JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i3.11025

ANALISIS FORENSIK DIGITAL DALAM PEMULIHAN DATA PADA MEDIA PENYIMPANAN FLASHDISK MENGGUNAKAN METODE NIST SP 800-86

Siti Sarah[1*], Yodi Susanto, Persis Haryo Winasis[3]

[1,2,3]Universitas IPWIJA; Jl. Letda Nasir No.7, Nagrak, Gn. Putri, Bogor, Jawa Barat; (021) 8233737

Keywords:
Forensik Digital;
Pemulihan Data;
Flashdisk; NIST SP 800-86
Autopsy.

Corespondent Email:
sitisarahipwija@gmail.com

Abstrak. Seiring dengan kemajuan teknologi yang berkembang pesat membuat penggunaan teknologi digital menjadi salah satu bagian penting dalam kehidupan manusia. Namun, adanya kemudahan digitalisasi tak luput dari ancaman cybercrime. Data-data yang didapatkan dari hasil kejahatan siber biasanya akan disembunyikan dalam media penyimpanan yang mana nantinya akan digunakan kembali untuk melakukan penipuan, pencurian, pengintaian dan bullying. Para pelaku kejahatan siber biasanya akan memilih menghapus, menyembunyikan, dan memformat data yang dikumpulkan sehingga proses file carving perlu dilakukan pada bukti digital yang ditemukan. Barang bukti elektronik umumnya perangkat elektronik atau media penyimpanan berbentuk fisik yang berisi riwayat suatu jejak kegiatan kejahatan Flashdisk digunakan dalam proses penyelidikan guna menunjukan adanya keterkaitan pelaku dalam aktivitas kejahatan siber. Forensik digital merupakan proses mengumpulkan dan menganalisis bukti digital dari barang bukti digital guna menindak kejahatan siber.Salah satu metode yang umum digunakan dalam analisis forensik digital yaitu metode NIST (National Institute of Standards and Technology). NIST membuat pedoman untuk membantu melakukan analisis forensik digital terhadap bukti digital pada media penyimpanan atau perangkat digital dengan kode NIST SP 800-86. Penelitan ini berhasil melakukan pemulihan data dengan menggunakan metode NIST SP 800-86. Terbukti dari tujuh file yang dihapus, semua file dapat dikembalikan dengan integritas data yang tetap terjaga dan tidak ada perubahan pada data tersebut.

Abstract. *Rapid technological advancements have made the use of digital technology an integral part of human life. However, the convenience brought about by digitalization is accompanied by the threat of cybercrime. Data obtained through cybercrimes is typically concealed within storage media, intended for future use in fraud, theft, surveillance, and bullying. Perpetrators often delete, hide, or format the collected data, necessitating the use of file carving techniques on the discovered digital evidence. Electronic evidence generally consists of electronic devices or physical storage media containing traces of criminal activity; for instance, flash drives are utilized during investigations to establish a perpetrator's link to cybercriminal acts. Digital forensics involves the collection and analysis of digital evidence to address cybercrime. A commonly employed method in digital forensic analysis is the NIST (National Institute of Standards and Technology) approach. NIST established guidelines—designated as NIST SP 800-86—to assist in the forensic analysis of digital evidence found on storage media or digital devices. This study successfully recovered data using the NIST SP 800-86 method; specifically, all seven deleted files were restored with their data integrity intact and without any alterations to the data itself.*

1. PENDAHULUAN

Seiring dengan kemajuan teknologi yang berkembang pesat membuat penggunaan teknologi digital menjadi salah satu bagian penting dalam kehidupan manusia. Kemajuan teknologi ini juga didukung dengan adanya internet. Pemanfaatan digitalisasi memberikan kemudahan bagi individu atau kelompok dalam melakukan berbagai aktivitas. Namun, adanya kemudahan digitalisasi tak luput dari ancaman cybercrime.

Cybercrime adalah memanfaatkan teknologi sistem informasi jaringan komputer dalam bentuk tindakan yang illegal yang dilakukan oleh pelaku kejahatan [1]. Secara sederhana cybercrime merupakan suatu aksi kejahatan seperti spamming, illegal access, DoS attack, pencurian data penipuan identitas menggunakan komputer dan jaringan komputer sebagai alat [2].

