https://doi.org/10.37817/ikraith-teknologi.v7i3
P-ISSN :2580-4308
E-ISSN :2654-8046

# Implementasi Kontrol Akses pada Folder 'System Volume Information' untuk Mencegah Kehilangan Berkas di Windows 10

**Nugroho Budhisantosa[1], Hendry Gunawan[2], Imam Sutanto[3], Ryan Putra Laksana[4], Alivia Yulfitri[5]**
[1, 2, 3, 4,5]Universitas Esa Unggul, Fakultas Ilmu Komputer, Indonesia

E-Mail: [1]Nugroho.budhisantosa@esaunggul.ac.id, [2]Hendry.gunawan@esaunggul.ac.id, [3]imam.sutanto@esaunggul.ac.id, [4]ryan.putra@esaunggul.ac.id, [5]alivia@esaunggul.ac.id

**ABSTRAK**

Penelitian ini menginvestigasi strategi komprehensif untuk memperkuat pertahanan sistem dan meningkatkan kemampuan pemulihan dalam konteks ancaman hilangnya file secara tidak sengaja. Studi ini mengeksplorasi kemanjuran titik pemulihan otomatis, konfigurasi Access Control Lists (ACL), dan pengujian sistematis terhadap metode penghapusan berkas. Temuan menunjukkan bahwa integrasi titik pemulihan otomatis dan konfigurasi ACL yang ketat secara signifikan meningkatkan praktik keamanan dari sistem operasi. Penelitian ini memberikan wawasan berharga bagi organisasi dan individu yang mencari tindakan proaktif melawan berbagai ancaman kehilangan berkas yang terus berkembang.

**Kata kunci: pertahanan sistem, konfigurasi acl, sistem operasi**

***ABSTRACT***

*This research investigates comprehensive strategies to fortify system defenses and enhance recovery capabilities in the context of accidentally and intentionally losing file threats. The study explores the efficacy of automated restore points, Access Control Lists (ACL) configurations, and systematic testing against file deletion methods. Findings suggest that the integration of automated restore points and stringent ACL configurations significantly improves operating system security practices. The research contributes valuable insights for organizations and individuals seeking proactive measures against evolving losing file threats.*

***Keyword: defense system, ACL configuration, operating system***

## 1. PENDAHULUAN

Dalam lanskap digital terkini, kehilangan berkas kerja komputer adalah ancaman terhadap keamanan dan integritas sistem komputer. Potensi kerugian yang diakibatkan oleh kehilangan berkas kerja memerlukan strategi proaktif dan inovatif untuk memperkuat kemampuan sistem operasi pada pemulihan berkas kerja yang terhapus. Studi ini menggali pendekatan dari banyak segi yang bertujuan untuk mengamankan dan memulihkan bukan saja berkas-berkas komputer tetapi juga komponen sistem operasi yang penting, dengan fokus pada snapshot titik pemulihan atau restore point, konfigurasi Daftar Kontrol Akses atau Access Control List (ACL) secara tepat, dan pengujian

P-ISSN :2580-4308
E-ISSN :2654-8046
https://doi.org/10.37817/ikraith-teknologi.v7i3

komprehensif terhadap beragam cara penghapusan berkas kerja.

Penelitian ini berupaya untuk mengatasi lanskap ancaman kehilangan berkas kerja melalui tindakan pencegahan strategis. Metodologi yang dipilih melibatkan kontrol atas akses administrator ke folder "System Volume Information", dan pengujian menggunakan berbagai cara penghapusan berkas kerja.

Penerapan Access Control List pada direktori “System Volume Information“ bertujuan untuk membatasi akses administrator, memberikan keseimbangan antara keamanan dan fungsi administratif. Pengujian penghapusan berkas kerja yang meniru skenario di dunia nyata memberikan evaluasi pragmatis terhadap ketahanan sistem.

Penelitian ini tidak hanya bertujuan untuk berkontribusi pada bidang keamanan komputer yang terus berkembang namun juga berupaya menawarkan wawasan praktis bagi administrator sistem dan praktisi keamanan. Dengan menggabungkan landasan teoritis dan pengujian langsung, penelitian ini berupaya memberikan pemahaman yang berbeda tentang efektivitas langkah-langkah keamanan yang diusulkan. Melalui analisis terhadap metodologi yang dipilih, penelitian ini bertujuan untuk mengungkap potensi kerentanan, mengusulkan peningkatan, dan berkontribusi pada wacana yang sedang berlangsung seputar pertahanan keberadaan berkas kerja dan pemulihan sistem.

