Jurnal Penelitian Sistem Informasi
Vol. 2 No. 1 Februari 2024
e-ISSN :2985-7759, p-ISSN :2985-6310, Hal 178-188
DOI: https://doi.org/10.54066/jpsi.v2i1.1594

Analisis Memory Forensics Windows Subsystem for Linux 2 (WSL2) Berbasis Hyper-V pada Windows 11 Berdasarkan Nist 800-86

Bagas Kurnadi
Keamanan Siber, PoltekSSN, Bogor
Korespondensi penulis: Bagas.kurnadi@poltekssn.ac.id

Fachrul Ali Nurfadillah
Keamanan Siber, PoltekSSN, Bogor
E-mail: Fachrul.ali@poltekssn.ac.id

Muhammad Tegar Sabila
Keamanan Siber, PoltekSSN, Bogor
E-mail: Muhammad.tegar@poltekssn.ac.id

Alamat: Jl. Raya H. Usa, Putat Nutug, Kec. Ciseeng, Kabupaten Bogor, Jawa Barat 16120

Abstract. *In the context of the growing blend of Windows and Linux operating systems through Windows Subsystem for Linux (WSL), this study explores forensic memory analysis on Hyper-V-based Windows Subsystem for Linux 2 (WSL2) in a Windows 11 environment using the NIST SP 800-86 method. WSL2, as the latest development of WSL, provides new opportunities in security and digital forensics, but also raises challenges related to security incidents. The study builds on the findings of previous research, focusing on forensic memory applications that have never been applied to WSL2 in Windows 11 before. By choosing Ubuntu 20.04 as the object of research and implementing the NIST SP 800-86 standard. The experimental results were obtained in scenario 1 where without deleting WSL2 all experimental artifacts were obtained or it can be said that artifacts were found by 100%, while in scenario 2 by deleting WSL2 only 2 experimental artifacts were found or by 16.7%. This research aims to provide in-depth insights into forensic analysis on WSL2, provide practical guidance for digital forensics experts in addressing security challenges that continue to evolve as technology evolves, and complement our understanding of security incidents involving a mix of Windows and Linux operating systems in the WSL2 era.*

Keywords: *digital forensics, virtual machine, linux, windows, wsl*

Abstrak. Dalam konteks berkembangnya perpaduan antara sistem operasi Windows dan Linux melalui Windows Subsystem for Linux (WSL), penelitian ini mengeksplorasi analisis memori forensik pada Windows Subsystem for Linux 2 (WSL2) berbasis Hyper-V di lingkungan Windows 11 dengan menggunakan metode NIST SP 800-86. WSL2, sebagai perkembangan terbaru dari WSL, memberikan peluang baru dalam keamanan dan forensik digital, tetapi juga memunculkan tantangan terkait insiden keamanan. Penelitian ini membangun pada temuan penelitian sebelumnya, berfokus pada aplikasi memori forensik yang belum pernah diterapkan pada WSL2 di Windows 11 sebelumnya. Dengan memilih Ubuntu 20.04 sebagai objek penelitian dan menerapkan standar NIST SP 800-86. Hasil percobaan didapatkan pada skenario 1 dimana tanpa melakukan penghapusan WSL2 didapatkan seluruh artefak percobaan atau dapat dikatakan artefak ditemukan sebesar 100%, sedangkan pada skenario 2 dengan menghapus WSL2 didapatkan hanya 2 artefak percobaan yang ditemukan atau sebesar 16.7 %. Penelitian ini bertujuan untuk memberikan wawasan mendalam terhadap analisis forensik pada WSL2, memberikan panduan praktis bagi ahli forensik digital dalam mengatasi tantangan keamanan yang terus berkembang seiring evolusi teknologi, dan melengkapi pemahaman kita tentang insiden keamanan yang melibatkan perpaduan sistem operasi Windows dan Linux di era WSL2.

Kata kunci: digital forensics, virtual machine, linux, windows, wsl

Received Desember 20, 2023, Accepted Januari 10, 2024; Published Februari 02, 2024
*Bagas Kurnadi, Bagas.kurnadi@poltekssn.ac.id

LATAR BELAKANG

Seiring berkembangnya teknologi, perpaduan antara sistem operasi Windows dan Linux menjadi semakin relevan melalui implementasi Windows Subsystem for Linux (WSL). Pada awalnya, Linux umumnya digunakan di lingkungan server, tetapi WSL merubah paradigma ini dengan memungkinkan pengguna menjalankan distribusi Linux di dalam lingkungan instalasi Windows 10 atau 11 tanpa perlu menginstall *virtual machine* terlebih dahulu [1].