Data-data yang didapatkan dari hasil kejahatan siber biasanya akan disembunyikan dalam media penyimpanan yang mana nantinya akan digunakan kembali untuk melakukan penipuan, pencurian, pengintaian dan bullying. Para pelaku kejahatan siber biasanya akan memilih menghapus, menyembunyikan, dan memformat data yang dikumpulkan sehingga proses file carving perlu dilakukan pada bukti digital yang ditemukan [3].

Barang bukti elektronik umumnya perangkat elektronik atau media penyimpanan berbentuk fisik yang berisi riwayat suatu jejak kegiatan kejahatan. Sedangkan bukti digital merupakan riwayat berupa file, log, event atau history yang berisi informasi kegiatan cybercrime yang didapat dari proses identifikasi dan pengambilan data dari barang bukti elektronik [4].

Flashdisk merupakan salah satu barang bukti elektronik media penyimpanan data portable yang memiliki port USB yang dapat dihubungkan ke suatu perangkat komputer, laptop, smartphone atau smartTV. Flashdisk digunakan dalam proses penyelidikan guna menunjukan adanya keterkaitan pelaku dalam aktivitas kejahatan siber [5].

Pelaku cybercrime biasanya akan melakukan berbagai cara untuk menghilangkan barang bukti yang berhubungan dengan tindak kejahatan yang mereka lakukan. Beragam cara dilakukan untuk menghilangkan barang bukti atas kejahatan yang dilakukan oleh pelaku cybercrime. Tindakan menghapus atau memformat data informasi agar tidak ditemukan merupakan salah satu cara untuk menghilangkan bukti digital [6]. Pada umumnya cara yang digunakan dalam menghapus data yaitu dengan melakukan perintah delete dan menghapus dari recycle bin atau trash pada sistem komputer. Untuk memulihkan data atau informasi yang telah di hapus atau di sembunyikan oleh pelaku maka diperlukan proses forensic digital agar penyidik dapat membereskan kasus cybercrime [7].

Forensik digital merupakan proses mengumpulkan dan menganalisis bukti digital dari barang bukti digital guna menindak kejahatan siber. Forensik digital adalah disiplin ilmu dalam mengumpulkan dan menganalisis bukti digital yang legal terkait dalam lingkup hukum untuk mengungkap dan menuntut kejahatan siber [8].

Salah satu metode yang umum digunakan dalam analisis forensik digital yaitu metode NIST (National Institute of Standards and Technology). NIST membuat pedoman untuk membantu melakukan analisis forensik digital terhadap bukti digital pada media penyimpanan atau perangkat digital dengan kode NIST SP 800-86. Dalam NIST SP 800-86 pelaksanaan forensik digital terdiri dari empat tahapan penting yaitu: Collection, Examination, Analysis, dan Reporting [9]. Adapun alat yang digunakan untuk melakukan pemulihan data dalam forensik digital yaitu Autopsy.

Oleh karena itu, penelitian ini bertujuan pada Analisis Forensik Digital Dalam Pemulihan Data pada Media Penyimpanan Flashdisk Menggunakan Metode NIST SP 800-86.

2. TINJAUAN PUSTAKA

2.1 Forensik digital

Forensik digital merupakan aktivitas mengumpulkan bukti yang bersumber dari sistem komputer dan jaringan yang memenuhi standar. Bukti yang terkumpul akan dilakukan pemeriksaan untuk mendapatkan informasi yang relevan. Bukti yang sesuai standar diharapkan dapat diterima oleh penegak hukum. Laporan forensik digital dibuat dari hasil analisis dan pemeriksaan bukti data digital yang merangkum inti dari data digital yang diperiksa. Bukti digital yang ditemukan dilakukan proses pemulihan dan pemeriksaan yang mana

merupakan metode dari digital forensik [10]. Tujuan digital forensik yaitu mendukung bukti digital agar dapat dipertanggungjawabkan secara digital dalam upaya hukum [11]

2.2 Cybercrime

Tindakan kejahatan yang dilakukan dengan memanfaatkan teknologi informasi komputer dan jaringan disebut sebagai cybercrime [12]. Cybercrime adalah sebuah kegiatan yang menggunakan teknologi sebagai alat atau media dalam melakukan tindakan kejahatan, seperti meretas jaringan, akses illegal, membobol informasi, menghilangkan informasi, menyembunyikan informasi dan mengubah informasi [3]

