini berpedoman pada kerangka kerja standar ISO/IEC 27042. Implementasi standarisasi ini bertujuan untuk memastikan proses penanganan bukti digital berjalan secara valid, terukur, dan objektif. Alur transformasi komponen bukti dari data mentah yang masih diindikasi sebagai potensi hingga menjadi data bukti digital yang sah ditunjukkan pada Gambar 5.



Gambar 5. Alur Status Bukti Digital

Tahap analisis dilakukan secara komprehensif terhadap dua sumber data. Analisis memori menggunakan Volatility 3 pada Kali Linux untuk mengidentifikasi proses *setup.exe* yang berjalan. Secara paralel, analisis *disk image* dilakukan menggunakan FTK Imager untuk memeriksa struktur sistem berkas NTFS. Investigator menelusuri artefak *registry NTUSER.DAT* dan *Amcache.hve* untuk membuktikan eksekusi program, serta memeriksa *Alternate Data Stream* (ADS) *Zone.Identifier* pada file *setup.exe* yang mengungkap URL sumber unduhan (ReferrerUrl) dari file ZIP berbahaya.

Interpretasi bertujuan menghubungkan temuan-temuan terfragmentasi menjadi narasi kronologis yang utuh. Investigator mengkorelasikan temuan *Zone.Identifier* yang menunjukkan asal file dari internet, log *Amcache.hve* yang mencatat waktu eksekusi pertama kali, dan daftar proses di RAM yang menunjukkan *malware* masih aktif. Fakta-fakta ini diinterpretasikan sebagai serangan *phishing* yang sukses, di mana pengguna dijebak untuk mengunduh dan menjalankan *malware*, yang kemudian menetap di sistem dan menyebabkan gangguan operasional pada Windows Server 2025.

Tahap akhir adalah penyusunan laporan forensik yang mendokumentasikan seluruh temuan teknis dan metodologi yang digunakan. Laporan ini menyajikan bukti visual berupa struktur direktori E01, nilai *hash* verifikasi, serta lokasi spesifik artefak *malware* dalam sistem direktori (\Users\Administrator\Downloads\Temp). Laporan disusun dengan bahasa yang jelas untuk menjelaskan kausalitas antara tindakan pengguna (mengunduh lampiran email) dan dampak sistem, serta menyertakan rekomendasi remediasi untuk membersihkan infeksi dan mencegah insiden serupa.

4. HASIL

4.1. Artefak Forensik Hasil Analisis *Disk*

Artefak	Lokasi/Detail	Temuan
setup.exe	Users\Administrat or\Downloads\Temp	File *malware* tersembunyi dalam ADS, tidak terlihat melalui *file explorer* standar
Zone.Identifier (ZoneId=3)	ADS metadata	Mengindikasikan file diunduh dari internet (zona internet)
NTUSER.DAT	Registry hive pengguna	Merekam aktivitas eksekusi program dan perubahan konfigurasi pengguna
Amcache.hve	C:\Windows\AppCompat\Programs\	Mencatat riwayat eksekusi aplikasi, termasuk *first execution timestamp* dari setup.exe

4.2. Artefak Forensik Hasil Analisis Memori

Artefak	Detail	Signifikansi
setup.exe	PID 1140	Proses dengan *parent process* tidak lazim, terindikasi sebagai *malware payload*. Ditemukan pada PPID: 3672 (Explorer); DLL: user32.dll, ws2_32.dll, kernel32.dll
user32.dll	Loaded by PID 1140	DLL untuk manipulasi antarmuka grafis berkorelasi dengan gejala *glitch* pada layar
ws2_32.dll	Loaded by PID 1140	DLL *Windows Sockets* yang mengindikasikan kapabilitas komunikasi jaringan (*C2 callback*)

4.3. Timeline Serangan

Waktu	Kejadian
19 Januari 2026, 20:16 WIB	Setup.exe pertama kali dieksekusi (Amcache.hve)
19 Januari 2026, 20:33 WIB	File setup.exe diekstraksi dan dijalankan ulang (skenario)
20 Januari 2026, 13:00 WIB	Preservasi Chain of Custody oleh Geowaldi Nainggolan