Dalam lanskap keamanan sistem operasi, kehilangan berkas kerja dapat menjadi ancaman tersendiri yang dapat menyebabkan kerugian finansial, dan gangguan pada layanan penting.

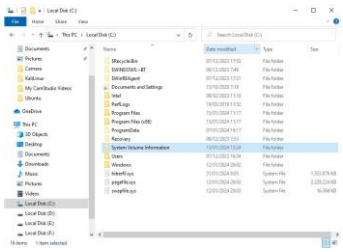
Kasus kehilangan berkas kerja umumnya paling banyak disebabkan oleh kegagalan logis, yaitu suatu keadaan dimana sistem operasi gagal untuk mengenali sistem file, baik disk, partisi atau karena sistem operasi yang rusak. Kasus umum penyebab kehilangan berkas kerja juga kerap terjadi akibat kesalahan penghapusan berkas kerja yang dilakukan secara tidak sengaja dari media penyimpanan dan dari recycle bin.

Studi latar belakang ini bertujuan untuk mengeksplorasi dan mengatasi tantangan ancaman kehilangan berkas kerja dalam konteks pemulihan sistem melalui pembuatan restore point, konfigurasi Access Control List (ACL), dan pengujian komprehensif terhadap penghapusan berkas kerja. Dengan memahami lanskap ancaman secara komprehensif, mengkaji mekanisme pertahanan yang ada, dan mengusulkan pendekatan beragam segi, penelitian ini bertujuan untuk memberikan kontribusi wawasan terhadap wacana yang sedang berlangsung mengenai strategi pertahanan berkas kerja pada komputer.

## 2. LANDASAN TEORI

### Volume Shadow Copy Service (VSS)

VSS merupakan layanan yang memungkinkan windows untuk membuat cadangan otomatis dan manual, atau snapshot dari kondisi saat ini dari file-file pada hard drive [1]. Layanan ini memfasilitasi pembuatan titik pemulihan, menyediakan mekanisme penting untuk pemulihan sistem. Memahami VSS sangat penting karena merupakan tulang punggung proses pembuatan titik pemulihan otomatis, memastikan ketersediaan snapshot yang konsisten dan andal.



Gambar 1. VSS disimpan di dalam direktori System Volume Information.

### Access Control Lists (ACL)

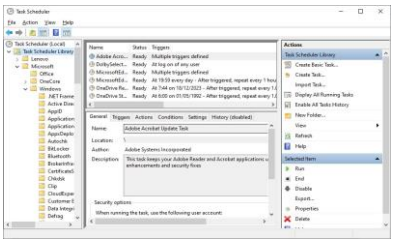
ACL adalah tabel yang memberitahu sistem operasi computer, hak akses apa saja yang dimilki setiap user ke suatu objek tertentu dari sebuah sistem. Misalnya berupa direktori, file atau layanan protocol yang lain. ACL pada sistem operasi Windows 10 terdiri dari kumpulan Access Control Entries (ACEs) dimana setiap ACE menentukan hak akses yang diperbolehkan, ditolak, atau diaudit untuk pengguna yang tercantum dalam

https://doi.org/10.37817/ikraith-teknologi.v7i3
P-ISSN :2580-4308
E-ISSN :2654-8046

entri [2]. Konfigurasi ACL yang cermat pada direktori penting, seperti "System Volume Information", memastikan bahwa hanya entitas yang berwenang, khususnya administrator, yang memiliki hak akses yang diperlukan, sehingga meningkatkan postur keamanan.

**Task Scheduler pada Windows 10**

Task Scheduler adalah komponen dari Microsoft Windows yang menyediakan kemampuan untuk menjadwalkan menjalankan program atau *script* padawaktu yang telah ditentukan atau setelah interval waktu tertentu [3]. Task Scheduler adalah alat penting untuk menjadwalkan pembuatan titik pemulihan otomatis. Task Scheduler berfungsi sebagai orkestrator untuk pembuatan titik pemulihan yang tepat waktu dan konsisten, selaras dengan keseluruhan strategi perlindungan sistem proaktif.



Gambar 2. Jendela Task Scheduler pada sistem operasi Microsoft Windows 10.