Sejak diperkenalkan pada tahun 2016, WSL telah mengalami perkembangan yang cepat. Versi terbarunya, WSL version 2 (WSL2), memiliki arsitektur yang sepenuhnya diperbarui dibandingkan dengan versi sebelumnya, WSL versi satu. WSL2 sudah mendukung aplikasi yang menggunakan *Graphical User Interface* dalam Windows 11 [2]. Namun, kedatangan teknologi ini membawa peluang baru dalam keamanan dan proses forensik digital. WSL2, sebagai bagian dari evolusi WSL, memunculkan sejumlah masalah yang perlu ditangani. Penggunaannya meningkatkan permukaan serangan pada sistem Windows karena kehadiran WSL2, dengan beberapa serangan malware ditemukan dan beberapa masih dalam tahap pengembangan khusus di dalam lingkungan WSL2. Oleh karena itu, investigasi forensik digital menjadi krusial untuk mengatasi permasalahan keamanan yang muncul dari penggunaan WSL2.

Penelitian sebelumnya [3], melakukan analisis memori forensik di lingkungan WSL versi perrtama yang berjalan di Windows 10. Penelitian ini menggunakan framework Volatility dalam melakukan memori analisis. Penelitian ini berhasil mengembangkan algoritma forensik memori baru dan plugin Volatility yang memungkinkan analisis mendalam terhadap WSL. Penelitian lain [4] telah melakukan analisis forensik digital di lingkungan WSL2 yang berjalan di Windows 10. Penelitian ini tidak mengacu pada metode dengan standard tertentu. Tools yang digunakan pada penelitian ini adalah RegRipper, WindPrefectView, JumpListsView, dan Event Viewer. Selain itu, terdapat penelitian lain [4] bertujuan melakukan analisis forensik digital untuk menemukan artefak digital yang dapat ditemukan ketika WSL digunakan dalam sistem operasi Windows 11 dan di mana artefak-artefak ini muncul. Tools yang digunakan adalah FTK Imager, Registry Explorer, KAPE (Kroll Artifact Parser and Extractor), Magnet Axiom, dan beberapa tools lainnya. pada penelitian ini tidak menggunakan metode dari standard internasional namun secara garis besar metode yang digunakan adalah identifikasi, akuisisi dan analisis.

Pada penilitian ini akan dilakukan analisis memori forensik pada Hyper-V Berbasis Windows Subsystem For Linux 2 (Wsl2) Berdasarkan Metode Nist 800-86. penelitian ini

merupakan penelitian lanjutan dari penelitian [3], yang melakukan memori forensik pada WSL di windows 10 pada penelitian ini akan dilakukan analisis memori forensik WSL2 pada windows 11. Penelitian ini menggunakan sistem operasi Windows 11 karena Windows 11 merupakan versi terbaru dari Windows saat ini. Perbedaan lainnya adalah penggunaan standard NIST SP 800-86 yang memberikan metode digital forensik yang lebih komprehensif.

Selain itu, perbedaan dengan penelitian [2], penelitian ini akan melakukan penelitian dengan metode memori forensik. Penelitian ini menggunakan memori forensik karena belum ada penelitian yang menerapkan memori forensik pada WSL2 di windows 11. Selain itu, memori forensik dapat mengumpulkan data *real-time* terkait dengan sistem operasi dan berbagai jenis informasi dapat diekstraksi dari memori termasuk *processes, dynamic link libraries (dll), process memory, image identification, networking, registry, malware* [5]. Penelitian ini menggunakan Ubuntu 22.04 sebagai objek yang diteliti. Penelitian ini memilih Ubuntu karena ubuntu sampai saat ini masih menjadi distro linux dengan pengguna terbanyak [6]. Diharapkan penelitian ini dapat memberikan informasi mengenai proses analisis digital forensik serta analisis artefak yang ditemukan pada WSL2 pada Hyper-V berbasis windows.