5. PEMBAHASAN

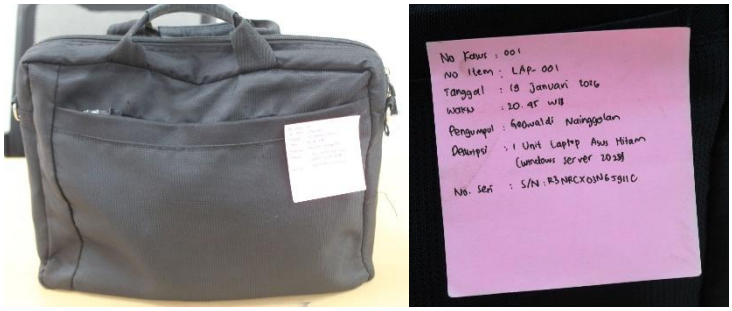
4.1. Identifikasi

Tahap identifikasi melibatkan pengenalan dan dokumentasi artefak digital potensial. Tim investigator menemukan perangkat server dalam kondisi menyala *(ON)* dengan layar menunjukkan anomali gangguan visual. Identifikasi dilakukan terhadap ciri fisik seperti stiker komunitas "DevFest" dan logo instansi sebagai tanda unik *(Unique Markings)* untuk memastikan rantai bukti. Laptop ditemukan di meja kerja dalam ruangan kantor dalam keadaan menyala dan dengan gangguan tampilan layar antara tampilan desktop dan google chrome seperti pada Gambar 6.

Gambar 6. Laptop yang Terinfeksi Malware

4.2. Koleksi

Proses koleksi dilakukan di tempat kejadian (TKP). Karena risiko hilangnya data volatil pada RAM akibat aktivitas *malware*, tim melakukan *live forensics* sebelum mematikan sistem. Setelah akuisisi memori selesai, perangkat dimatikan secara aman dan dimasukkan ke dalam *Faraday Bag* (tas pelindung sinyal) untuk mencegah akses kendali jarak jauh.



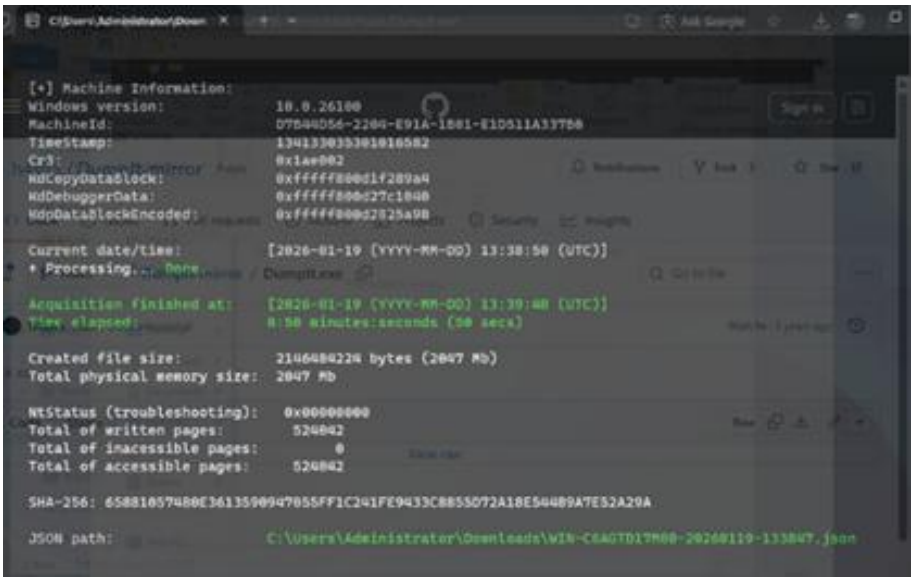
Gambar 7. Faraday Bag dengan Label

Proses pengamanan akhir barang bukti fisik. Setelah sistem dimatikan, perangkat dimasukkan ke dalam *Faraday Bag* untuk mencegah adanya akses kendali jarak jauh atau interferensi sinyal elektromagnetik dari luar yang dapat mengubah data di dalam server. Di bagian luar tas, ditempelkan Label Barang Bukti (LAP-001) yang berisi informasi nomor kasus, waktu koleksi, dan tanda tangan investigator sebagai bagian dari prosedur *Chain of Custody*.