**Command Prompt**

*Command Prompt* merupakan baris perintah pada aplikasi yang tersedia untuk sistem operasi Windows yang digunakan untuk menjalankan perintah ataupun masukan [4]. Dalam lingkungan ini, pengguna dapat menjalankan perintah-perintah sistem untuk melakukan berbagai tugas administratif, konfigurasi, dan troubleshooting. Command Prompt memberikan kontrol langsung terhadap banyak aspek sistem operasi, memungkinkan pengguna untuk mengelola file, folder, dan tugas administratif lainnya. Command Prompt adalah shell yang dapat digunakan untuk menyelesaikan masalah sistem dimana pengguna dapat menggunakan perintah untuk memeriksa koneksi jaringan, menemukan dan memperbaiki kesalahan file, serta mengelola proses dan layanan. Command Prompt juga dapat memfasilitasi pembuatan automatisasi Batch Script yaitu kemampuan untuk membuat dan menjalankan Batch Script secara otomatis untuk menjalankan serangkaian perintah, memudahkan otomatisasi tugas-tugas rutin.

## 3. METODOLOGI

Penelitian ini menggunakan metodologi yang sistematis untuk secara komprehensif mengatasi tantangan kehilangan berkas kerja komputer dan meningkatkan ketahanan sistem. Metodologi ini disusun dalam beberapa fase berbeda, yang masing-masing berkontribusi terhadap tujuan menyeluruh dalam menciptakan strategi pertahanan dan pemulihan yang kuat.

a. Literature Review
   Tahapan ini dimaksudkan untuk mengevaluasi literatur yang terkait dengan strategi pemulihan sistem dan mekanisme keamanan, guna memberikan landasan teoritis bagi penelitian ini [5]. Pendekatan yang digunakan adalah melakukan eksplorasi terhadap artikel ilmiah, buku, dan publikasi yang relevan untuk memperoleh pemahaman mendalam tentang lanskap kehilangan berkas kerja dan tindakan penanggulangan yang efektif.
b. Theoretical Framework Development
   Tahapan ini bertujuan untuk membangun kerangka teoritis yang mengintegrasikan konsep-konsep utama seperti VSS, ACL, Task Scheduler, dan skrip PowerShell [6]. Pendekatan yang digunakan adalah

mensintesis informasi dari tinjauan literatur untuk membangun landasan teori yang komprehensif, selaras dengan tujuan penelitian.

c. System Configuration
Tahapan ini bertujuan untuk mengkonfigurasi lingkungan pengujian dengan sistem Windows 10, menerapkan pembuatan titik pemulihan otomatis, pengaturan ACL, dan langkah-langkah keamanan yang relevan [7]. Pendekatan yang digunakan adalah menyiapkan lingkungan terkendali yang mencerminkan skenario dunia nyata, memastikan representasi komponen sistem dan konfigurasi keamanan yang akurat

d. Implementasi Task Scheduler
Tahapan ini bertujuan untuk menjadwalkan tugas secara otomatis untuk pembuatan titik pemulihan pada interval tertentu menggunakan Task Scheduler [8]. Pendekatan yang digunakan adalah memanfaatkan Task Scheduler untuk membuat tugas berulang untuk pembuatan titik pemulihan otomatis, memastikan konsistensi dan ketepatan waktu.

e. ACL Configuration
Tahapan ini bertujuan untuk mengkonfigurasi Access Control List untuk folder "System Volume Information", menghapus akses administrator ke izin Full Control, dan Modify [9]. Pendekatan yang digunakan adalah menerapkan pengaturan ACL yang tepat menggunakan fitur keamanan Windows untuk meningkatkan keamanan direktori penting.

f. Pengujian Hapus Berkas
Tahapan ini bertujuan untuk mengevaluasi efektivitas strategi yang diterapkan dengan menjadikan folder "System Volume Information" menjadi target penghapusan. Pendekatan yang digunakan adalah melakukan skenario pengujian terkontrol, mengamati respons sistem, dan menilai kemampuan menahan simulasi penghapusan berkas.

g. Analisis Data
Tahap ini bertujuan untuk menganalisis hasil tahap pengujian dan menarik kesimpulan mengenai efektivitas strategi yang diterapkan [10]. Pendekatan yang digunakan adalah secara sistematis menganalisis data yang dikumpulkan selama pengujian, membandingkan perilaku sistem dengan tolok ukur yang telah ditentukan, dan mengevaluasi keberhasilan strategi pemulihan.