METODE PENELITIAN

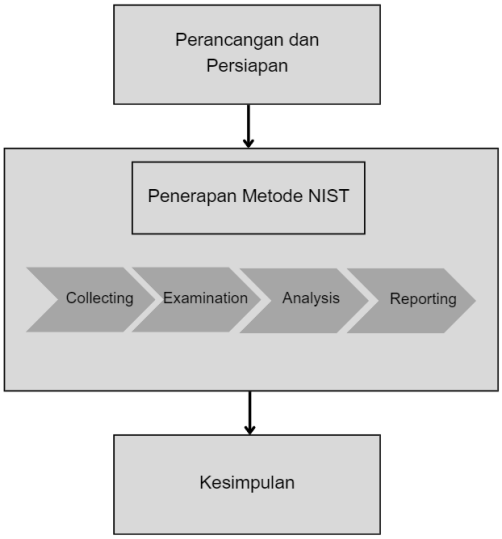
A. Objek Penelitian

Objek penelitian ini berupa Windows Subsystem for Linux 2 (WSL2) menggunakan Ubuntu 22.04 pada Sistem Operasi Windows 11. Data yang diolah pada penelitian ini adalah hasil forensik memori pada WSL2 menggunakan sistem operasi Windows 11. Penelitian ini mengimplementasikan tools HxD Hex Editor dan Volatility 3 Versi 2.4.1 untuk kebutuhan akuisisi dan analisis barang bukti digital dari WSL2 pada Sistem Operasi Windows 11.

B. Jenis penelitian

Penelitian ini mengadopsi jenis penelitian kualitatif dengan fokus pada analisis memory forensics pada Hyper-V berbasis Windows Subsystem for Linux 2 (WSL2), dengan penerapan metode NIST 800-86. Pendekatan kualitatif dipilih untuk memungkinkan pemahaman yang mendalam terhadap fenomena kompleks dalam konteks keamanan sistem. Dengan melibatkan studi kasus, penelitian ini akan mengeksplorasi secara mendalam tentang bagaimana WSL2 berinteraksi dengan Hyper-V, dengan penekanan pada identifikasi, akuisisi, dan analisis forensik memori. Jenis penelitian ini diharapkan dapat memberikan wawasan yang komprehensif terhadap tantangan keamanan yang mungkin muncul dari penggunaan WSL2 di lingkungan Hyper-V serta menyajikan solusi yang relevan melalui metode NIST 800-86.

C. Desain penelitian



Gambar 1. Diagram alir penelitian

Tahapan penelitian yang dilakukan pada penelitian ini dapat dilihat pada Gambar 1, yang merupakan tahapan forensik digital yang telah diolah dari [7]. Tahapan tersebut mencakup perancangan dan persiapan, identifikasi sampel dan data, penerapan metode NIST 800-86, dan kesimpulan.

a) Perancangan Lingkungan Penelitian

Menyiapkan lingkungan penelitian dengan mengonfigurasi Hyper-V yang menjalankan Windows Subsystem for Linux 2 (WSL2) seperti laptop dan tools yang diperlukan pada penelitian ini. Selain itu juga memastikan keamanan dan kestabilan lingkungan untuk memfasilitasi proses analisis memory forensics.

Tabel 1. Spesifikasi Device

No	Hardware	Spesifikasi
1	Infinix Inbook X1 Pro	Processor : Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz 1.50 GHz RAM : 16,0 GB (15,7 GB usable) OS : Windows 11 Pro 64 Bit Disk : 512GB

Tabel 2. *Tools* yang digunakan

No	Software	Keterangan
1	Ubuntu 22.04	Sistem operasi yang di install pada WSL
2	WSL2	Fitur dari Windows yang bisa menjalankan distribusi Linux
3	Volatility 3 Versi 2.4.1	Tools untuk mendapatkan salinan memori dari Windows
4	HxD	Editor untuk mengubah dan mengedit isi berkas biner dalam bentuk heksadesimal

b) Pengumpulan Data

Melakukan pengumpulan data forensik dengan mengambil data dari memory dan catatan kejadian dari mesin virtual yang berjalan di dalam WSL2. Memastikan bahwa proses pengumpulan data dilakukan secara teliti dan terdokumentasi. Skenario yang digunakan untuk mengumpulkan data pada penelitian ini adalah installasi WSL2 dengan distro linux Ubuntu 22.04, menjalankan WSL2, melakukan beberapa operasi file seperti membuat file, menghapus file, edit file, mengunduh file, dan menjalankan aplikasi. Proses selanjutnya yaitu menutup WSL2.

c) Examination

Proses examination mencakup identifikasi, ekstraksi, dan interpretasi data memori untuk memahami potensi kelemahan keamanan, jejak aktivitas, dan informasi forensik yang dapat mendukung investigasi pada lingkungan tersebut.