4.3. Akuisisi

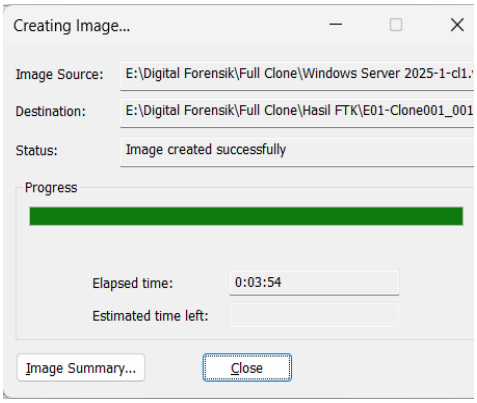
Tahapan akuisisi bertujuan membuat salinan forensik dari bukti digital. Adapun akuisisi yang dijalankan adalah sebagai berikut:

1. Akuisisi RAM menggunakan alat *DumpIt.exe* saat sistem masih menyala. Proses ini menghasilkan file WIN-C6AGTD17M08...dmp berukuran 2,09 GB. Akuisisi selesai dalam waktu 50 detik. Proses akuisisi memori (*Memory Dump*) dilakukan menggunakan teknik *Live Forensics* pada saat sistem Windows Server 2025 masih dalam kondisi operasional. Hal ini bertujuan untuk mengambil data yang bersifat *volatile* (mudah hilang), seperti proses *malware* yang sedang berjalan, koneksi jaringan, dan skrip PowerShell di dalam RAM. DumpIt.exe adalah perangkat lunak khusus utilitas forensik *portable* yang meminimalisir jejak (*footprint*) pada sistem target agar tidak merusak integritas bukti asli. Verifikasi Integritas Data Segera setelah proses akuisisi selesai, sistem secara otomatis menghasilkan nilai *fingerprint* digital untuk menjamin bahwa data tidak berubah selama proses pemindahan. Berdasarkan hasil rekaman pada yang disajikan pada Gambar 8, nilai integritas bukti RAM adalah SHA-256:
   65881057480E3613590947055FF1C241FE9433C8855D72A18E54489A7E52A29A



Gambar 8. Akuisisi RAM Menggunakan DumpIt.exe

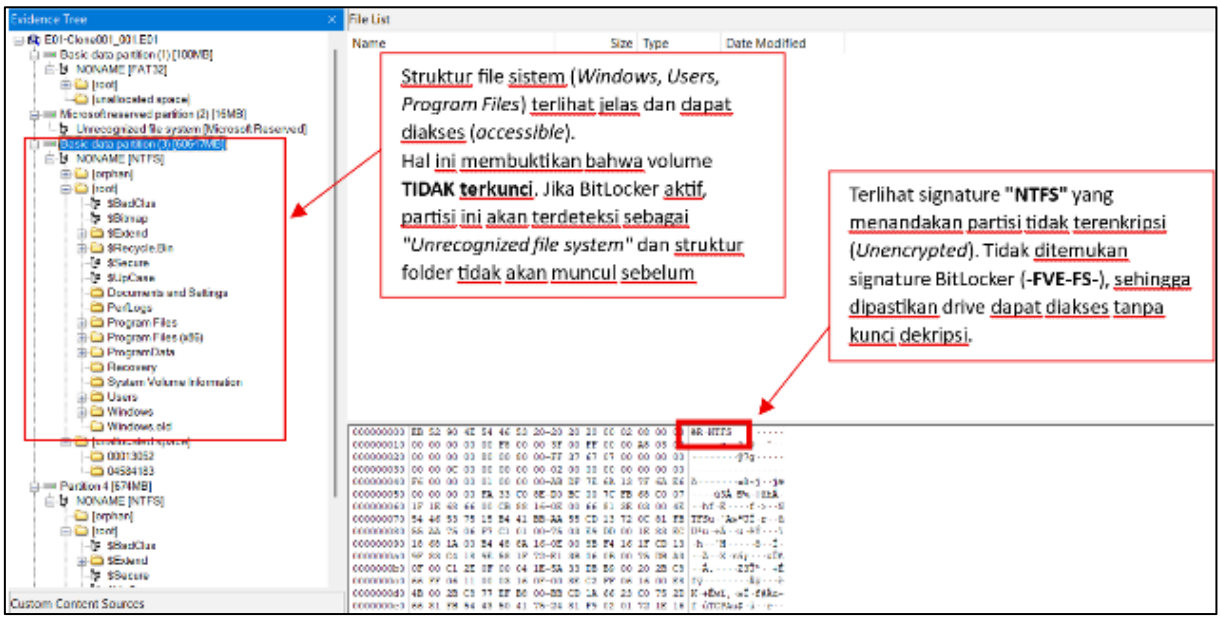
2. Akuisisi Disk menggunakan *FTK Imager* untuk membuat *Physical Image* format E01 dari penyimpanan NVMe. Berdasarkan log akuisisi, proses berlangsung selama 3 menit 54 detik seperti yang disajikan pada Gambar 9, tapi verifikasi full 1 jam 31 menit dan menghasilkan nilai hash MD5 serta SHA-1 yang sama antara asli dan salinan, serta tidak ditemukan sektor rusak, sehingga keaslian bukti digital tersebut tetap terjaga dan bisa digunakan untuk analisis selanjutnya. Proses akuisisi bukti digital dilakukan dengan mengambil data dari sistem Windows Server 2025 untuk membuat salinan forensik dalam format E01, yaitu file gambar yang dikompresi dan terlindungi. Proses ini menggunakan perangkat lunak FTK Imager dengan melakukan pemeriksaan integritas data menggunakan perhitungan algoritma *hash*.



