UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

UMSIDA
DARI SINI PENCERAHAN BERSEMI

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

Oleh:

Andhika Dwi Surya Achmad Saputra ,

Azmuri Wahyu Azinar

Progam Studi

Universitas Muhammadiyah Sidoarjo

2025

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*.

Pendahuluan

Flashdisk adalah perangkat penyimpanan berbasis memori flash yang portabel dan mudah digunakan untuk menyimpan dan memindahkan data. Meski bermanfaat, peningkatan penggunaannya membuka risiko kejahatan digital seperti pencurian data. Oleh karena itu, metode pemulihan data efektif sangat penting. Salah satu metode forensik digital yang sering digunakan adalah metode dari National Institute of Justice (NIJ), yang memiliki tahapan runtut dan terperinci: persiapan, penanganan insiden, pengumpulan, identifikasi, pemeriksaan, analisis, dan pelaporan. Metode NIJ dianggap lebih komprehensif dibanding metode lain seperti NIST, Static Forensics, dan GCFIM.

Metode Penelitian

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. 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.

Metode Penelitian

- Tahap identifikasi merupakan langkah awal akuisisi data yang bertujuan mengumpulkan informasi relevan untuk memahami objek atau kasus yang diteliti. Investigasi awal mencakup identifikasi kejadian, motif pelaku, dan dampaknya, serta pengumpulan dan penyimpanan barang bukti sesuai prosedur untuk menjaga integritasnya.

Metode Penelitian

- Tahap pengumpulan melibatkan pengambilan barang bukti, dokumentasi, dan pelabelan berdasarkan jenis atau merek. Dalam penelitian ini, pihak berwenang menemukan flashdisk biru merek Toshiba yang berfungsi baik tetapi telah diformat tanpa file.

Metode Penelitian

- Tahap pemeriksaan adalah proses verifikasi untuk memastikan keakuratan data dengan membandingkan data di lokasi kejadian dan file digital, serta mencegah manipulasi. Dalam penelitian ini, data dari flashdisk dianalisis menggunakan FTK Imager, Autopsy, dan WinMd5.

Metode Penelitian

- Tahap analisis dilakukan setelah verifikasi untuk mengungkap informasi penting menggunakan metode ilmiah dan legal. Hasil analisis berhasil memulihkan 4 file yang dihapus pelaku dalam format PDF, Word, Excel, dan PPT.

Metode Penelitian

- reporting, Setelah analisis data, langkah berikutnya adalah menyusun laporan terperinci yang mencakup seluruh tahapan investigasi, dari metode hingga hasil akhir. Laporan ini memberikan gambaran proses forensik dan menjadi dasar penyampaian fakta di persidangan.

Hasil Dan Pembahasan

Pemulihan data yang hilang biasanya memerlukan waktu singkat, tetapi kasus kompleks seperti data terfragmentasi, rusak, atau terenkripsi dapat memakan waktu lebih lama, bahkan hingga beberapa minggu, tergantung pada kompleksitas dan kondisi perangkat. Untuk efisiensi analisis forensik, penggunaan perangkat keras dan lunak khusus sangat penting. Tabel 1 mencantumkan alat-alat yang umum digunakan dalam praktik forensik data.

Hasil Dan Pembahasan

- Tabel 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

Hasil Dan Pembahasan

- 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 :

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

Hasil Dan Pembahasan

- Collection

Melakukan proses pengambilan barang bukti dari berbagai sumber yang relevan dengan kasus yang sedang diselidiki dan melakukan dokumentasi serta memeriksa jenis atau merk dari barang bukti guna dilakukan pelabelan barang bukti

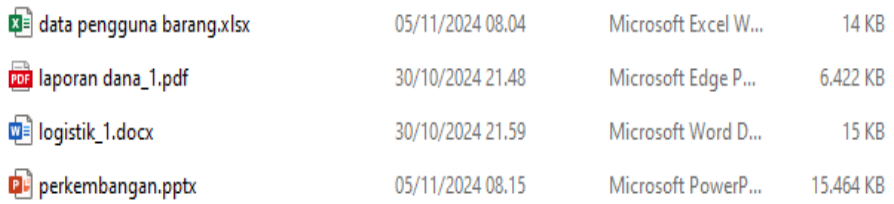
Dalam penelitian ini, pihak berwenang menemukan barang bukti berupa flashdisk berwarna biru bermerek Toshiba, seperti ditampilkan pada Gambar 4 Perangkat penyimpanan tersebut berfungsi dengan baik, namun dalam kondisi terformat atau kosong tanpa file apa pun.

