PENERAPAN VOLATILITY DALAM MEMORY FORENSICS UNTUK DETEKSI REMOTE ACCESS TROJAN MELALUI PORT 1337

I Komang Ary Wiguna[1*], I Nyoman Andy Wirajaya[2], Indriyani[3]
[123]Program Studi Teknologi Informasi, ITB Stikom Bali, Bali 80363, Indonesia
arywiguna206@gmail.com, andywirajaya13@gmail.com, indriyani@stikom-bali.ac.id

Abstrak

Perkembangan teknologi informasi meningkatkan ancaman keamanan siber, salah satunya malware jenis Trojan yang dapat memberikan akses ilegal kepada penyerang melalui komunikasi jaringan tersembunyi. Penelitian ini bertujuan mengidentifikasi indikasi serangan Trojan melalui analisis memory forensics menggunakan Volatility Framework pada file memory dump sistem operasi Windows XP SP2 32-bit. Proses analisis dilakukan menggunakan plugin imageinfo, psscan, procdump, dan connscan untuk mengidentifikasi profil sistem, proses aktif, file executable, serta koneksi jaringan mencurigakan pada port 1337. Hasil penelitian menunjukkan adanya proses notepad.exe dengan PID 1776 yang terhubung dengan IP remote melalui port 1337. File hasil process dumping kemudian diverifikasi menggunakan VirusTotal dan terdeteksi malicious oleh 59 dari 72 engine antivirus dengan tingkat deteksi sebesar 79,17%. Hasil penelitian menunjukkan bahwa metode memory forensics mampu membantu proses investigasi digital dalam mendeteksi aktivitas Trojan melalui analisis artefak volatile pada memory dump.

Kata kunci : Memory Forensics, Trojan, Volatility, Port 1337, Digital Forensics.

Abstract

The development of information technology has increased cybersecurity threats, one of which is Trojan malware that can provide unauthorized access to attackers through hidden network communications. This study aims to identify indications of Trojan attacks through memory forensics analysis using Volatility Framework on a Windows XP SP2 32-bit memory dump file. The analysis process used the imageinfo, psscan, procdump, and connscan plugins to identify system profiles, active processes, executable files, and suspicious network connections on port 1337. The results showed the presence of a notepad.exe process with PID 1776 connected to a remote IP through port 1337. The dumped executable file was then verified using VirusTotal and detected as malicious by 57 out of 73 antivirus engines with a detection rate of 79.17%. The results indicate that the memory forensics method can support digital investigation processes in detecting Trojan activity through the analysis of volatile artifacts in memory dumps.

Keywords*: Memory Forensics, Trojan, Volatility, Port 1337, Digital Forensics.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan jaringan komputer memberikan banyak kemudahan dalam komunikasi dan pertukaran data[1]. Namun, perkembangan tersebut juga meningkatkan berbagai ancaman keamanan siber, salah satunya adalah serangan malware jenis Trojan yang dapat menyusup ke dalam sistem tanpa disadari pengguna dan memberikan akses ilegal kepada penyerang[2]. Trojan merupakan malware yang menyamar

sebagai aplikasi normal untuk mengelabui pengguna agar menginstalnya. Setelah berhasil masuk ke dalam sistem, Trojan bekerja secara tersembunyi dan memungkinkan attacker memperoleh akses tidak sah ke perangkat korban[3].
Salah satu jenis Trojan yang umum digunakan adalah Remote Access Trojan (RAT), yaitu malware yang memungkinkan penyerang mengendalikan sistem korban dari jarak jauh melalui koneksi jaringan[4]. Dengan RAT, penyerang dapat mencuri data penting, memantau aktivitas pengguna, serta mengontrol file dan perangkat tanpa sepengetahuan korban. Dalam praktiknya, Trojan sering memanfaatkan port tertentu sebagai jalur komunikasi tersembunyi antara attacker dan korban. Salah satu port yang sering dikaitkan dengan aktivitas backdoor dan komunikasi ilegal adalah port 1337[5]. Aktivitas jaringan pada port tersebut dapat menjadi indikasi adanya serangan Trojan dalam sistem.

