PENERAPAN METODE NATIONAL INTITUTE OF JUSTICE DALAM PEMULIHAN DATA PADA FLASHDISK -1.pdf

by Isiah Eaton

Submission date: 20-Jan-2025 05:54AM (UTC-0800)

Submission ID: 2565258556

File name: PENERAPAN_METODE_NATIONAL_INTITUTE_OF_JUSTICE_DALAM_PEMULIHAN_DATA_PADA_FLASHDISK_-1.pdf (479.51K)

Word count: 2885

Character count: 18389

PENERAPAN METODE *NATIONAL INTITUTE OF JUSTICE* DALAM PEMULIHAN DATA PADA FLASHDISK

Andhika Dwi Surya Achmad Saputra *[1], Azmuri Wahyu Azinar [2], Irwan Alnarus Kautsar [3], Dr. Suprianto, S.Si. M.Si[4]
[1,2,3] Informatika, Universitas Muhammadiyah Sidoarjo, Jl. Mojopahit No.666 B, Sidowayah, Celep, Kec. Sidoarjo, Kabupaten Sidoarjo, Jawa Timur, 61215, Indonesia
e-mail: *[1]suryaandhika699@gmail.com,[2] azmuri@umsida.ac.id,[3] irwan@umsida.ac.id,[4] Suprianto@umsida.ac.id

Abstrak

Flashdisk adalah perangkat penyimpanan portabel berbasis memori flash yang digunakan untuk menyimpan, memindahkan, dan mencadangkan data. Meski praktis, perangkat ini rentan terhadap kejahatan digital, seperti pencurian data, penghapusan data tidak sah, dan penyalahgunaan informasi. Untuk mengatasi ancaman ini, metode pemulihan data yang efektif sangat diperlukan. Salah satu metode yang digunakan dalam forensik digital adalah metode dari *National Institute of Justice* (NIJ), yang mencakup tahapan persiapan, pengumpulan, identifikasi, pemeriksaan, analisis, dan pelaporan. Tujuan penelitian ini untuk menguji efektivitas metode NIJ dalam memulihkan data yang hilang dari *flashdisk*. Dengan menggunakan tools seperti FTK Imager, Autopsy, dan WinMd5, file yang dihapus melalui *Shift + delete* dan *quick* format berhasil dipulihkan. Meski nama file berubah, ekstensi, ukuran, dan nilai hash MD5 tetap sama seperti aslinya, menunjukkan file tidak dimodifikasi. Kesimpulannya, metode NIJ efektif memulihkan dan menganalisis bukti digital dari *flashdisk*.

Kata kunci : kejahatan siber, bukti digital, NIJ, digital forensik, flash disk, forensic tools.

Abstract

A flash drive is a portable storage device based on flash memory used for storing, transferring, and backing up data. While practical, it is vulnerable to digital crimes such as data theft, unauthorized data deletion, and information misuse. To address these threats, an effective data recovery method is essential. One method commonly used in digital forensics is the National Institute of Justice (NIJ) method, which includes preparation, collection, identification, examination, analysis, and reporting stages. This study evaluates the effectiveness of the NIJ method in recovering lost data from flash drives. Using tools such as FTK Imager, Autopsy, and WinMd5, files deleted through Shift + Delete and quick format were successfully recovered. Although file names changed, the file extensions, sizes, and MD5 hash values remained the same as the originals, indicating that the files were not modified. In conclusion, the NIJ method is effective in recovering and analyzing digital evidence from flash drives.

Keywords : *Cybercrime, digital evidence, NIJ, digital forensics, flash drives, forensic tools.*