Tahap ini juga mencakup penggunaan alat-alat forensik yang digunakan pada penelitian ini yaitu HxD Hex Editor dan Volatility 3 Versi 2.4.1. Memastikan bahwa alat-alat tersebut diterapkan dengan benar dan menghasilkan hasil analisis yang akurat.

e) Analisis Data

Menganalisis hasil data yang diperoleh dari penggunaan alat forensik dan menerapkan metode NIST 800-86. Fokus pada temuan kritis, pola perilaku mencurigakan, dan potensi risiko keamanan yang mungkin muncul dalam lingkungan WSL2 di Hyper-V.

f) Penyusunan Laporan

Menyusun laporan penelitian yang mencakup semua tahapan penelitian, temuan, dan kesimpulan. Menyajikan laporan dengan jelas dan terstruktur agar dapat dipahami oleh pembaca.

g) Kesimpulan

Setelah melakukan semua tahapan diatas, akan dilakukan penarikan kesimpulan berdasarkan hasil penelitian yang dilakukan. Hasil analisis dari penelitian ini diharapkan dapat memberikan wawasan yang mendalam tentang keamanan serta temuan penting yang mendukung investigasi pada sistem WSL2 pada Windows 11.

HASIL DAN PEMBAHASAN

Metode NIST 800-86 merupakan kerangka kerja forensik yang diakui secara luas, terutama dalam analisis memori. Penerapannya dalam penelitian ini melibatkan serangkaian tahapan yang sistematis untuk mengumpulkan, memeriksa, menganalisis, dan melaporkan data memori dari Windows Subsystem for Linux 2 (WSL2) yang dijalankan di bawah Hyper-V pada Windows 11.

A. Tahap Collecting

Tahapan ini melibatkan pengumpulan data forensik dari sistem yang menjadi fokus penelitian, yaitu WSL2 di bawah Hyper-V. Penggunaan alat forensik Volatility 3 Versi 2.4.1 menjadi kunci dalam tahap ini. Volatility 3 Versi 2.4.1 digunakan untuk mengambil snapshot dari memori sistem pada titik tertentu selama eksperimen. Proses ini memungkinkan penciptaan salinan data memori yang dapat dianalisis lebih lanjut tanpa mempengaruhi integritas data asli.

Selama pengujian, skenario telah dirancang untuk mereplikasi situasi forensik yang umum di lingkungan WSL2, termasuk instalasi distro Linux, operasi file seperti pembuatan, pengeditan, dan penghapusan, serta aktivitas jaringan. Pengumpulan data mencakup informasi tentang kegiatan ini untuk mendapatkan gambaran menyeluruh tentang penggunaan sistem. Berikut dijelaskan skenario yang dilakukan:

Gambar 2. Skenario penelitian

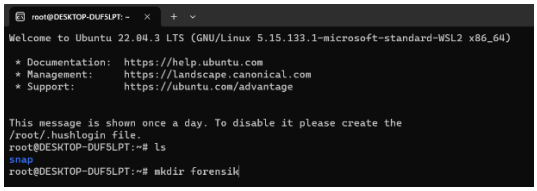
Skenario pada penelitian ini ditampilkan pada Gambar 2. Berikut penjelasan dari setiap skenario yang dilakukan:

a) Melakukan Instalasi WSL2

Tahapan ini dilakukan pengunduhan dan instalasi WSL2 juga memastikan konfigurasi yang diperlukan untuk menjaankan WSL2.

b) Menjalankan WSL2

Setelah proses instalasi jalankan WSL2 pada sistem operasi untuk malekukan skenario berikutnya. Pada tahap ini dilakukan pembuatan direktori di dalam WSL2.



Gambar 3. Membuat direktori forensic

c) Operasi File

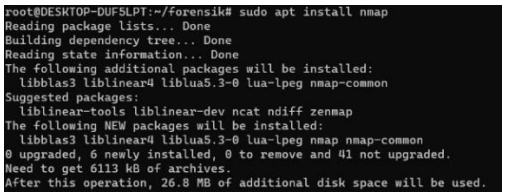
Melakukan serangkaian operasi file dasar yaitu membuat 10 file dan menghapus 10 file dalam lingkungan WSL2. Pembuatan file dapat menggunakan command touch file, sedangkan penghapusan file dapat menggunakan command rm file.