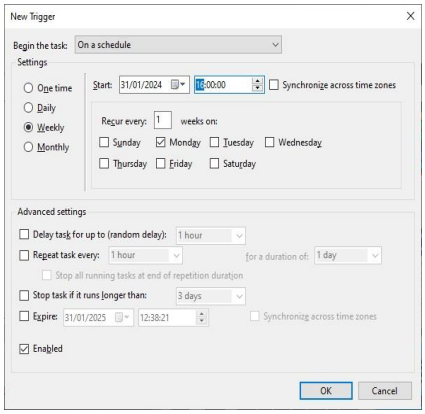
h. Temuan dan Rekomendasi

Tahap ini bertujuan untuk menyajikan temuan penelitian dan memberikan rekomendasi untuk meningkatkan kemampuan pertahanan dan pemulihan sistem [11]. Pendekatan yang digunakan adalah meringkas temuan-temuan utama, menarik kesimpulan berdasarkan analisis data, dan mengusulkan rekomendasi untuk meningkatkan postur keamanan secara keseluruhan.

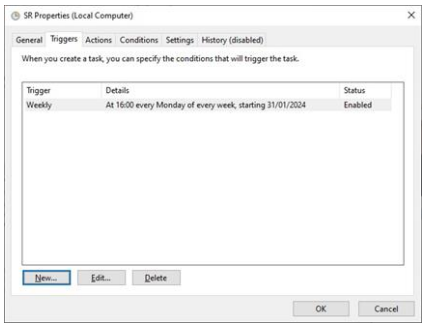
## 4. HASIL DAN PEMBAHASAN

Pembuatan titik pemulihan otomatis pada interval terjadwal menunjukkan efektivitasnya dalam memelihara snapshot sistem. Strategi ini memastikan bahwa sistem memiliki titik pemulihan terkini, memungkinkan pengguna untuk kembali ke kondisi stabil jika terjadi masalah kehilangan berkas kerja.

https://doi.org/10.37817/ikraith-teknologi.v7i3
P-ISSN :2580-4308
E-ISSN :2654-8046

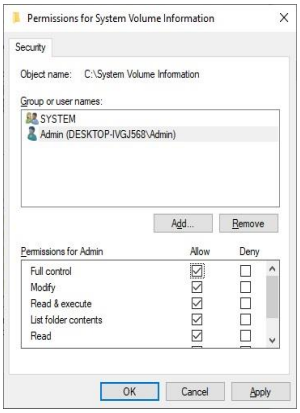



Gambar 3. penjadwalan pembuatan restore point secara mingguan

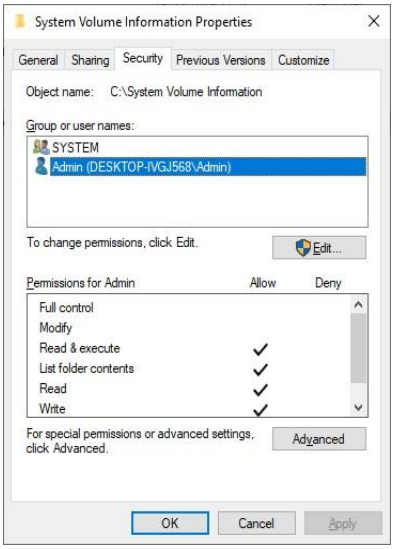



Gambar 4. tampilan informasi penjadwalan pembuatan restore point setiap hari Senin jam 16:00.

Konfigurasi ACL untuk folder "System Volume Information" berhasil membatasi akses administrator.




Gambar 5. konfigurasi default dari ACL pada direktori System Volume Information dari sistem operasi Windows 10.

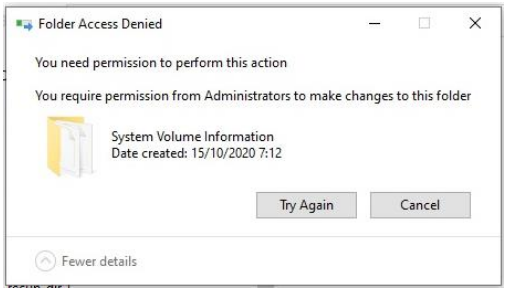



Gambar 6. konfigurasi ACL dengan menghapus ijin Full control, dan Modify.