Hasil Dan Pembahasan

- 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 :



data pengguna barang.xlsx	05/11/2024 08.04	Microsoft Excel W...	14 KB
laporan dana_1.pdf	30/10/2024 21.48	Microsoft Edge P...	6.422 KB
logistik_1.docx	30/10/2024 21.59	Microsoft Word D...	15 KB
perkembangan.pptx	05/11/2024 08.15	Microsoft PowerP...	15.464 KB

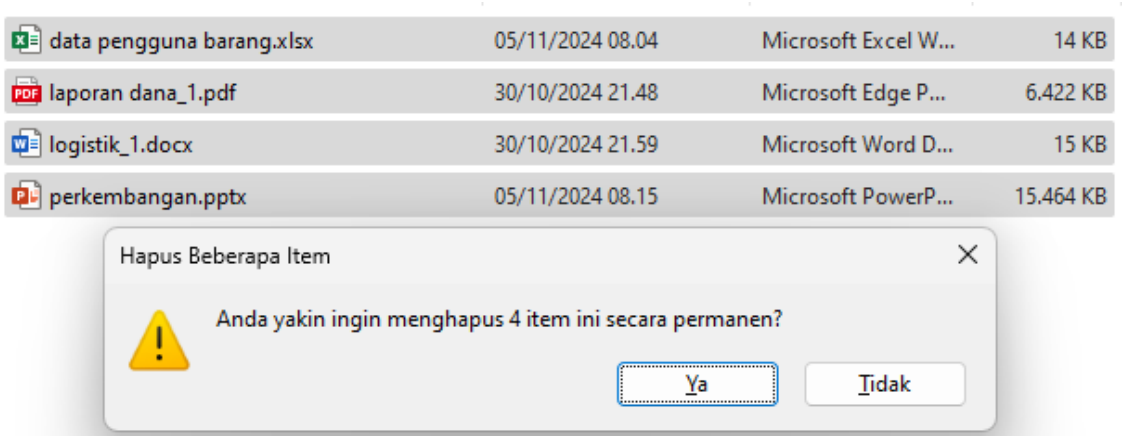
Hasil Dan Pembahasan

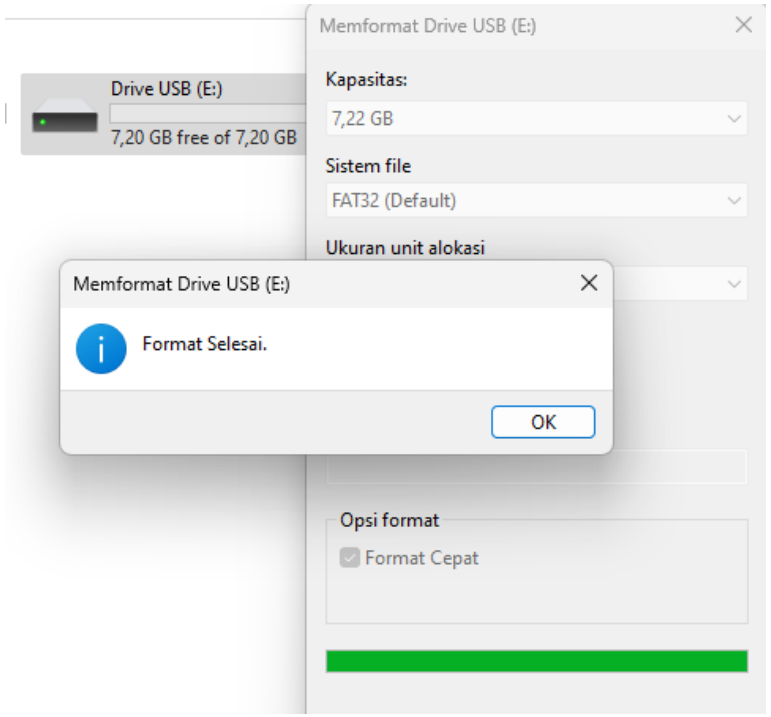
Kemudian, nilai hash dari setiap file diperiksa menggunakan tools *WinMd5*. Pemeriksaan nilai hash ini bertujuan untuk memastikan apakah hasil pemulihan data nantinya akurat atau tidak.