Gambar 9. Akuisisi Disk dengan FTK Imager

Berdasarkan pedoman ISO/IEC 27042, tahap verifikasi terhadap *Full Volume Encryption* dilakukan guna menentukan kebutuhan prosedur dekripsi sebelum analisis artefak dilanjutkan. Melalui pemeriksaan teknis pada Basic Data Partition 3 menggunakan FTK Imager, analisis hex *header* pada offset 0x03 menunjukkan file *system signature* berupa "NTFS" secara eksplisit, yang menandakan bahwa partisi sistem Windows Server 2025 berada dalam kondisi tidak terenkripsi (*unencrypted*). Hal ini didukung oleh kemampuan panel *Evidence Tree* untuk memuat struktur direktori utama seperti folder Windows, Users, dan Program Files secara plaintext, yang secara teknis membuktikan tidak adanya tanda tangan Full Volume Encryption File System (FVE-FS) yang umum ditemukan pada volume terproteksi BitLocker seperti yang disajikan pada Gambar 10. Dengan terbukanya akses

langsung terhadap konten partisi, investigator dapat mengonfirmasi bahwa data sistem dapat diinterpretasikan secara utuh tanpa hambatan enkripsi, sehingga proses analisis forensik terhadap artefak *malware* dapat dilaksanakan secara valid.



Gambar 10. Pemeriksaan BitLocker

4.4. Preservasi

Preservasi bertujuan menjaga integritas data. Dilakukan perhitungan nilai *hash* menggunakan algoritma MD5 dan SHA-1/SHA-256 segera setelah akuisisi. Hasil verifikasi *hash* ditunjukkan pada Tabel 1. Hasil nilai hashing menunjukkan status cocok, memastikan bahwa salinan identik dengan data asli dan integritas terjaga selama investigasi. Setelah penghitungan hash selesai, dilakukan proses kloning atau pembuatan salinan dari file akuisisi dalam format E01 (untuk disk) dan DMP (untuk memori).

Tabel 1. Preservasi Hash Barang Bukti dan Salinan

Barang Bukti	Tipe Hash	Status
Image Disk (E001)	MD5 & SHA-1	Cocok
Memory Dump (DMP)	SHA-256	Cocok

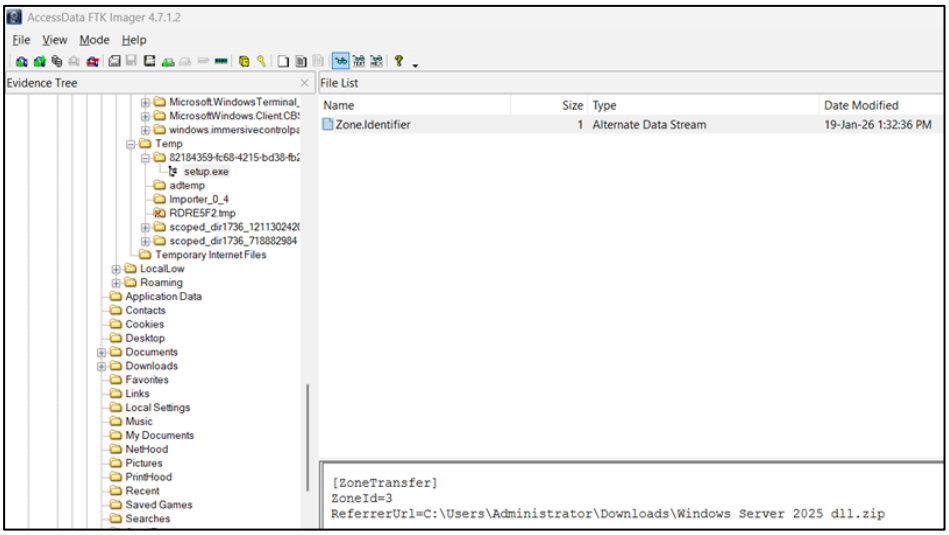
Proses kloning bertujuan untuk menjaga integritas data asli selama proses investigasi, dengan memastikan bahwa analisis forensik hanya dilakukan pada salinan, bukan pada data asli. Hal itu penting untuk meminimalkan risiko perubahan (modifikasi) atau kerusakan bukti digital yang dapat memengaruhi validitas hasil investigasi. Selain itu, proses kloning juga mendukung prinsip *chain of custody* dan forensik yang dapat dipertanggungjawabkan, dengan memastikan bahwa data asli tetap utuh dan tidak terpengaruh selama proses investigasi. Setelah salinan dibuat, dilakukan verifikasi integritas dengan mencocokkan nilai hash antara file asli dan salinannya. Karena nilai hash keduanya sama (identik), maka dapat dipastikan bahwa salinan benar-benar identik dengan data asli, dan tidak ada perubahan yang terjadi selama proses kloning. Proses preservasi data tersebut didokumentasikan dalam *Chain of Custody* pada 20 Januari 2026 pukul 13:00 WIB dan disimpan di Lemari Penyimpanan Bukti.