Menurut laporan keamanan siber global, serangan malware dan ransomware terus mengalami peningkatan setiap tahunnya seiring berkembangnya teknologi jaringan dan internet[6]. Malware berbasis backdoor dan RAT menjadi salah satu ancaman yang banyak digunakan dalam serangan siber modern karena mampu memberikan akses jarak jauh secara tersembunyi kepada penyerang. Kondisi ini menunjukkan bahwa deteksi aktivitas malware pada sistem komputer menjadi hal yang sangat penting untuk mendukung keamanan jaringan dan proses investigasi digital[7].

Keamanan jaringan merupakan upaya untuk melindungi sistem dari akses tidak sah, serangan siber, dan penyalahgunaan data dengan menerapkan mekanisme seperti firewall, enkripsi, serta intrusion detection system (IDS)[8]. Namun, metode keamanan tradisional masih memiliki keterbatasan dalam mendeteksi artefak volatile yang berada di memori sistem. Firewall dan IDS umumnya hanya memantau lalu lintas jaringan dan aktivitas sistem secara real-time, tetapi tidak mampu mengidentifikasi artefak yang tersimpan sementara di RAM, seperti proses tersembunyi, injeksi malware, dan koneksi jaringan yang telah berhenti namun masih tersimpan dalam memory dump. Selain itu, Trojan cenderung berjalan di latar belakang dan menggunakan teknik penyamaran sehingga sulit dideteksi melalui analisis konvensional.

Oleh karena itu, diperlukan pendekatan Digital Forensics, khususnya memory forensics, untuk menganalisis aktivitas tersembunyi yang terdapat pada memori sistem. Digital forensics merupakan proses identifikasi, pengumpulan, analisis, dan pelaporan bukti digital secara sistematis untuk kebutuhan investigasi[9]. Dalam penelitian ini, proses analisis dilakukan menggunakan Volatility, yaitu tools open-source yang digunakan untuk menganalisis memory dump dan mengekstraksi informasi penting seperti proses aktif, koneksi jaringan, serta indikasi keberadaan malware[3], [10].

Penelitian sebelumnya umumnya berfokus pada analisis malware secara umum tanpa menitikberatkan pada komunikasi jaringan melalui port tertentu. Oleh karena itu, penelitian ini memiliki kebaruan dengan mengintegrasikan analisis memory forensics menggunakan Volatility dan identifikasi komunikasi pada port 1337 sebagai indikator aktivitas Remote Access Trojan (RAT)[11]. Pendekatan ini diharapkan dapat menjadi framework investigasi awal dalam mendeteksi malware berbasis komunikasi jaringan tersembunyi.

Penelitian ini bertujuan untuk mengidentifikasi koneksi jaringan mencurigakan serta mendeteksi indikasi serangan Trojan berdasarkan data memory dump. Hasil penelitian diharapkan dapat membantu proses investigasi digital forensics, menjadi referensi dalam analisis

malware berbasis memory forensics, serta meningkatkan keamanan jaringan komputer[12].

2. METODE

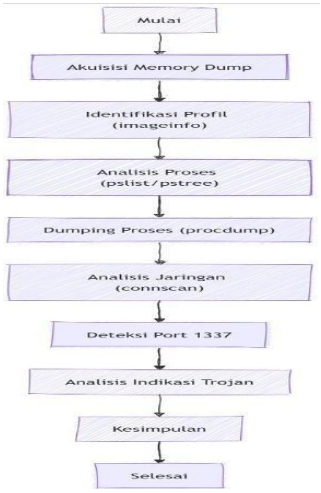
Penelitian ini menggunakan metode eksperimen dengan pendekatan digital forensics berbasis memory forensics untuk mengidentifikasi aktivitas mencurigakan dan indikasi serangan malware Trojan pada sistem komputer. Analisis dilakukan menggunakan Volatility melalui file memory dump yang diperoleh dari sistem operasi Microsoft Windows XP[13].