1. PENDAHULUAN

Flashdisk adalah perangkat penyimpanan yang menggunakan teknologi memori flash untuk menyimpan dan mengakses data[1]. Dengan ukuran yang kecil dan portabilitas tinggi, flashdisk mudah digunakan karena dapat langsung terhubung ke port USB pada komputer atau perangkat lainnya. Flashdisk sering dimanfaatkan untuk menyimpan, memindahkan, dan mencadangkan berbagai jenis data, seperti dokumen, foto, musik, dan video. Kapasitas penyimpanannya beragam, mulai dari beberapa gigabyte hingga terabyte. Perkembangan teknologi informasi dan komunikasi telah memberi dampak positif pada kehidupan manusia, salah satunya dengan penggunaan flashdisk sebagai media penyimpanan digital. Namun, meningkatnya penggunaan *flashdisk*

juga membuka peluang kejahatan digital, seperti pencurian dan penyalahgunaan data[2]. Oleh karena itu, metode pemulihan data yang efektif sangat penting untuk menangani data yang hilang atau terhapus dari *flashdisk*[3]. Salah satu metode yang umum digunakan dalam forensik digital adalah metode dari *National Institute of Justice* (NIJ), pentingnya Metode NIJ dibanding dengan metode yang lain seperti NIST, *Static Forensics,* dan *GCFIM* adalah metode NIJ mempunyai tahapan - tahapan yang runtut dan terperinci, yang terdiri dari beberapa tahapan, yaitu persiapan, penanganan insiden, pengumpulan, identifikasi, pemeriksaan, analisis, dan pelaporan. Penelitian yang berjudul " Analisis forensic recovery pada *smartphone* android menggunakan metode National Institute Of Justice " imam riadi melakukan *recovery* data pesan, history panggilan, kontak, gambar, video dan file dokumen pada *smartphone* dengan metode NIJ degan bantuan 3 tool forensik yaitu *MOBILedit forensics*, *Wondershare dr. Fone for Android*, dan *Belkasoft Evidence Center*. Keterbaruan dari penelitian ini adalah merecovery file seperti Word, Excel, Pdf dan PPT, karena penelitian yang sudah ada hanya merecovery file gambar dan video. Dengan menerapkan metode NIJ, investigator dapat memulihkan data yang hilang atau sengaja dihapus dari perangkat USB. Penelitian ini bertujuan untuk mengevaluasi seberapa efektif metode NIJ dalam memulihkan data dari *flashdisk*[4],[5],[6].

2. METODE PENELITIAN

gambar 2 tahapan penelitian

Langkah-langkah penelitian yang terlihat pada Gambar 1 mencakup rangkaian proses yang dirancang secara sistematis untuk dilaksanakan. Berikut ini adalah tahapan-tahapan penelitian tersebut.

1. Identifikasi Masalah

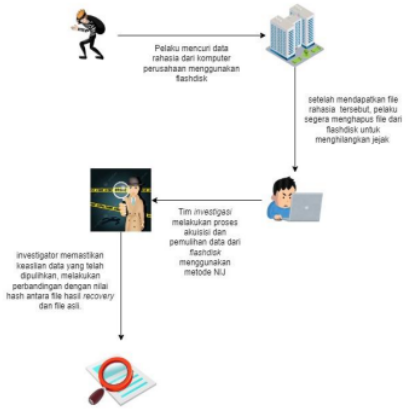
Perkembangan teknologi informasi dan komunikasi telah memberikan manfaat yang signifikan dalam kehidupan manusia. salah satunya melalui penggunaan flashdisk sebagai media penyimpanan data digital. Meningkatnya penggunaan flashdisk, potensi kejahatan digital seperti pencurian data dan penyalahgunaan data akan terjadi. Oleh karena itu, penting untuk memiliki metode pemulihan data yang efektif untuk menangani data yang hilang atau terhapus dari flashdisk

2. Studi Literatur

Pada tahap ini, dilakukan tinjauan literatur dengan mengumpulkan informasi dari berbagai penelitian sebelumnya terkait forensik digital sebagai referensi dari berbagai sumber. Temuan dari kajian tersebut dijadikan sebagai landasan untuk merencanakan atau merancang skenario dalam penelitian ini.[7],[8],[9],[10].

3. Pembuatan Skenario

Pemilihan skenario kasus kejahatan siber berhubungan dengan salah satu bentuk pelanggaran terhadap pencurian data. Dalam skenario ini, pelaku mencuri data sensitif milik perusahaan dengan tujuan mendapatkan



gambar 1 skenario kasus

keuntungan pribadi, seperti yang ditampilkan pada Gambar 2.
Secara lebih spesifik, tahapan-tahapan dalam skenario ini adalah sebagai berikut.