Gambar 4. Membuat file

Gambar 5. Menghapus file

d) Download Aplikasi

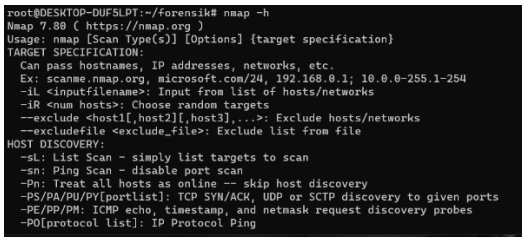
Melakukan skenario berupa download sebuah aplikasi pada WSL2 yaitu Nmap dengan commad sudo apt install nmap



Gambar 6. *Download* aplikasi nmap

e) Menjalankan Aplikasi

Selanjutnya menjalankan aplikasi Nmap yang telah di download aplikasi sebelumnya pada WSL2 dengan commad nmap -h



Gambar 7. Menjalankan aplikasi

f) Menutup WSL2

Langkah terakhir adalah menutup aplikasi WSL2 untuk selanjutnya di lakukan Examination.

B. Tahap Examination

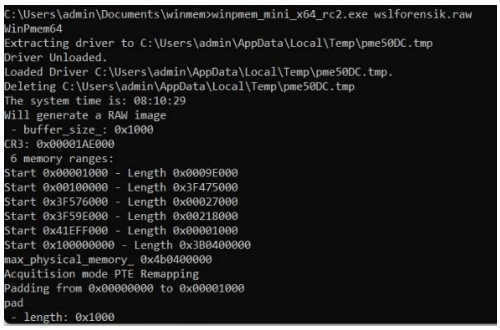
Setelah data memori dikumpulkan, tahap examination dimulai. Data tersebut dieksplorasi secara mendalam menggunakan alat analisis forensik, seperti hex editor. Pada tahap ini, fokus diberikan pada identifikasi dan pemahaman artefak memori yang mungkin

terkait dengan aktivitas yang terjadi pada WSL2. Informasi tentang proses WSL2, entri log, dan file yang terlibat dieksplorasi untuk mendapatkan pemahaman yang komprehensif.

Selain itu, tahap examination melibatkan analisis terhadap metadata file, catatan proses, dan jejak jaringan. Pemeriksaan metadata file memberikan wawasan tentang waktu pembuatan, modifikasi, dan akses terakhir ke file, sedangkan catatan proses memberikan informasi tentang aplikasi atau proses yang dijalankan. Jejak jaringan dicermati untuk melacak komunikasi yang mungkin terjadi selama pengujian.

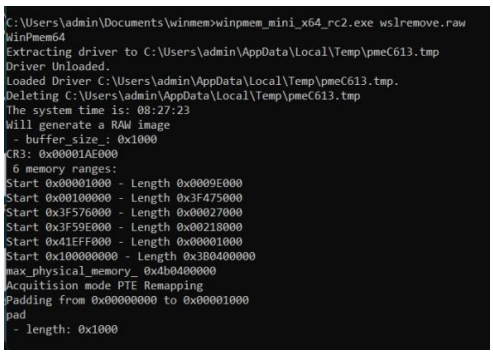
Tahap examination pada penelitian ini digunakan tools Winpmem. Examination dilakukan sebanyak 2 kali sesuai skenario yang dilakukan. Proses examination dapat dilihat pada 2 gambar dibawah ini.

Skenario 1:



Gambar 8. Akuisisi memori skenario 1

Skenario 2:



Gambar 9. Akuisisi memori skenario 2

Maka akan dihasilkan 2 file hasil examination dengan nama sesuai perintah diatas menggunakan ekstensi raw.

C. Tahap Analysis

Tahap analysis mencakup interpretasi dan pemahaman lebih lanjut terhadap data yang dikumpulkan. Data memori dievaluasi dengan menggunakan panduan dan standar forensik,

khususnya sesuai dengan metode NIST 800-86. Analisis ini melibatkan korelasi antara berbagai artefak untuk mengidentifikasi pola, hubungan kausal, atau tindakan yang mencurigakan.

Selama tahap ini, fokus diberikan pada melacak aktivitas pengguna, identifikasi potensial tindakan yang melanggar kebijakan atau mencurigakan, dan menentukan dampak dari aktivitas tersebut pada keamanan sistem. Analisis juga mencakup pengeksplorasi keberadaan malware atau aktivitas aneh yang dapat membahayakan integritas sistem.