2.3 Bukti Digital

Data yang disimpan atau dikirim melalui perangkat seperti komputer, laptop, smartphone atau media penyimpanan seperti hdd, flash drive, kartu memori. (Yuwono, Juhairiah, & Sonedi, 2019). Bukti digital bersifat mudah rusak, tidak stabil, dan rawan jika tidak dikelola dengan baik. Bukti digital perlu dikelola dengan baik karena sifatnya yang mudah rusak dan labil maka perlu disimpan dan diamankan pada tempat yang sesuai standar. Bukti digital disebut sebagai informasi elektronik dan dokumen elektronik berdasarkan UU No. 11 Tahun 2008 RI tentang Informasi dan Transaksi Elektronik, maka dalam menangani kasus kejahatan yang berhubungan dengan bukti elektronik atau digital, perlu menganalisis dan menyelidiki dengan teliti ragam barang bukti digital [13]

2.4 Pemulihan Data (Recovery Data)

Pemulihan data adalah proses pemulihan atau pemulihan data yang disebabkan karena hilang, rusak, atau tidak sengaja terhapus dari penyimpanan digital [14].Upaya untuk memulihkan data yang hilang atau dihapus secara sengaja atau tidak sengaja pada perangkat penyimpanan seperti Hard drive, Flash drive, atau kartu memori. Beberapa hal yang menyebabkan data dapat hilang seperti adanya malware, kerusakan pada perangkat penyimpanan, kesalahan atau kelalaian manusia. Proses pemulihan data dimulai dengan mengidentifikasi penyebab hilangnya data dan menentukan apakah data masih dapat dipulihkan. Hal pertama yang dilakukan dalam proses pemulihan data yaitu dengan mengenali penyebab data dapat hilang dan memastikan data dapat dipulihkan kembali atau tidak. [5]

2.5 NIST SP 800-86

Metode NIST SP 800-68 merupakan metode yang umum digunakan untuk melakukan analisis forensik. NIST (National Institute of Standards and Technology) merupakan lembaga yang bertugas membuat standar, panduan, dan persyaratan minimum untuk mempersiapkan keamanan informasi yang sesuai bagi tiap aset serta menjadi pihak yang mempunyai keahlian di bidang digital forensic. Metode yang dikembangkan oleh NIST ini umumnya digunakan oleh pemerintah pusat di Amerika, namun tidak menutup kemungkinan dapat diimplementasikan juga oleh organisasi seperti akademisi, badan penyidik swasta dan lainnya [15]. Terdapat empat langkah dalam NIST SP800-86 yaitu tahap pengumpulan data, tahap pemeriksaan informasi, tahap analisis, dan tahap pelaporan bukti [16]

2.6 USB Flash Drive (Flashdisk)

USB flash drive atau lebih dikenal Flashdisk, merupakan perangkat berukuran kecil yang digunakan sebagai media penyimpanan data portable. Data yang dapat disimpan berupa dokumen, audio, video, gambar dan juga sistem operasi. Dilengkapi dengan port USB sehingga dapat terhubung ke komputer atau perangkat lainnya. Karena ukurannya yang kecil, Flashdisk mudah untuk dibawa ke mana-mana. Flashdisk memiliki kapasitas yang beragam sesuai dengan kebutuhan mulai dari 2GB, 8GB, 16GB, 32GB, 64 GB, 128GB, 256GB bahkan hingga 1TB.

2.7 Autopsy

Autopsy merupakan perangkat lunak yang sifatnya open source, umunya digunakan untuk membantu analisis forensik pada data digital, perangkat keras dan perangkat lunak. Autopsy dikembangkan oleh Basis Technology Corp dan diperbarui secara berkala oleh komunitas pengembang terbuka. Perangkat lunak ini dapat digunakan pada berbagai sistem operasi seperti Windows, Linux, dan MacOS. Autopsy membantu dalam melakukan analisis forensik digital dan banyak digunakan oleh seperti peneliti, penegak hukum, tim investigasi dalam menyelidiki suatu kasus kejahatan digital [5]

2.8 FTK Imager

FTK Imager adalah perangkat lunak forensik yang digunakan untuk memperoleh salinan

forensik atau memperoleh gambar dari perangkat penyimpanan data [5]

3. METODE PENELITIAN

Makalah Metode yang digunakan pada penelitian ini yaitu menggunakan metode NIST SP 800-86 dengan tahapan sebagai berikut:

3.1 Penerapan Metode Penelitian

a. Collection, pada tahap ini peneliti mengumpulkan barang bukti fisik dan bukti digital dari sumber yang relevan serta melakukan prosedur pemeliharaan dan pengawasan terhadap objek agar keaslian objek tidak berubah dan integritas data tetap terjaga
b. Examination, pada tahap ini peneliti melakukan pemeriksaan dam pemulihan data secara cermat dari barang bukti yang ditemukan dan bukti digital. Pada tahapan ini penulis menggunakan alat digital forensik yaitu Autopsy dan FTK Imager.
c. Analysis, Bukti digital yang telah ditemukan akan dilakukan analisis, mencocokan nilai hash MD5 untuk mendapatkan validasi dari bukti digital yang ditemukan.
d. Reporting yaitu hasil dari tahapan-tahapan yang dilakukan akan didokumentasikan dalam bentuk laporan.