- pelaku dengan sengaja mengambil data pada komputer target dengan *credential* yang ilegal dan *previlege* yang tidak benar.
- Setelah itu, pelaku mengambil semua data penting Perusahaan dengan copy paste ke flashdisk milik pelaku. Ada 4 file, bentuknya PDF, Word, Excel dan PPT.
- Lalu pelaku Menghilangkan semua data yang tersimpan di dalam flashdisk. dengan *Shift + delete* dan *quick format* untuk menghilangkan jejak.
- Tim *investigasi* melakukan proses akuisisi dan pemulihan data dari *flashdisk* dengan metode NIJ
- Selanjutnya investigator memastikan keaslian data yang telah dipulihkan, melakukan perbandingan dengan nilai hash antara file hasil *recovery* dan file asli.

4. Penerapan Metode NIJ

Penelitian ini menggunakan metode forensik yang dikembangkan oleh *National Institute of Justice* (NIJ), yang terstruktur dalam lima tahap utama, yaitu identifikasi, pengumpulan, pemeriksaan, analisis, dan pelaporan[11],[12]. sebagaimana ditunjukkan pada gambar 3 Metode ini dirancang untuk memastikan setiap langkah dalam investigasi forensik dilakukan secara sistematis, mulai dari identifikasi barang bukti hingga pelaporan hasil akhir dengan tujuan menjaga keutuhan data dan validitas temuan.

gambar 3 metode NIJ

A. Identification

Tahap identifikasi adalah langkah awal dalam proses akuisisi data, yang bertujuan mengumpulkan informasi relevan untuk memahami objek atau kasus yang diteliti. Dalam penelitian ini, pihak berwenang akan melakukan investigasi awal untuk mengidentifikasi secara mendalam kejadian yang terjadi, termasuk motif pelaku dan dampak terhadap korban. Selanjutnya, seluruh barang bukti yang relevan akan dikumpulkan dan disimpan sesuai prosedur guna menjaga integritas dan keasliannya.

B. Collection

Tahap pengumpulan melibatkan pengambilan barang bukti dari berbagai sumber yang terkait dengan kasus yang diselidiki, disertai dokumentasi dan identifikasi jenis atau merek barang bukti untuk pelabelan. Dalam penelitian ini, pihak berwenang menemukan sebuah flashdisk berwarna biru bermerek Toshiba. Perangkat penyimpanan tersebut berfungsi dengan baik, tetapi dalam kondisi terformat tanpa file apa pun.

C. Examination

Tahap ini merupakan proses verifikasi data forensik yang dilakukan dengan membandingkan data yang diperoleh di lokasi kejadian dengan data yang tersimpan dalam file digital. Tujuannya adalah memastikan tidak ada manipulasi data dan menjamin keakuratan data yang digunakan dalam penyelidikan. Pada tahap ini, data dari bukti fisik berupa flashdisk akan dicari, dianalisis, dan diproses menggunakan tiga software, yaitu FTK Imager, Autopsy, dan WinMd5.

D. Analysis

Setelah melewati tahap verifikasi dan memastikan keaslian data, analisis mendalam dilakukan menggunakan metode yang diakui secara ilmiah dan legal. Langkah ini bertujuan untuk mengungkap informasi penting yang dapat dijadikan bukti kuat dalam kasus yang diselidiki. Hasil dari proses ini menunjukkan bahwa file atau data yang telah dihapus oleh pelaku berhasil direcovery. Data tersebut terdiri dari 4 file dalam berbagai format, termasuk PDF, Word, Excel, dan PPT.

E. Reporting

Setelah data digital dianalisis, langkah berikutnya adalah menyusun laporan terperinci yang mencakup seluruh tahapan investigasi, mulai dari pemilihan alat dan metode hingga hasil akhir yang diperoleh. Laporan ini bertujuan memberikan gambaran menyeluruh tentang proses forensik digital yang telah dilakukan. Dalam penelitian ini, seluruh tahapan

analisis telah selesai, dan informasi yang diperoleh akan disusun dalam laporan. Laporan tersebut akan menjadi dasar utama untuk menyampaikan fakta-fakta di persidangan.