4.5. Analisis

Analisis dilakukan terhadap bukti *image disk* dan memori menggunakan standar ISO/IEC 27042.

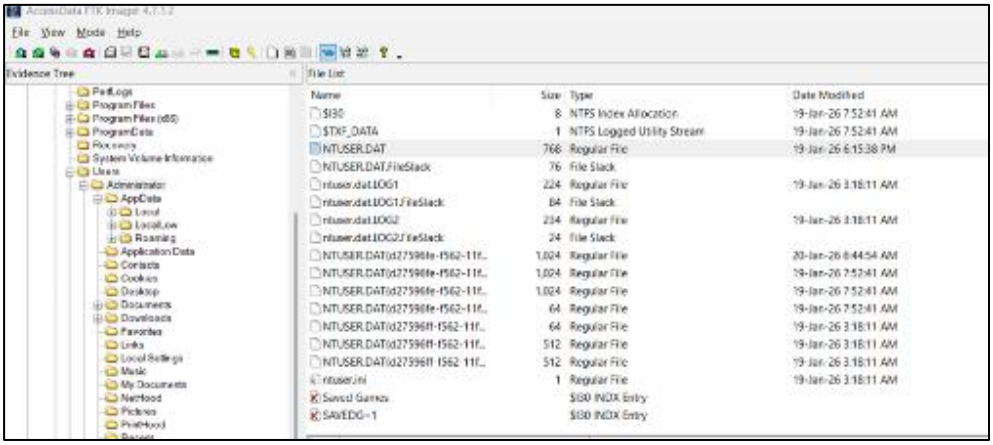
1. *Analisis Artefak Sistem Berkas (Disk)*

Teridentifikasi berkas *setup.exe* di direktori *Downloads*. Analisis menggunakan fitur *Alternate Data Stream* (ADS) pada artefak *Zone.Identifier* menunjukkan nilai ZoneId=3. Nilai ini membuktikan secara hukum bahwa file diunduh dari zona Internet. Referrer URL menunjukkan file berasal dari Windows Server 2025 dll.zip. Analisis Registry pada *hive NTUSER.DAT* mengungkap jejak eksekusi *setup.exe* oleh pengguna, yang dikonfirmasi oleh log *Amcache.hve*. Ini membuktikan interaksi manual pengguna terhadap *malware*.



Gambar 11. Analisis *Disk* pada ADS

Terdapat textbox yang berisikan ZoneId=3 menunjukkan bahwa berkas ini diunduh dari zona internet (risiko tinggi). Terdeteksi bahwa *setup.exe* berasal dari hasil ekstraksi berkas kompresi bernama Windows Server 2025 dll.zip dengan adanya tulisan ReferrerUrl. Hal ini memperkuat skenario *phishing* di mana korban menerima paket unduhan palsu.