3.2 Skenario Kasus

Adapun simulasi skenario kasus kejatahatan digital sebagai berikut:
Seorang karyawan tidak mengunci layar laptop sebelum meninggalkan ruangan.

a. Pelaku yang sedang melintas di area tersebut secara tidak sengaja melihat kesempatan untuk melakukan kejahatan, pelaku segera yang masuk keruangan dan menggunakan laptop tersebut untuk mencari suatu data-data yang sifatnya rahasia.
b. Setelah menemukan data yang dibutuhkan, pelaku menyalin data tersebut lalu menyimpannya dalam media penyimpanan berupa flashdisk.
c. Karyawan menyadari kelalaiannya lalu segera kembali keruangan untuk mengunci layar laptopnya. Namun ketika sampai diruangan, posisi laptop sudah berubah dan folder berisi data-data rahasia terbuka.
d. Karena khawatir, karyawan kemudian melakukan pengecekan CCTV dan didapatkan ada seseorang yang menggunakan laptopnya dan memegang sebuah perangkat berupa flashdisk.
e. Pelaku yang tertangkap melakukan pembelaan dengan mengatakan bahwa dia tidak melakukan hal apapun diruangan tersebut. Sebelum tertangkap, pelaku telah menghapus data-data pada flashdisk untuk menghilangkan jejak kejahatan dan bukti digital.
f. Perangkat flashdisk yang dicurigai sebagai tempat menyimpan data-data dilakukan pemeriksaan. Namun hasil pemeriksaan tidak ditemukan data apapun.
g. Ahli IT ditugaskan untuk melakukan recovery data pada flashdisk yang bertujuan untuk mengungkap dan memastikan kejadian yang sebenarnya telah terjadi.
h. Setelah melakukan recovery data, Ahli IT memastikan bahwa data yang telah di recovery tidak ada yang berubah dan integritas data masih terjaga.

4. HASIL DAN PEMBAHASAN

Pada analisis forensik dibutuhkan bahan pendukung berupa perangkat lunak dan perangkat keras yang digunakan dalam selama proses penyeledikan suatu kasus.

Tabel 1. Spesifikasi alat

Alat	Spesifikasi	Keterangan
Laptop	HP Laptop 14-ep0xxx, Windows 11	Perangkat keras untuk melakukan forensik
Flashdisk	Jete 4GB	Perangkat keras yang merupakan barang bukti
Autopsy	Autopsy v4.22.1	Perangkat lunak untuk melakukan forensik

4.1Collection

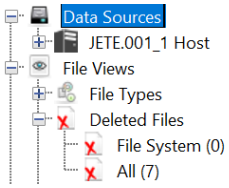
Pada tahap ini pengumpulan barang bukti elektronik yaitu flashdisk Jete dengan kapasistas 4GB yang berisi bukti digital yang digunakan pelaku untuk menyimpan data-data.

Gambar 2. Barang Bukti Elektronik berupa Flashdisk

Pada proses ini, pemeliharaan dan pengawasan dilakukan pada barang bukti fisik dan membuat salinan yang serupa dengan aslinya dalam bentuk file image menggunakan perangkat lunak forensik yaitu FTK Imager.

4.2Examination

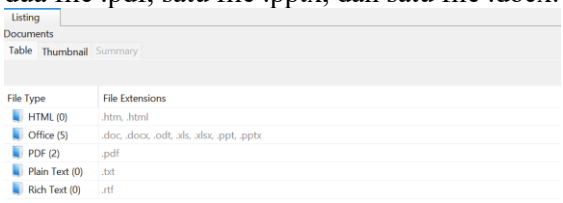
Tahan examination yaitu dilakukan proses akuisisi data untuk memperoleh informasi terkait riwayat data-data yang pernah disimpan dalam flashdisk. Proses ini menggunakan perangkat lunak Autopsy, hasilnya terdapat tujuh data yang sebelumnya telah dihapus ditemukan kembali.