5. Kesimpulan

Kesimpulan penelitian ditarik berdasarkan analisis bukti digital yang diperoleh dari barang bukti dalam skenario yang telah dirancang. Analisis ini dilakukan dengan memanfaatkan perangkat forensik serta menerapkan metode dari *National Institute of Justice*.

3. HASIL DAN PEMBAHASAN

Dalam sejumlah penelitian, pemulihan data yang hilang melalui proses diseksi sering kali Bisa diselesaikan dalam durasi yang cukup cepat, seperti dalam hitungan menit atau jam, terutama jika data yang perlu dipulihkan relatif sederhana atau mudah diakses. Namun, dalam kasus-kasus yang lebih kompleks, seperti data yang terfragmentasi, rusak parah, atau tersimpan dalam perangkat dengan enkripsi atau kerusakan fisik, proses pemulihan dapat membutuhkan waktu yang lebih panjang. Dalam situasi seperti ini, waktu yang dibutuhkan bisa mencapai beberapa hari, minggu, atau bahkan lebih lama, tergantung pada kompleksitas data dan kondisi perangkat penyimpanan. Untuk mendukung proses analisis forensik secara lebih efektif, penggunaan alat khusus menjadi penting. Alat-alat tersebut mencakup perangkat keras dan perangkat lunak forensik, yang dirancang untuk membantu pemeriksa forensik dalam menyelesaikan proses pemulihan dan analisis data dengan lebih efisien. Perangkat-perangkat ini tercantum dalam tabel 1 berikut, yang memberikan gambaran umum mengenai jenis alat yang biasa digunakan dalam praktik forensik data.

tabel 1 alat dan software

No	Alat dan Software	Deskripsi
1.	Laptop Lenovo	Windows 11, 64 bit, 8gb RAM
2.	Flashdisk Thosiba	Objek penelitian
3.	FTK Imager (https://accessdata-ftk-imager.software.informer.com/3.2/)	Tools Forensik
4.	Autopsy (https://www.autopsy.com/download/)	Tools Forensik
5.	WinMd5 (https://www.winmd5.com/)	Tools Forensik

A. Identification

Tahapan identifikasi pada kasus investigasi forensik digital meliputi proses pengumpulan informasi awal untuk menentukan sumber bukti digital yang relevan, mengidentifikasi perangkat atau media penyimpanan yang terkait dengan kasus. Tahapan identifikasi dalam penelitian ini adalah sebagai berikut :

- Menentukan jenis kasus yang sedang diinvestigasi
- Mengumpulkan informasi awal terkait kejadian, termasuk laporan insiden dan kronologi
- Mengidentifikasi perangkat fisik yang berpotensi menyimpan bukti

B. Collection

Melakukan proses pengambilan barang bukti dari berbagai sumber Yang berkaitan dengan perkara yang tengah diselidiki dan melakukan dokumentasi serta memeriksa jenis atau merk dari barang bukti guna dilakukan pelabelan barang bukti.

gambar 4 barang bukti

Dalam penelitian ini, pihak berwenang menemukan barang bukti berupa flashdisk berwarna biru bermerek Toshiba, seperti ditampilkan pada Gambar 4 Perangkat penyimpanan tersebut berfungsi dengan baik, namun dalam kondisi terformat atau kosong tanpa file apa pun.

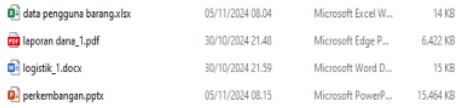
tabel 2 spesifikasi barang bukti

Bukti digital	Size	keterangan
Flashdisk (Thosiba)	8 giga byte	Barang bukti

C. Examination

Analisis hasil tahap akuisisi dilakukan untuk mendapatkan data yang diharapkan sebagai bukti digital. Proses ini bertujuan untuk menelusuri rekam jejak digital berupa file yang tersimpan di flashdisk. Tahap ini memerlukan waktu karena melibatkan penggalian terhadap seluruh data yang pernah tercatat sebelumnya. Dengan bantuan tiga perangkat lunak, yaitu *FTK Imager*, *Autopsy,* dan *WinMd5*, pencarian serta analisis data dari bukti fisik pada flashdisk akan dilakukan.