No	File	Hasil sebelum analisis
1.	Data pengguna barang.xls	703ac897869 4a6ad23fef1b92fa2b344
2.	Laporan dana_1.pdf	f1847951a327be7f0ec7b3d39c632a60
3.	Logistik_1.docx	bf5b76ff01a6c71527063ba71d409cdf
4.	Perkembangan.pptx	a70dfaf10b42bf511670422713b4e77f

Hasil Dan Pembahasan

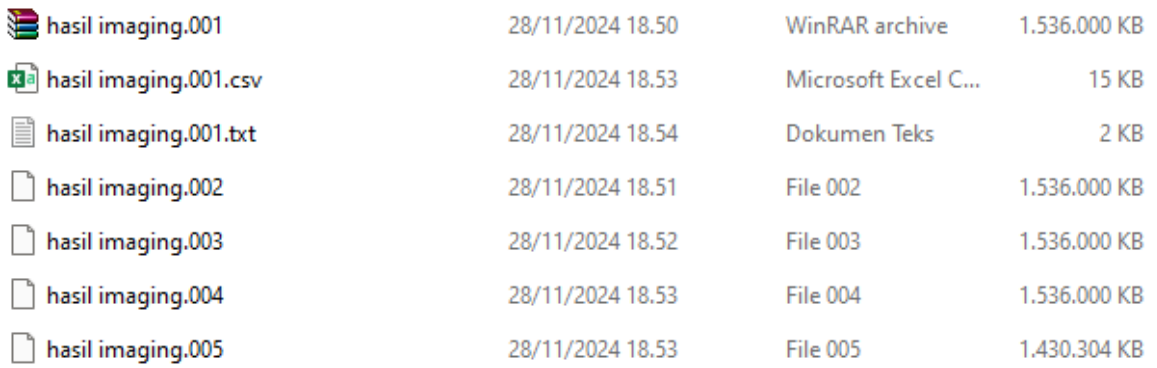
Berdasarkan skenario dalam penelitian ini, semua file yang terdapat di flashdisk akan dihapus menggunakan kombinasi *Shift + Delete*, kemudian dilakukan *quick format* seperti yang ditunjukkan pada gambar 6 di bawah ini.





Hasil Dan Pembahasan

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



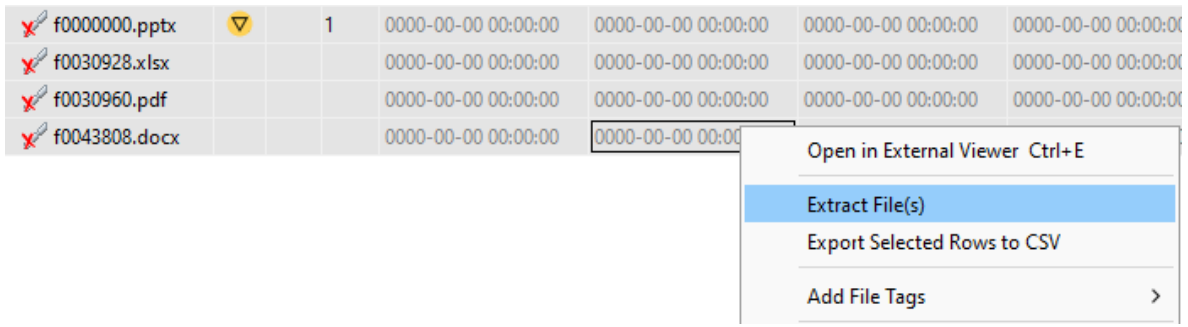
hasil imaging.001	28/11/2024 18.50	WinRAR archive	1.536.000 KB
hasil imaging.001.csv	28/11/2024 18.53	Microsoft Excel C...	15 KB
hasil imaging.001.txt	28/11/2024 18.54	Dokumen Teks	2 KB
hasil imaging.002	28/11/2024 18.51	File 002	1.536.000 KB
hasil imaging.003	28/11/2024 18.52	File 003	1.536.000 KB
hasil imaging.004	28/11/2024 18.53	File 004	1.536.000 KB
hasil imaging.005	28/11/2024 18.53	File 005	1.430.304 KB