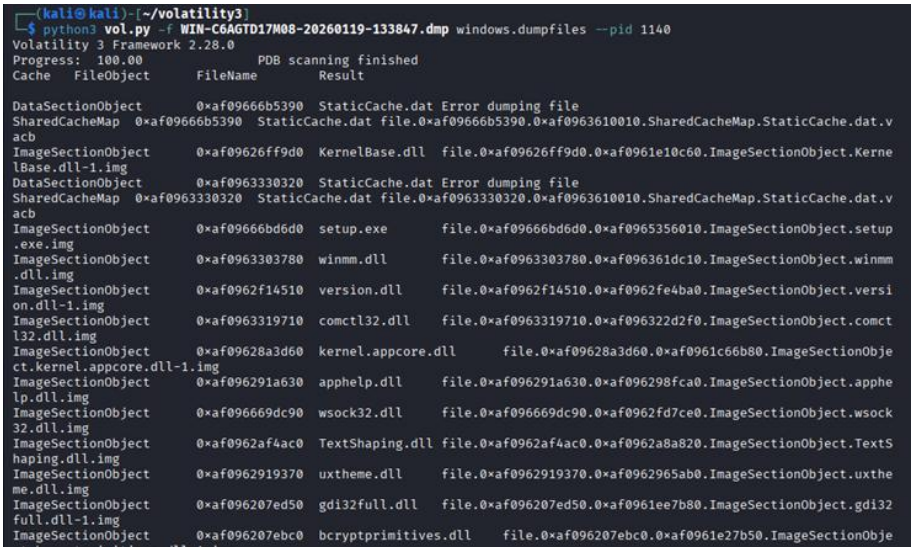


Gambar 12. Analisis Disk pada *NTUSER.DAT*

Terekam entri terkait *setup.exe* di dalam direktori, yang menandakan adanya interaksi pengguna terhadap berkas tersebut. Log *NTUSER.DAT* tersebut dilihat merupakan jenis file biasa namun ketika dilihat lebih lanjut pada *textbox*, terlihat bahwa terdapat log *setup.exe*. Kemudian, pemeriksaan pada *Amcache.hve*.LOG1 menunjukkan rekaman metadata aplikasi *setup.exe*. Artefak ini sangat valid untuk membuktikan *timestamp* kapan program pertama kali dijalankan dan lokasi instalasinya di sistem, meskipun berkas aslinya mungkin sudah dihapus yang mana ditunjukkan pada tanggal 20 Januari 2026 pada pukul 20:16:33 WIB.

2. *Analisis Memori (RAM)*

Menggunakan *Volatility 3*, terdeteksi proses *setup.exe* berjalan dengan Process ID (PID) 1140. Proses ini dipicu oleh Parent PID 3672 (Explorer). Analisis modul menunjukkan *malware* memuat user32.dll, yang menjelaskan manipulasi grafis pada layar, serta ws2_32.dll yang mengindikasikan kemampuan koneksi jaringan.



Gambar 13. Analisis RAM dengan Volatility 3

Terekam proses bernama *setup.exe* dengan Process ID (PID) 1140. Keberadaan proses ini selaras dengan temuan pada analisis sistem berkas yang mana file tersebut teridentifikasi sebagai agen infeksi utama. Proses *setup.exe* dipicu oleh Parent PID (PPID) 3672. Analisis pada PPID tersebut menunjukkan keterkaitan dengan sesi pengguna yang aktif, mengonfirmasi bahwa eksekusi terjadi akibat interaksi manual oleh pengguna (*Administrator*). Melalui analisis lebih lanjut pada PID 1140, diketahui bahwa *setup.exe* memuat berbagai pustaka dinamis (DLL) penting seperti kernel32.dll, user32.dll, dan ws2_32.dll. Pemuatan user32.dll menjelaskan mengapa terjadi gangguan pada antarmuka grafis yang dirasakan pengguna, sementara ws2_32.dll menunjukkan bahwa *malware* memiliki kemampuan koneksi jaringan keluar.

4.6. Interpretasi

Berdasarkan korelasi bukti digital antara artefak sistem berkas (*non-volatile*) dan memori fisik (*volatile*), teridentifikasi bahwa vektor serangan awal bermula dari aktivitas pengunduhan berkas berbahaya melalui peramban web. Analisis forensik disk pada artefak *Alternate Data Stream* (ADS) secara konklusif menunjukkan bahwa berkas *setup.exe* memiliki atribut ZoneId=3 dengan ReferrerUrl yang mengarah pada arsip Windows Server 2025 dll.zip. Temuan ini mengindikasikan bahwa subjek penelitian (pengguna) telah terpapar teknik rekayasa sosial (*social engineering*), di mana *malware* disamarkan sebagai komponen sistem yang sah. Keberadaan berkas tersebut di direktori *Temporary* mengonfirmasi bahwa eksekusi terjadi segera setelah proses ekstraksi arsip dilakukan, memvalidasi hipotesis bahwa infeksi terjadi akibat interaksi langsung pengguna terhadap objek unduhan yang tidak terverifikasi keamanan sumbernya.