Kita asumsikan bahwa 4 file yang telah dicuri oleh pelaku adalah sebagai berikut :



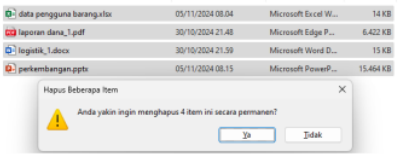
gambar 5 file percobaan

Kemudian, nilai hash dari setiap file diperiksa menggunakan tools *WinMd5*. Pemeriksaan nilai hash ini bertujuan untuk memastikan apakah hasil pemulihan data nantinya akurat atau tidak.

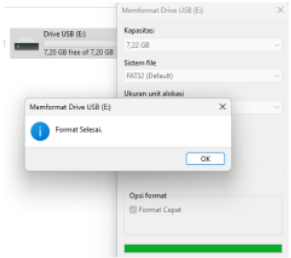
tabel 3 nilai hash sebelum analisis

No	File	Hasil sebelum analisis
1.	Data pengguna barang.xls	703ac897869 4a6ad23fef1b92fa2b34 4
2.	Laporan dana_1.pdf	f1847951a327be7f0ec7 b3d39c632a60
3.	Logistik_1.docx	bf5b76ff01a6c7152706 3ba71d409cdf
4.	Perkembangan.pptx	a70dfaf10b42bf511670 422713b4e77f

Berdasarkan skenario dalam penelitian ini, semua file yang terdapat di flashdisk akan dihapus menggunakan kombinasi *Shift* + *Delete*, kemudian dilakukan *quick format* seperti yang ditunjukkan pada gambar 6 di bawah ini.



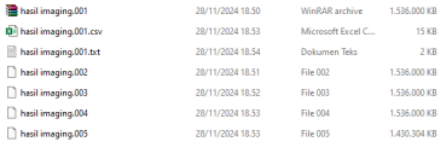
gambar 6 file dilakukan shift + delete



gambar 7 flashdisk di format

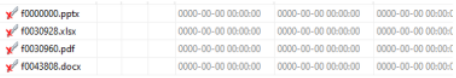
setelah flashdisk berada dalam kondisi kosong, dilakukan proses imaging terhadap barang bukti berupa flashdisk menggunakan tools *FTK Imager* dan *Autopsy*.

Gambar 8 menunjukkan partisi yang dihasilkan dari proses imaging menggunakan tools FTK Imager.



gambar 8 hasil imaging

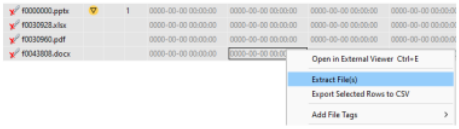
Setelah proses imaging selesai, langkah selanjutnya adalah melakukan akuisisi menggunakan tools *Autopsy*. Gambar 9 menunjukkan partisi yang dihasilkan dari proses akuisisi menggunakan Autopsy tersebut.



gambar 9 hasil akuisisi

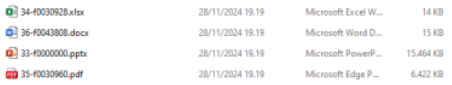
D. **Analysis**

Pada tahap analisis dilakukan pengambilan data dari hasil *examinasi*. Hal ini dapat dilakukan dengan menggunakan pencarian manual, yaitu pencarian berdasarkan jenis file. Pada tahap ini proses yang dilakukan telah membuahkan hasil yaitu ter-*recovery* nya file atau data yang telah di hapus oleh pelaku. Data tersbeut terdiri dari berbagai macam yaitu 4 file *PDF*, *Word, Excel dan PPT*. Selanjutnya, data yang telah melalui proses imaging diambil untuk dilakukan pemeriksaan nilai hash, seperti ditampilkan pada gambar 10.