Pendekatan memory forensics dipilih karena mampu menganalisis artefak digital yang bersifat volatile di dalam RAM, seperti proses aktif, koneksi jaringan, modul sistem, dan aktivitas malware yang tidak tersimpan pada hard disk. Dengan metode ini, proses investigasi dapat dilakukan secara lebih mendalam terhadap aktivitas yang sedang berjalan pada sistem[14].

Lingkungan pengujian menggunakan Volatility Framework versi 2.6 yang dijalankan melalui Command Prompt (CMD) pada sistem operasi Microsoft Windows. Objek penelitian berupa file memory dump dengan profil sistem WinXPSP2x86 yang berasal dari sistem operasi Microsoft Windows XP Service Pack 2 32-bit. File memory dump digunakan sebagai sumber utama dalam proses analisis untuk mengidentifikasi proses aktif, koneksi jaringan, serta indikasi aktivitas malware pada sistem[12].

Tahapan penelitian dilakukan secara sistematis mulai dari identifikasi profil sistem, analisis proses aktif, process dumping, analisis koneksi jaringan, hingga interpretasi hasil investigasi. Validasi hasil dilakukan dengan mengkorelasikan PID proses, hasil process dumping, dan koneksi jaringan yang diperoleh menggunakan plugin connscan untuk memastikan adanya hubungan antara proses mencurigakan dan aktivitas komunikasi jaringan pada port 1337.

- Alur Penelitian



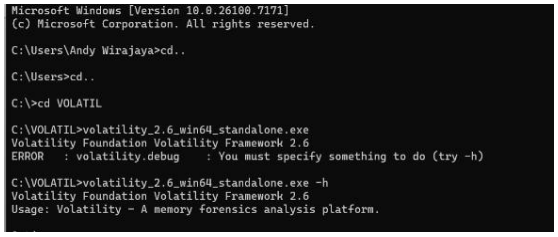
Gambar 1 Flowchart

Tabel 2.1 Tahapan Penelitian

Tahap	Input	Proses	Output
Akuisisi Data	Memory dump	Pengambilan file memory	File memory dump
Identifikasi Sistem	Memory dump	Analisis menggunakan imageinfo	Profil WinXPSP2x86
Analisis Proses	Memory dump	Analisis menggunakan psscan	PID proses aktif
Process Dumping	PID proses	Ekstraksi executable menggunakan procdump	File executable
Analisis Jaringan	Memory dump	Analisis koneksi menggunakan connscan	Informasi IP dan port
Korelasi Data	PID, IP, port	Analisis hubungan proses dan koneksi	Indikasi aktivitas Trojan
Interpretasi Hasil	Seluruh artefak digital	Analisis keseluruhan hasil investigasi	Kesimpulan investigasi

..

2.1. Tampilan Awal Volatility



Gambar 2 Tampilan Awal Volatility

Tahap awal penelitian dilakukan dengan menjalankan Volatility melalui Command Prompt (CMD). Pengguna masuk ke direktori tempat file Volatility berada menggunakan perintah cd, kemudian menjalankan file volatility_2.6_win64_standalone.exe.

Ketika dijalankan tanpa parameter, Volatility menampilkan pesan kesalahan yang menunjukkan bahwa pengguna perlu menentukan plugin atau perintah tertentu untuk melakukan analisis. Selanjutnya, digunakan opsi -h (help) untuk menampilkan daftar plugin dan informasi penggunaan tools dalam proses memory forensics.

Tahap ini bertujuan untuk memastikan tools dapat berjalan dengan baik sebelum dilakukan analisis terhadap memory dump.