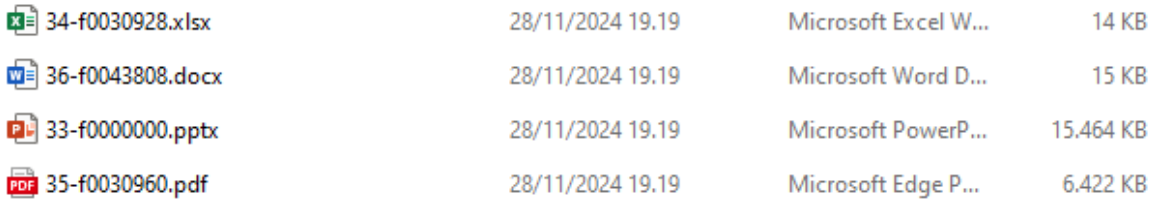
Setelah proses imaging selesai, langkah selanjutnya adalah melakukan akuisisi menggunakan tools *Autopsy*. Gambar 9 menunjukkan partisi yang dihasilkan dari proses akuisisi menggunakan Autopsy tersebut.

Hasil Dan Pembahasan

- Analysis

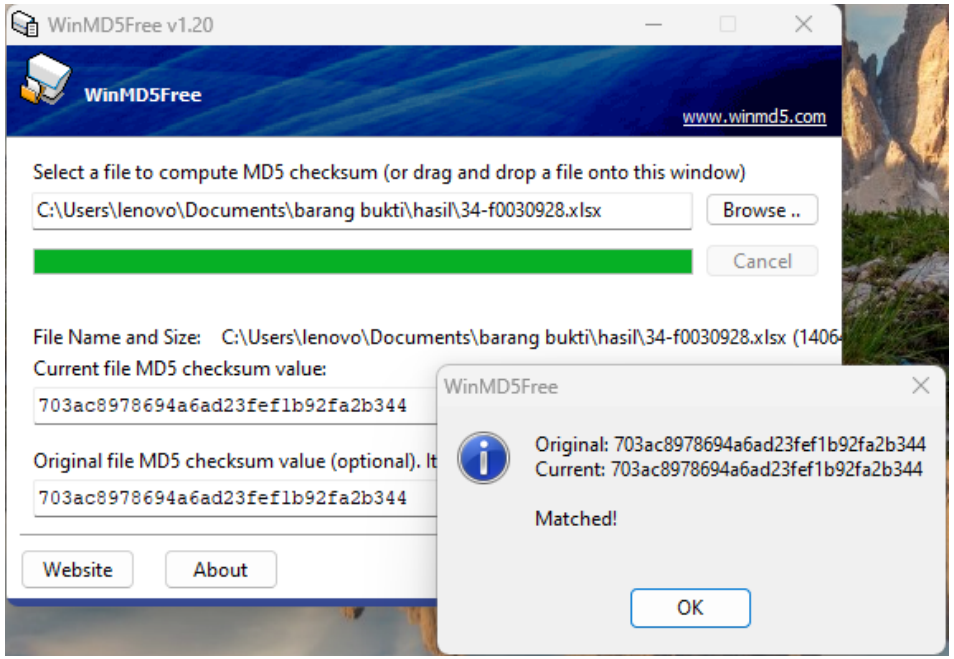
Pada tahap analisis dilakukan pengambilan data dari hasil *examinasi*. Hal ini dapat dilakukan dengan menggunakan pencarian manual, yaitu pencarian berdasarkan jenis file. Pada tahap ini proses yang dilakukan telah membuahkan hasil yaitu ter-*recovery* nya file atau data yang telah di hapus oleh pelaku. 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