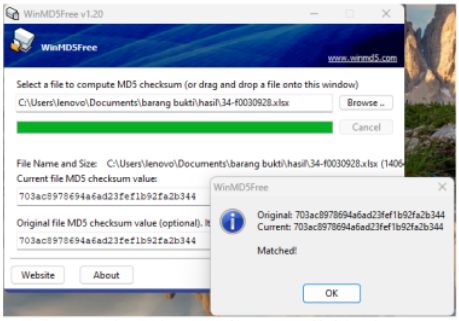
gambar 10 Extrak File

Semua file telah diekstrak ke dalam computer



gambar 11 File yang berhasil di recovery

akan diperiksa nilai hash-nya satu per satu menggunakan tools *WinMd5* seperti yang terlihat pada gambar di bawah ini.



gambar 12 Pemerikasaan nilai hash

Hasil validasi nilai hash untuk semua file menggunakan tools *WinMd5* menunjukkan kecocokan dengan file aslinya, yang dapat dilihat pada tabel 3.4

tabel 4 nilai hash

file	Hasil sesudah analisis	Validasi
Data pengguna barang.xls	703ac897869 4a6ad23fef1b92fa2b344	Cocok
Laporan dana_1.pdf	f1847951a327be7f0ec7b3d39c632a60	Cocok
Logistik_1.docx	bf5b76ff01a6c71527063ba71d409cdf	Cocok
Perkembangan.pptx	a70dfaf10b42bf511670422713b4e77f	Cocok

E. **Reporting**

Berdasarkan hasil analisis yang telah dilakukan, ditemukan file-file yang dihapus oleh pelaku pada media penyimpanan flash disk menggunakan tools forensik *FTK Imager*, *Autopsy,* dan *WinMd5*. Setelah dilakukan pemulihan dengan metode *Shift + delete* dan *quick format*, nama file yang terhapus berubah menjadi nama yang berbeda dari aslinya. Selain itu, ukuran dan nilai hash MD5 dari semua file tidak menunjukkan perubahan, yang mengindikasikan bahwa file-file tersebut tidak mengalami perubahan setelah pemulihan.

4. KESIMPULAN

Penelitian berjudul "Penerapan Metode National Institute of Justice dalam Pemulihan Data pada Flashdisk" menyimpulkan bahwa bukti digital yang dihapus dari flashdisk menggunakan metode Shift + Delete dan Quick

Format berhasil ditemukan dan dipulihkan dengan bantuan perangkat lunak forensik FTK Imager dan Autopsy. Seluruh bukti digital yang dipulihkan sesuai dengan data awal yang dimasukkan ke dalam flashdisk berdasarkan skenario kasus yang telah dirancang. Meskipun nama file berubah setelah proses pemulihan, ekstensi file tetap sama. Selain itu, hasil pemeriksaan nilai hash menggunakan WinMd5 menunjukkan bahwa ukuran file dan nilai hash MD5 tidak mengalami perubahan dibandingkan dengan file aslinya, yang membuktikan bahwa file tidak dimodifikasi. Penelitian ini menegaskan bahwa metode National Institute of Justice efektif sebagai pedoman untuk menganalisis bukti digital pada media penyimpanan flashdisk, khususnya pada tahap pemeriksaan dan analisis. Metode NIJ menyediakan panduan yang terorganisasi dengan baik dan terdokumentasi secara lengkap, memastikan setiap tahap proses pemulihan data dilakukan secara sistematis dan dapat dipertanggungjawabkan secara hukum. Selain itu, metode ini membantu melindungi integritas bukti dengan mencegah perubahan atau kerusakan data selama pemulihan, termasuk penggunaan teknik pencitraan forensik untuk menyalin isi flashdisk tanpa memengaruhi data asli. Namun kekurangan dari metode NIJ yaitu pembaruannya sering tertinggal dari perkembangan teknologi di bidang forensik digital. Hal ini menyebabkan metode tersebut kurang tanggap terhadap ancaman dan teknik baru, seperti analisis data cloud dan teknologi blockchain.