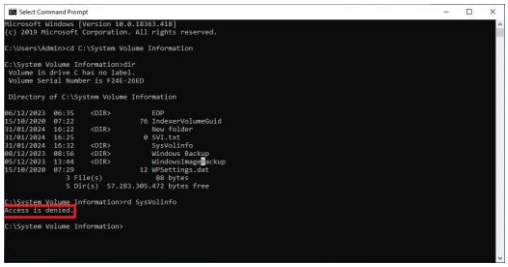
Akses terbatas ini meningkatkan keamanan direktori penting, mengurangi risiko perubahan direktori “System Volume Information” bukan saja secara tidak sengaja tetapi juga jika dilakukan secara sengaja.

Pada pengujian penghapusan file, sistem ini menunjukkan ketahanan berkas terhadap penghapusan berkas secara normal dan secara paksa. Pengujian terkontrol memvalidasi kemampuan sistem untuk menahan skenario kehilangan berkas komputer di dunia nyata, menyoroti pentingnya strategi pertahanan proaktif.

P-ISSN :2580-4308
E-ISSN :2654-8046
https://doi.org/10.37817/ikraith-teknologi.v7i3



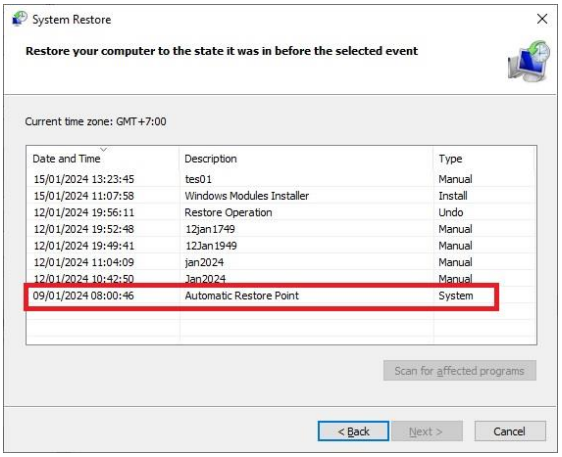

Gambar 7. tampilan layar pesan dari upaya penghapusan direktori System Volume Information menggunakan Graphical User Interface ketika ijin Full control, dan Modify dihilangkan



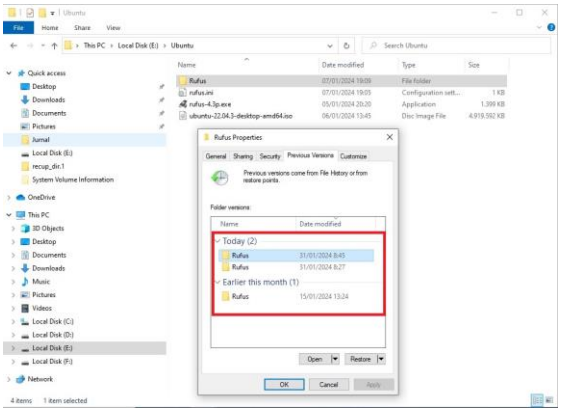
Gambar 8. tampilan layar pesan dari upaya penghapusan direktori System Volume Information menggunakan Command Prompt ketika ijin Full control, dan Modify dihilangkan

Task Scheduler menunjukkan performa yang andal dalam menjalankan tugas otomatis untuk pembuatan titik pemulihan. Fungsi Task Scheduler yang konsisten memastikan pembuatan titik pemulihan secara sistematis, yang merupakan aspek fundamental dari strategi pertahanan secara keseluruhan.

Kombinasi Restore Point otomatis, konfigurasi ACL, dan pengujian rutin berkontribusi terhadap ketahanan sistem. Dengan konfigurasi yang tepat pada Restore Point dan Task Scheduler pemulihan dapat dilakukan bukan saja pada konfigurasi sistem operasi juga pada pemulihan berkas kerja yang dapat disesuaikan dengan kebutuhan.




Gambar 9. restore point yang dibuat oleh sistem secara otomatis.



Gambar 10. restore point untuk kustomisasi pemulihan berkas kerja

Pendekatan holistik, mengintegrasikan berbagai strategi, meningkatkan kemampuan sistem untuk pencegahan kehilangan berkas sistem dan berkas kerja komputer.

Penelitian menunjukkan bahwa mengintegrasikan titik pemulihan otomatis dan konfigurasi ACL yang ketat dapat mendukung praktik keamanan sistem operasi. Organisasi dan individu dapat mengadopsi strategi serupa untuk membentengi sistem mereka terhadap ancaman ransomware, dengan menekankan pentingnya tindakan proaktif.