2.2 Analisis Memory dan Informasi Sistem

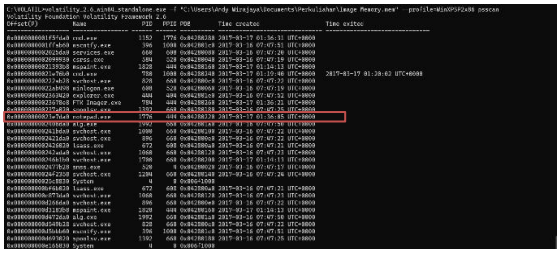
Gambar 3 Analisis Memory dan Informasi

Tahap berikutnya dilakukan analisis memory menggunakan perintah imageinfo untuk mengidentifikasi profil sistem dari file memory dump. Hasil analisis menunjukkan bahwa sistem menggunakan profil WinXPSP2x86, yaitu Microsoft Windows XP Service Pack 2 dengan arsitektur 32-bit.

Informasi profil sistem sangat penting karena menentukan kompatibilitas plugin yang digunakan pada proses analisis lanjutan, seperti identifikasi proses aktif dan koneksi jaringan[15].

Pada penelitian ini, penggunaan plugin netscan tidak dapat dilakukan karena profil WinXPSP2x86 tidak mendukung plugin tersebut. Oleh karena itu, analisis jaringan difokuskan menggunakan plugin connscan yang kompatibel dengan sistem. Keterbatasan ini menyebabkan analisis jaringan hanya difokuskan pada koneksi aktif yang berhasil terdeteksi dalam memory dump.

2.3 Analisis Proses Aktif



Gambar 4 Analisis Notepad.exe

Tahap analisis proses dilakukan menggunakan plugin **psscan** untuk mengidentifikasi proses yang sedang berjalan pada sistem. Analisis ini bertujuan menemukan proses yang mencurigakan atau tidak normal berdasarkan nama proses, PID, serta hubungan antar proses.

Hasil analisis menunjukkan adanya proses dengan PID 1776 yang terdeteksi sebagai notepad.exe. Proses tersebut kemudian dijadikan fokus investigasi karena memiliki indikasi aktivitas jaringan yang mencurigakan.

2.4 Process Dumping

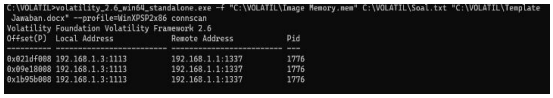
Gambar 5 Process Dumping

Setelah proses mencurigakan berhasil diidentifikasi, dilakukan process dumping menggunakan perintah procdump untuk

mengekstraksi file executable dari memori sistem.

Hasil dumping menunjukkan bahwa proses PID 1776 berhasil diekstraksi dengan status OK: executable.1776.exe. File hasil dump kemudian disimpan pada folder hasil untuk kebutuhan analisis lanjutan.
Process dumping dilakukan untuk memperoleh artefak digital yang dapat digunakan dalam proses identifikasi malware serta analisis hubungan antara proses aktif dan aktivitas jaringan pada sistem.

2.5 Analisis Koneksi Jaringan



Gambar 6 Analisis Koneksi Jaringan

Tahap selanjutnya adalah analisis koneksi jaringan menggunakan plugin connscan. Analisis ini dilakukan untuk mendeteksi koneksi aktif maupun koneksi tersembunyi yang terdapat pada memory dump.

Hasil analisis menunjukkan adanya koneksi jaringan sebagai berikut:

- IP Lokal (Korban) : 192.168.1.3
- Port Lokal : 1113
- IP Remote (Attacker) : 192.168.1.1
- Port Remote : 1337
- PID : 1776

Koneksi tersebut menunjukkan adanya komunikasi antara sistem korban dan attacker melalui port 1337. Port ini diketahui sering dikaitkan dengan aktivitas backdoor dan Remote Access Trojan (RAT), sehingga komunikasi tersebut menjadi indikasi adanya aktivitas malware pada sistem[16].

Untuk memperkuat hasil analisis, dilakukan korelasi antara PID proses, koneksi jaringan, dan hasil process dumping guna mengidentifikasi hubungan antara proses aktif dan komunikasi jaringan yang mencurigakan.