5. SARAN

Agar penelitian ini dapat dikembangkan lebih lanjut, perlu dilakukan peningkatan kualitas penelitian. Mengingat adanya keterbatasan dalam penelitian saat ini, beberapa usulan perbaikan untuk penelitian selanjutnya adalah sebagai berikut :

1. Menggunakan perangkat forensik lain untuk proses imaging maupun analisis file dapat menjadi alternatif untuk meningkatkan keakuratan dan efisiensi dalam proses forensik digital. Selain itu, menerapkan metode berbeda, seperti metode *static forensic*, juga dapat memberikan pendekatan yang lebih mendalam dan terfokus dalam menganalisis bukti digital pada media penyimpanan flashdisk, sehingga hasil analisis dapat lebih optimal dan mendukung validitas temuan dalam proses investigasi.
2. Melakukan penelitian dengan menggunakan objek lain, seperti hard disk, microSD, solid-state drive (SSD), dan perangkat penyimpanan lainnya, dapat memberikan wawasan yang lebih luas tentang efektivitas metode forensik digital yang digunakan. Penelitian ini juga dapat menguji kemampuan alat dan teknik yang berbeda dalam menangani berbagai jenis media penyimpanan, sehingga hasilnya dapat menjadi referensi yang lebih komprehensif untuk investigasi forensik digital di masa mendatang.

UCAPAN TERIMA KASIH

Dengan penuh rasa syukur, penulis menyampaikan penghargaan dan terima kasih kepada Universitas Muhammadiyah Sidoarjo, almamater tercinta, yang telah menjadi tempat menimba ilmu dan membentuk karakter selama masa studi. Ucapan terima kasih yang mendalam juga penulis sampaikan kepada Bapak Azmuri Wahyu Azinar, ST., M.Comp. selaku dosen pembimbing atas bimbingan, arahan, dan motivasi yang diberikan selama proses penelitian ini. Tidak lupa, penulis juga mengucapkan terima kasih kepada Bapak Irwan A. Kautsar, S.Kom., M.Kom., Ph.D selaku dosen penguji 1 dan Dr. Suprianto, S.Si. M.Si selaku dosen penguji 2 atas kritik, saran, dan masukan yang berharga dalam menyempurnakan penelitian ini. Semoga Allah SWT senantiasa memberikan keberkahan dan balasan atas segala ilmu dan kebaikan yang telah diberikan.

PENERAPAN METODE NATIONAL INTITUTE OF JUSTICE DALAM PEMULIHAN DATA PADA FLASHDISK -1.pdf

ORIGINALITY REPORT

13%	12%	6%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Purdue University Student Paper	4%
2	e-journals.unmul.ac.id Internet Source	2%
3	Submitted to Uganda Christian University Student Paper	1%
4	Submitted to Universitas Muhammadiyah Sidoarjo Student Paper	1%
5	id.scribd.com Internet Source	1%
6	Submitted to Universitas Muslim Indonesia Student Paper	<1%
7	repository.unmuhjember.ac.id Internet Source	<1%
8	animator.uho.ac.id Internet Source	<1%

9	Mochammad Choirul Anam, Irwan. "Utilization of Microservices for E-portfolio Digital Document Management Based on Telegram Bot", Procedia of Engineering and Life Science, 2022 Publication	<1 %
10	archive.org Internet Source	<1 %
11	jurnal.upnyk.ac.id Internet Source	<1 %
12	www.scilit.net Internet Source	<1 %
13	Candra Iswayudi, Irwan Alnarus Kautsar, Suprianto Suprianto. "Designing and Building a Web-Based Book Sales and Tenancy Platform", Procedia of Engineering and Life Science, 2023 Publication	<1 %
14	Rakhmad Fahmi Putra. "Rancang Bangun Sistem Log Server Berbasis RSyslog dan MySQL Untuk Monitoring Aktivitas Komputer Laboratorium", Electrician : Jurnal Rekayasa dan Teknologi Elektro, 2023 Publication	<1 %
15	eprints.unram.ac.id Internet Source	<1 %

16	jdih.kominfo.go.id Internet Source	<1%
17	muhariefeffendi.files.wordpress.com Internet Source	<1%
18	www.researchgate.net Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		