Hasil Dan Pembahasan

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



Hasil Dan Pembahasan

Hasil validasi nilai hash untuk semua file menggunakan tools *WinMd5* menunjukkan kecocokan dengan file aslinya

,

file	Hasil sesudah analisis	Validasi
Data pengguna barang.xls	703ac897869 4a6ad23fe f1b92fa2b344	Cocok
Laporan dana_1.pdf	f1847951a32 7be7f0ec7b 3d39c632a60	Cocok
Logistik_1.docx	bf5b76ff01a6 c71527063b a71d409cdf	Cocok
Perkembangan.pptx	a70dfaf10b42 bf511670422 713b4e77f	Cocok

Hasil Dan Pembahasan

- 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.

Kesimpulan

Penelitian "Penerapan Metode National Institute of Justice dalam Pemulihan Data pada Flashdisk" menyimpulkan bahwa data yang dihapus dengan Shift + Delete dan Quick Format berhasil dipulihkan menggunakan FTK Imager dan Autopsy. Meskipun nama file berubah, ekstensi dan nilai hash MD5 tetap sama, membuktikan integritas file tidak terganggu. Metode NIJ efektif sebagai pedoman sistematis untuk analisis bukti digital, melindungi integritas data, dan menggunakan pencitraan forensik. Namun, metode ini kurang responsif terhadap teknologi baru seperti analisis data cloud dan blockchain karena pembaruannya sering tertinggal.

Saran

Untuk pengembangan lebih lanjut, penelitian dapat ditingkatkan dengan menggunakan perangkat forensik alternatif dan metode seperti static forensic untuk meningkatkan akurasi dan efisiensi analisis data. Selain itu, menggunakan objek lain seperti hard disk, microSD, dan SSD akan memperluas wawasan tentang efektivitas metode dan alat forensik, memberikan referensi yang lebih komprehensif untuk investigasi 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.

Referensi

[1] H. Sutanto, "Disruptive Strategy and Innovation: Cloud Storage dan Flashdisk." [Online]. Available: https://youtu.be/-ZnuYxaERfA

[2] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)," *Jurnal Telekomunikasi dan Komputer*, vol. 9, no. 3, p. 186, Jan. 2020, doi: 10.22441/incomtech.v9i3.7210.

[3] D. Anjani, D. Novianti, and R. Ningsih, "Training to Rescue and Repair Data on Flashdisk Storage for Elementary School Teachers of Pal Merah 19, West Jakarta," *Mattawang: Jurnal Pengabdian Masyarakat*, vol. 1, no. 2, pp. 99–103, Dec. 2020, doi: 10.35877/454ri.mattawang234.

[4] S. Soni, Y. Fatma, and R. Anwar, "Akuisisi Bukti Digital Aplikasi Pesan Instan 'Bip'Menggunakan Metode National Institute Of Justice (NIJ)," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 3, no. 1, pp. 34–42, Jun. 2022, doi: 10.37859/coscitech.v3i1.3694.

[5] M. Syaiful Huda Mubarok, Ms. Huda Mubarok, R. Novrianda Dasmen, V. Pranata, and Ma. Januarta, "Digital Analysis of Forensic Data Recovery on Flash Drive Using National Institute Of Justice (NIJ) Method."

Referensi

- [7] S. K. Saad, R. Umar, A. Fadlil, U. Ahmad, D. Jl, and S. H. Soepomo, “Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas,” 2020.
- [8] G. Maulana Zamroni, R. Umar, and I. Riadi, “Analisis Forensik Aplikasi Instant Messaging Berbasis Android,” 2016. [Online]. Available: http://ars.ilkom.unsri.ac.id
- [9] A. Wijaya Kusuma, E. I. Alwi, and R. Ramdaniah, “Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST),” 2024.
- [10] B. Bulan, T. Tahun, A. Yudhana, R. Umar, and A. Ahmadi, “X X X X738X 738X 738X 738X (Print) (Print) (Print) (Print) Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ).”
- [11] M. Riskiyadi, “INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP CYBERCRIME,” 2020.
- [12] “1490-Article Text-2859-1-10-20190413”.


UMSIDA
DARI SINI PENCERAHAN BERSEMI