Tabel 2.2 Korelasi Proses dan Koneksi Jaringan

PID	Nama Proses	IP Lokal	IP Remote	Port	Indikasi
1776	notepad.exe	192.168.1.3	192.168.1.1	1337	Aktivitas mencurigakan

2.6 Interpretasi Hasil

Tahap akhir dilakukan dengan mengkorelasikan seluruh artefak digital yang diperoleh dari proses analisis, seperti PID proses, hasil process dumping, dan koneksi jaringan. Berdasarkan hasil korelasi, proses notepad.exe dengan PID 1776 teridentifikasi memiliki komunikasi jaringan menuju IP penyerang melalui port 1337 yang mengarah pada indikasi aktivitas Trojan atau Remote Access Trojan (RAT).

Hasil penelitian menunjukkan bahwa metode memory forensics menggunakan Volatility mampu membantu proses identifikasi aktivitas malware melalui analisis artefak volatile pada memory dump.

Identifikasi aktivitas mencurigakan diperkuat melalui analisis file executable hasil process dumping menggunakan **VirusTotal** untuk memverifikasi indikasi malware berdasarkan hasil deteksi antivirus. Berdasarkan hasil korelasi antara proses aktif, koneksi jaringan, dan hasil analisis executable, ditemukan indikasi aktivitas Remote Access Trojan (RAT) yang memanfaatkan komunikasi melalui port 1337.

3. HASIL DAN PEMBAHASAN

Proses analisis dilakukan menggunakan Volatility Framework terhadap file memory dump sistem Microsoft Windows XP Service Pack 2 32-bit dengan profil WinXPSP2x86. Tahap awal dilakukan menggunakan plugin imageinfo untuk mengidentifikasi profil sistem sebelum dilakukan analisis lanjutan. Hasil analisis

menunjukkan bahwa memory dump berasal dari sistem operasi Windows XP SP2 32-bit. Informasi profil sistem digunakan untuk menentukan kompatibilitas plugin dalam proses investigasi digital. Pada penelitian ini, plugin netscan tidak dapat digunakan karena tidak didukung oleh profil WinXPSP2x86, sehingga analisis jaringan difokuskan menggunakan plugin connscan.

Selanjutnya dilakukan analisis proses aktif menggunakan plugin psscan. Hasil analisis menunjukkan adanya proses notepad.exe dengan PID 1776 yang memiliki aktivitas mencurigakan. Proses tersebut kemudian diekstraksi menggunakan plugin procdump untuk memperoleh file executable dengan nama executable.1776.exe sebagai objek analisis malware lanjutan.

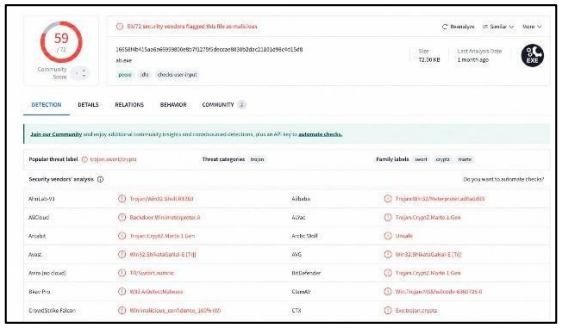
Analisis koneksi jaringan menggunakan plugin connscan menunjukkan adanya komunikasi jaringan antara IP lokal 192.168.1.3 dan IP remote 192.168.1.1 melalui port 1337 dengan PID 1776. Port 1337 diketahui sering dikaitkan dengan aktivitas backdoor dan Remote Access Trojan (RAT) karena digunakan sebagai jalur komunikasi tersembunyi antara attacker dan korban.

Hubungan antara PID proses dan koneksi jaringan menunjukkan bahwa proses notepad.exe memiliki aktivitas yang tidak normal dan diduga digunakan sebagai media penyamaran malware untuk melakukan komunikasi secara tersembunyi[17],[18].