## 5. KESIMPULAN

Penelitian ini melakukan eksplorasi strategi yang komprehensif untuk memperkuat pertahanan sistem dan meningkatkan kemampuan pemulihan dalam menghadapi ancaman kehilangan berkas komputer. Temuan-temuan utama dan wawasan yang diambil dari penelitian ini berkontribusi signifikan terhadap wacana praktik keamanan sistem operasi dan langkah-langkah proaktif.

## 6. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada institusi (Universitas Nusa Putra, Universitas Muhammadiyah, dan Universitas Esa Unggul) yang telah memberi dukungan ber-kolaborasi dalam pelaksanaan pengabdian kepada masyarakat.

## DAFTAR PUSTAKA

[1] A. Ghafarian and E. D. Hills, "Forensic analysis of windows 10 volume shadow copy service," *IMCIC 2018 - 9th Int. Multi-Conference Complexity, Informatics Cybern. Proc.*, vol. 2, no. Imcic, pp. 47–52, 2018.

[2] P. Simanjuntak, C. E. Suharyanto, and Jamilah, "Analisis Penggunaan Access Control List ( Acl ) Dalam Jaringan Komputer Di Kawasan," *Isd*, vol. 2, no. 2, pp. 122–128, 2017.

[3] I. F. Al hadi, C. Chusna, S. Ilham, and A. C. Fauzan, "Implementasi Penjadwalan Round Robin pada Task Scheduler untuk Pembaruan Aplikasi Otomatis," *Ilk. J. Comput. Sci. Appl. Informatics*, vol. 1, no. 1, pp. 11–14, 2019, doi: 10.28926/ilkomnika.v1i1.7.

[4] T. Yusnanto and D. Lestiono, "Optimalisasi Penggunaan Cmd Dan Sysinternalsuits Sebagai Malware Detection," *J. Transform.*, vol. 15, no. 1, pp. 66–74, 2019.

[5] dr. Z. S. Ulhaq, "Panduan Penulisan Skripsi : Literatur Review," *J. Phys. A Math. Theor.*, vol. 44, no. 8, p. 32, 2018.

[6] "Summary of Theoretical Frameworks and Literature," no. 1928, p. 2013, 2013.

[7] P. Anderson, *What Is System Configuration?*, vol. 14. 2006. [Online]. Available: http://www.sage.org/pubs/14_sysconfig/%0Ahttps://www.usenix.org/lisa/books/system-configuration%0Ahttp://homepages.inf.ed.ac.uk/dcspaul/homepage/live/work/publications.html

[8] E. Åström, "Task Scheduling in Distributed Systems," 2016, [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1088396

[9] B. P. Guide, "Windows ACL Configuration," no. March, 2020.

[10] A. Abdul, "Teknik Analisis Data Analisis Data," *Tek. Anal. Data Anal. Data*, pp. 1–15, 2020.

[11] R. Salsabila and I. Wahyudi, "Pengaruh Temuan Audit, Rekomendasi Hasil Pemeriksaan, Dan Ukuran Pemerintahan Daerah Terhadap Opini Audit Pada Pemerintah Daerah Di Indonesia," *AKSELERASI J. Ilm. Nas.*, vol. 4, no. 1, pp. 38–45, 2022, doi: 10.54783/jin.v4i1.515.

[12] K Krianto Sulaiman dan Darjat Saripurna, "Network Security System Analysis Using Access Control List, (ACL)", International Journal of Information System & Technology, Vol. 5, No. 2, pp. 192-197, 2021

[13] Sudhakar Govindavajhala, and Andrew W. Appel, Windows Access Control Demystified,

Princeton University, January 2006

[14] William Mahoney, and James Harr, A Linux Implementation of Windows ACLs, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010

[15] Theo Lucia, What Is System Volume Information and How to Access/Delete It, https://recoverit.wondershare.com/harddrive-recovery/what-is-system-volume-information.html, diakses Januari 2024

[16] Kyle Heath, and Katherine Delude, Volume Shadow Copy Forensics Report, Champlain College, Patrick Leahy Center for Digital Investigation, March 2012

[17] ALJI Mohamed, and CHOUGDALI Khalid, Detection of Suspicious Timestamps in NTFS using Volume Shadow Copies, I. J. Computer Network and Information Security, 2021, 4, 62-69, April 2021

[18] IBM Release notes, IBM Storage Support for Microsoft Volume Shadow Copy Service and Virtual Disk Service Version 4.14.0, IBM Corporation, November 2017