Validasi terhadap eksekusi *malware* diperkuat melalui analisis forensik memori yang menunjukkan adanya konsistensi temporal (waktu) dan perilaku sistem. Proses *setup.exe* terdeteksi aktif dengan PID 1140, yang berjarak sekitar lima menit sebelum proses akuisisi memori dilakukan. Pola proses ini memiliki korelasi linear dengan aktivitas proses chrome.exe yang masif pada rentang waktu yang berdekatan, serta didukung oleh bukti persistensi pada *hive* registri *Amcache.hve* dan *NTUSER.DAT*. Hal ini membuktikan bahwa *setup.exe* bukan sekadar berkas pasif yang tersimpan di *hard disk*, melainkan entitas berbahaya yang berhasil menjangkiti memori (*resident in memory*) dan memiliki *lifecycle* aktif pada saat insiden berlangsung.

Ditinjau dari kapabilitas teknisnya, analisis struktur memori pada PID 1140 mengungkap potensi dampak destruktif terhadap kerahasiaan dan integritas sistem. Teridentifikasinya pemuatan modul pustaka dinamis (DLL) ws2_32.dll mengindikasikan kemampuan *malware* untuk menginisiasi koneksi jaringan (*socket creation*), yang berpotensi digunakan untuk komunikasi *Command and Control* (C2) atau eksfiltrasi data. Selain itu, injeksi terhadap modul grafis user32.dll memberikan penjelasan teknis terhadap anomali visual yang dilaporkan terjadi pada antarmuka pengguna. Dengan integritas bukti yang terjamin melalui verifikasi *hash* SHA-256, penelitian ini menyimpulkan bahwa sistem Windows Server 2025 telah mengalami kompromi keamanan tingkat lanjut yang diawali dari kelalaian pengguna dalam memvalidasi integritas berkas unduhan.

4.7. Pelaporan

Laporan disusun berdasarkan fakta hukum yang ditemukan. Pengguna target diverifikasi sebagai pemilik akun email hanifnh15@outlook.com. Kerugian yang ditimbulkan mencakup gangguan operasional server dan anomali visual persisten yang mengganggu responsivitas layanan grafis. Analisis ini menyajikan fakta-fakta hukum yang ditemukan dari proses analisis *Live Forensics* terhadap citra memori (*memory dump*) dan artefak sistem pada Windows Server 2025. Seluruh temuan yang dipaparkan telah melalui proses verifikasi integritas menggunakan fungsi *hashing* SHA-256 dan dikorelasikan antar artefak untuk merekonstruksi kronologi insiden *Persistent Windows Server Glitch Malware*. Pelaporan ini bertujuan untuk menjawab hipotesis investigasi terkait intrusi *malware* yang menyebabkan gangguan visual dan operasional pada server.

6. KESIMPULAN

Pada fase awal masuknya ancaman ke dalam sistem, artefak digital menunjukkan pola yang konsisten dengan aktivitas pengunduhan berkas dari sumber eksternal. Artefak sistem berkas, khususnya *Alternate Data Streams* (ADS), secara eksplisit menandai berkas *setup.exe* dengan ZoneId=3, yang mengindikasikan bahwa berkas tersebut berasal dari zona Internet. Hal ini diperkuat dengan temuan pada direktori unduhan yang menjadi lokasi awal keberadaan berkas. Temuan ini menegaskan bahwa pada tahap inisiasi, pertahanan sistem ditembus melalui interaksi pengguna terhadap berkas yang diunduh, bukan melalui eksploitasi celah keamanan jaringan secara langsung. Pada kondisi saat *malware* berhasil dieksekusi, analisis memori (*RAM*) mengungkapkan aktivitas proses yang destruktif dan manipulatif. Proses *setup.exe* teridentifikasi berjalan dengan PID 1140 dan memuat modul-modul kritis sistem. Modul ws2_32.dll yang dimuat mengindikasikan kapabilitas koneksi jaringan, sementara manipulasi terhadap modul user32.dll dan *User Media* menjadi penyebab teknis utama gangguan visual pada layar server. Hal ini menunjukkan bahwa pada skenario eksekusi, *malware* mampu beroperasi di memori aktif dan memanipulasi fungsi sistem operasi untuk menciptakan gangguan yang persisten.

Pada aspek persistensi dan atribusi pengguna, artefak *registry* meninggalkan jejak yang tidak terbantahkan meskipun insiden telah berlalu. *Hive NTUSER.DAT* merekam interaksi spesifik pengguna Hanif Nur dalam mengeksekusi berkas tersebut, yang menjadi bukti atribusi subjek hukum. Selain itu, artefak *Amcache.hve* tetap menyimpan metadata rinci termasuk jalur fail dan nilai *hash* SHA-1 dari *setup.exe*. Hal ini menegaskan bahwa meskipun berkas mungkin dihapus atau disembunyikan di kemudian hari, sistem Windows tetap menyisakan residu pencatatan eksekusi program pada basis data kompatibilitas aplikasi. Dari keseluruhan temuan, dapat disimpulkan bahwa artefak digital dari *disk* maupun memori dapat ditemukan, dianalisis, dan diinterpretasikan untuk merekonstruksi serangan *malware*, mulai dari metode pengunduhan, dampak eksekusi di memori, hingga jejak interaksi pengguna.