Untuk memperkuat hasil analisis, file hasil process dumping dianalisis menggunakan VirusTotal untuk memverifikasi indikasi malware berdasarkan hasil deteksi antivirus. Hasil analisis menunjukkan bahwa file terdeteksi malicious oleh 59 dari 72 engine antivirus dengan tingkat deteksi sebesar.

$$\frac{59}{72} \text{ j } 100 = 79.17\%$$

Persentase tersebut menunjukkan indikasi kuat bahwa file merupakan malware jenis Trojan atau Remote Access Trojan (RAT). Hasil verifikasi menggunakan VirusTotal memperkuat hasil memory forensics sebelumnya yang menunjukkan adanya komunikasi mencurigakan melalui port 1337.



Gambar 7 Hasil Analisis VirusTotal

Berdasarkan keseluruhan hasil analisis, metode memory forensics menggunakan Volatility mampu membantu proses investigasi digital dalam mengidentifikasi artefak volatile seperti proses aktif, koneksi jaringan, dan file executable yang tidak dapat ditemukan melalui analisis disk konvensional. Korelasi antara proses aktif, koneksi jaringan, process dumping, dan verifikasi malware menunjukkan adanya indikasi aktivitas Trojan pada sistem komputer.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, metode memory forensics menggunakan Volatility Framework mampu membantu proses investigasi digital dalam mengidentifikasi aktivitas malware pada sistem komputer melalui analisis artefak volatile pada memory dump. Proses analisis menggunakan plugin imageinfo, psscan, procdump, dan connscan berhasil mengidentifikasi proses aktif, file executable, serta koneksi jaringan yang mencurigakan pada sistem operasi Windows XP SP2 32-bit.

Hasil penelitian menunjukkan adanya proses notepad.exe dengan PID 1776 yang melakukan komunikasi jaringan dengan IP remote 192.168.1.1 melalui port 1337. Port tersebut diketahui sering dikaitkan dengan aktivitas backdoor dan Remote Access Trojan (RAT). Selain itu, hasil process dumping dan verifikasi menggunakan VirusTotal menunjukkan bahwa file executable terdeteksi malicious oleh 59 dari 72 engine antivirus dengan tingkat deteksi sebesar 79,17%, sehingga memperkuat indikasi adanya aktivitas Trojan pada sistem.

Berdasarkan korelasi antara proses aktif, koneksi jaringan, dan hasil analisis executable, penelitian ini membuktikan bahwa pendekatan memory forensics efektif digunakan untuk mendeteksi aktivitas malware yang tidak dapat ditemukan melalui analisis disk konvensional. Penelitian ini juga menunjukkan bahwa analisis komunikasi jaringan melalui port 1337 dapat digunakan sebagai indikator awal dalam mendeteksi aktivitas Remote Access Trojan (RAT) pada sistem komputer.

DAFTAR PUSTAKA

[1] H. Pribadi Firtiani, K. Naya, N. Syaima Zain, and N. Nurhafidah, "Integrasi Teknologi Inovatif dalam Pengembangan Jaringan Komputer Untuk Pendidikan," *Jurnal Komputer, Informasi dan Teknologi*, vol. 5, no. 2, pp. 1–10, 2025, doi: 10.53697/jkomitek.v5i1.33.

[2] S. Nurmadani *et al.*, "Keamanan Informasi dalam Sistem Informasi Modern: Analisis Ancaman dan Upaya Pengamanan Berdasarkan Studi Literatur," 2026. doi: 10.62671/jikum.v2i1.141.

[3] S. Roberson, M. Abdus Salam, M. Kourouma, and O. Kandara, "Safely Scaling Virtual Private Network for a Major Telecom Company during A Pandemic," *International Journal of Computer Science and Information Technology*, vol. 14, no. 1, pp. 63–74, Feb. 2022, doi: 10.5121/ijcsit.2022.14105.

[4] J. Smallman, "A Survey on Malware Detection and Analysis," *Journal of Science & Technology*, vol. 5, no. 4, pp. 1–14, Jul. 2024, doi: 10.55662/jst.2024.5401.