Tahap ini menggunakan alat HxD untuk melakukan analisis terhadap file hasil examination yang telah dilakukan sebelumnya menggunakan Winpmem yaitu file wslforensik.raw. Berikut hasil analisis berdasrakan skenario yang dilakukan:

1) Skenario 1

   Skenario 1 dilakukan dengan tahapan menjalankan skenario berupa pembuatan file, penghapusan file dan menjalankan aplikasi Nmap yang telah dijelaskan pada tahapan Collecting. Namun pada skenario tahap examination dilakukan tanpa menghapus WSL2. Hasil yang didapatkan adalah semua command dan isi dalam file dapat didapatkan. Bukti hasil analysis akan dijelaskan pada tahap reporting.

2) Skenario 2

   Skenario 2 dilakukan dengan tahapan menjalankan skenario berupa pembuatan file, penghapusan file dan menjalankan aplikasi Nmap yang telah dijelaskan pada tahapan Collecting. Namun pada skenario tahap examination dilakukan setelah menghapus WSL2.

   Hasil yang didapatkan adalah tidak semua command skenario yang dijalankan didapatkan, hanya 2 operasi file yang didapatkan yaitu touch file5 dan touch file7. Bukti hasil analysis akan dijelaskan pada tahap reporting.

   Berikut dijelaskan Tabel perbedaan hasil analisis skenario 1 dan skenario 2.

Tabel 3. Hasil akuisisi memori

Tindakan	Skenario 1	Skenario 2
Pembuatan 10 file	Didapatkan seluruhnya	Didapatkan 2 file
Penghapusan 10 file	Didapatkan seluruhnya	Tidak didapatkan
Install Nmap	Didapatkan	Tidak didapatkan
Menjalankan Nmap	Didapatkan	Tidak didapatkan

KESIMPULAN

Dalam penelitian ini, telah dilakukan analisis memori forensik pada Hyper-V Berbasis Windows Subsystem For Linux 2 (WSL2) berdasarkan Metode Nist 800-86. Proses analisis memori forensik dilakukan pada sistem operasi Ubuntu yang digunakan di WSL2. Dengan menggunakan percobaan melakukan pembuatan 10 file, penghapusan 10 file, install aplikasi Nmap dan menjalankan aplikasi Nmap. Percobaan ini menggunakan 2 skenario dimana proses examination dilakukan dengan penghapusan WSL2 dan tanpa penghapusan WSL2. Proses examination digunakan tools Winpmem sedangkan proses analisis menggunakan HxD editor.

Hasil percobaan didapatkan pada skenario 1 dimana tanpa melakukan penghapusan WSL2 didapatkan seluruh artefak percobaan atau dapat dikatakan artefak ditemukan sebesar 100%, sedangkan pada skenario 2 dengan menghapus WSL2 didapatkan hanya 2 artefak percobaan yang ditemukan atau sebesar 16.7%. Penelitian ini bertujuan untuk memberikan wawasan mendalam terhadap analisis forensik pada WSL2, memberikan panduan praktis bagi ahli forensik digital dalam mengatasi tantangan keamanan yang terus berkembang seiring evolusi teknologi, dan melengkapi pemahaman kita tentang insiden keamanan yang melibatkan perpaduan sistem operasi Windows dan Linux di era WSL2.

DAFTAR REFERENSI

Craig Loewen. What is Windows Subsystem for Linux. 2023. https://docs.microsoft.com/en-us/windows/wsl/about

M. Juhendajad, S. Mamdouh, K. Msc, and S. Medri, “Windows 11 liidese Windows Subsystem for Linux kriminalistiline analüüs.”

Lewis, A. Case, A. Ali-Gombe, and G. G. Richard, “Memory forensics and the windows subsystem for linux,” in Proceedings of the Digital Forensic Research Conference, DFRWS 2018 USA, Digital Forensic Research Workshop, 2018, pp. S3–S11. doi: 10.1016/j.diin.2018.04.018.

P. Boigner and R. Luh, “WSL2 Forensics: Detection, Analysis & Revirtualization,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Aug. 2022. doi: 10.1145/3538969.3544439.

M. Parekh and S. Jani, “Memory Forensic: Acquisition and Analysis of Memory and Its Tools Comparison,” International Journal of Engineering Technologies and Management Research, vol. 5, no. 2, pp. 90–95, Apr. 2020, doi: 10.29121/ijetmr.v5.i2.2018.618.

Gunawan, Indra, “Keamanan Data: Teori dan Implementasi”, CV Jejak. 2021. *National Institute of Standards and Technology.* (n.d.). NIST *Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response.*