Sementara itu, penerapan ISO/IEC 27037:2012 dan ISO/IEC 27042:2015 dalam seluruh tahapan forensik meliputi identifikasi, akuisisi, preservasi, analisis, interpretasi, hingga pelaporan mampu menjaga integritas dan keaslian bukti digital. Hal ini dibuktikan dengan penggunaan metode *hashing* SHA-256 pada proses verifikasi hasil akuisisi, pencatatan yang sistematis, serta penyusunan laporan forensik yang sesuai standar. Penelitian yang telah dilakukan menjelaskan bahwa meskipun serangan *malware* bersifat merusak, sistem operasi tetap menyisakan artefak digital yang valid yang dapat digunakan untuk investigasi forensik digital. Hasil investigasi dapat dipertanggungjawabkan dengan menerapkan standar ISO/IEC 27037:2012 dan ISO/IEC 27042:2015.

Penelitian ini memiliki beberapa keterbatasan, di antaranya pengujian yang dilakukan pada lingkungan tersimulasi (skenario *phishing* yang dikontrol) pada Windows Server 2025 dengan konfigurasi standar tunggal sehingga tidak sepenuhnya mencerminkan kompleksitas penyebaran *malware* di infrastruktur jaringan skala organisasi yang sebenarnya. Untuk penelitian selanjutnya, disarankan untuk melakukan pengujian menggunakan topologi jaringan terdistribusi serta mengintegrasikan pemantauan keamanan otomatis secara *real-time* berbasis *machine learning* untuk mendeteksi anomali (*glitch*) secara dinamis.

REFERENSI

[1] N. Reuben, R. Irawan, R. N. Jovann, S. Achmad, F. A. Junior, and Nadia, "Raising Cyber Security Awareness to Reduce Social Engineering Through Social Media in Indonesia," in Proc. 3rd Int. Conf. Electronic and Electrical Engineering and Intelligent System (ICE3IS), 2023, doi: 10.1109/ICE3IS59323.2023.10335454.

[2] M. U. Rana, M. A. Shah, and O. Ellahi, "Malware Persistence and Obfuscation: An Analysis on Concealed Strategies," in Proc. 26th Int. Conf. Automation and Computing (ICAC), 2021, doi: 10.23919/ICAC50006.2021.9594197.

[3] Nasrullah, Judhariksawan, A. Ilyas, and Haeranah, "The Role of Digital Forensics in Criminal Investigations: An Analysis of Electronic Evidence in the Indonesian Legal System," Pakistan Journal of Criminology, vol. 16, no. 4, pp. 255–268, Dec. 2024.

[4] Badan Standardisasi Nasional, "SNI ISO/IEC 27037:2012 Teknologi Informasi — Teknik Keamanan — Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital," Jakarta, Indonesia, 2014.

[5] Badan Standardisasi Nasional, "SNI ISO/IEC 27042:2015 Teknologi Informasi — Teknik Keamanan — Pedoman untuk Analisis dan Interpretasi Bukti Digital," Jakarta, Indonesia, 2021.

[6] R. Sihwail, K. Omar, and K. Z. Ariffin, "A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis," International Journal of Advanced Science Engineering and Information Technology, vol. 8, no. 4-2, p. 1662, 2018.

[7] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," IEEE Access, vol. 10, pp. 11065–11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[8] Volatility Foundation, "Volatility Foundation," [Online]. Available: https://www.volatilityfoundation.org/. [Accessed: Feb. 12, 2025].

[9] N. D. W. Cahyani, E. M. Jadied, N. H. A. Rahman, and E. Ariyanto, "The Influence of Virtual Secure Mode (VSM) on Memory Acquisition," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 11, p. 547, 2022, ISSN: 2156-5570.

[10] J. Krause, Mastering Windows Server 2025: Accelerate Your Journey from IT Pro to System Administrator Using the World's Most Powerful Server Platform. Birmingham, U.K.: Packt Publishing, 2025.

[11] H. Nyholm, K. Monteith, S. Lyles, M. Gallegos, M. DeSantis, J. Donaldson, and C. Taylor, "The Evolution of Volatile Memory Forensics," Journal of Cybersecurity and Privacy, vol. 2, no. 3, 2022.