[5] H. B. S. T. Annisa Rizky Damanik, "Analisis Trojan dan Spyware Menggunakan Metode Hybrid Analysis," *Jurnal Matrik*, vol. 25, no. 1, p. 1, Apr. 2023, doi: 10.33557/jurnalmatrik.v25i1.2327.

[6] Pasha, E. A., Utomo, Y. B., & Fatmawati, E. W. (2026). Model Edukasi Keamanan Digital Anak Berbasis Evaluasi Terstruktur pada Program KKN Internasional di Malaysia. KOMUNITA: Jurnal Pengabdian Dan Pemberdayaan Masyarakat, 5(2), 996–1005.

[7] C. J. W. Chew, V. Kumar, P. Patros, and R. Malik, "Real-time system call-based ransomware detection," *Int. J. Inf. Secur.*, vol. 23, no. 3, pp. 1839–1858, Jun. 2024, doi: 10.1007/s10207-024-00819-x.

[8] F. Ardiansyah Sihombing, N. N. Zuhra, L. Zahra, R. Alfarisyi, H. Nisa, and R. A. Astiyanto, "Implementasi Keamanan Jaringan Menggunakan Firewall dan Intrusion Detection System (IDS) pada Infrastruktur Jaringan Skala Kecil-Menengah," 2026. doi: 10.62671/jikum.v2i1.184.

[9] D. Sun *et al.*, "A Scale Balanced Loss for Bounding Box Regression," *IEEE Access*, vol. 8, pp. 108438–108448, 2020, doi: 10.1109/ACCESS.2020.3001234.

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

[11] H. Nyholm *et al.*, "The Evolution of Volatile Memory Forensics," Sep. 01, 2022, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/jcp2030028.

[12] S. Zhang, C. Hu, L. Wang, M. J. Mihaljevic, S. Xu, and T. Lan, "A Malware Detection Approach Based on Deep Learning and Memory Forensics," *Symmetry (Basel).*, vol. 15,

no. 3, Mar. 2023, doi: 10.3390/sym15030758.

[13] Sunbal Faraz Hayat, Mazhar Iqbal Sharif, Hafiz Muneed Ahmad, Ali Raza Lateef, Abdul Wahab Waseem, and I. Ahmad, "Deep Learning-Driven Malicious URL Detection: A comprehensive analysis using Convolutional Neural Networks A feature engineering on the Phiusiil dataset," *International Journal for Electronic Crime Investigation*, vol. 10, no. 1, Apr. 2026, doi: 10.54692/ijeci.2026.1001/266.

[14] A. S. Bozkir, E. Tahillioglu, M. Aydos, and I. Kara, "Catch them alive: A malware detection approach through memory forensics, manifold learning and computer vision," *Comput. Secur.*, vol. 103, Apr. 2021, doi: 10.1016/j.cose.2020.102166.

[15] A. A. Elsonbaty and M. Shams, "The Smart Parking Management System," *International Journal of Computer Science and Information Technology*, vol. 12, no. 4, pp. 55–66, Aug. 2020, doi: 10.5121/ijcsit.2020.12405.

[16] Rabia Mehmood, "Live Memory Forensic: Capture and Analyzing Volatile Data," *International Journal for Electronic Crime Investigation*, vol. 8, no. 3, Sep. 2024, doi: 10.54692/ijeci.2024.0803208.

[17] Asif Ibrahim, Syed Khurram Hassan, and Saima Sheikh, "Advanced Volatile Memory Forensics through Autopsy Integration," *International Journal for Electronic Crime Investigation*, vol. 8, no. 2, Jun. 2025, doi: 10.54692/ijeci.2024.0802195.

[18] S. Andy, "Automasi Forensik Memori berbasis Volatility dan YARA untuk Deteksi Ransomware," *Info Kripto*, vol.19, no. 3, pp. 135–143, Dec. 2025, doi: 10.56706/ik.v19i3.13