Gambar 3. Akuisisi Data

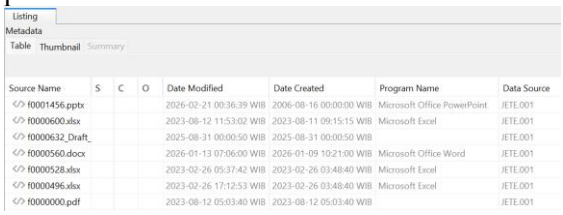
4.3 Analysis

Pada tahap ini menganalisis bukti digital dengan mencari nama berkas secara manual. Berkas yang ditemukan terdiri dari tujuh file dengan beberapa format file yaitu tiga file .xlsx, dua file .pdf, satu file .pptx, dan satu file .docx.



Gambar 4. File Type

Tujuh data tersebut berhasil dilakukan pemulihan data dengan kondisi baik yaitu data masih terjaga integritasnya dan tidak ada perubahan



Gambar 5. Pemulihan Data

Selanjutnya dilakukan validasi terhadap tujuh data tersebut dengan mencocokan nilai hash (MD5) pada data bukti digital. Berikut hasil pencocokan nilai hash hasil pemulihan data dari Autopsy. Hasil validasi yaitu semua berkas sama seperti berkas aslinya

Tabel 2. Validasi Hash (MD5)

Nama File	Autopsy	Validasi
f0000000.pdf	5410ac152b24dbd81a7211c844303088	Cocok
f0000496.xlsx	f9ac49ea95169fca6c1cd27f1ee612b1	Cocok
f0000528.xlsx	dff2ebb640783e15b182b88eae608a37	Cocok
f0000560.docx	e92e18723cdfca15c3e2b73bef42505a	Cocok
f0000600.xlsx	8f489ed5b5655ecc77b1c3722aa5d9b2	Cocok
f0000632_Draft_.pdf	e13f48b39acc46e85351453aa725b17c	Cocok
f0001456.pptx	a15b29cbe43a2162a14fcbb4e6048fba	Cocok

4.4 Reporting

Setelah melewati beberapa tahapan yang telah dilakukan, semua data-data yang sebelumnya dihapus dari barang bukti Flashdisk yaitu terdiri dari tujuh file bisa dilakukan pemulihan data. Penggunaan metode NIST SP 800-86 beserta perangkat lunak forensik yaitu FTK Imager dan Autopsy terbukti dapat membantu pemulihan data yang sebelumnya telah dihapus.

KESIMPULAN

Penelitian ini telah berhasil melakukan pemulihan data dengan menggunakan metode NIST SP 800-86 beserta perangkat lunak forensik yaitu FTK Imager dan Autopsy. Terbukti dari tujuh file yang dihapus, semua file dapat dikembalikan dengan integritas data yang tetap terjaga dan tidak ada perubahan pada data tersebut.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] A. I. Yuladi and R. Indrayani, “ANALISIS DAN PERBANDINGAN TOOLS FORENSIK MENGGUNAKAN METODE NIST DALAM PENANGANAN KASUS KEJAHATAN SIBER,” *J. Teknol. Terpadu*, vol. 9, no. 2, pp. 95–100, 2023.

[2] H. Handrizal, “Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik,” *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 1, no. 1, 2017, doi: 10.30645/j-sakti.v1i1.31.

[3] D. T. Yuwono, S. Juhairiah, and Sonedi, “ANALISIS FILE CARVING PADA FILE SYSTEM DENGAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST),” *J. Teknol. dan Sist.*

Inf., 2019.

[4] W. Agustiono, D. W. Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus," *J. Teknol. dan Inf.*, vol. 14, no. 2, pp. 174–185, 2024, doi: 10.34010/jati.v14i2.12952.

[5] Mega Rosita, "Analisis Komparatif Performa FTK IMAGER dan AUTOPSY dalam Forensik Digital pada Flashdisk," *J. Info Kripto*, vol. 17, no. 3, 2023, doi: 10.56706/ik.v17i3.83.

[6] W. Agustiono, D. Wulan Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," *J. Teknol. dan Inf.*, vol. 14, 2024, doi: 10.34010/jati.v14i2.

[7] A. Al Anhar, M. Gandeva Bayu Satrya ST., and F. A. Yulianto, "Analisis Perbandingan Keamanan Teknik Penghapusan Data Pada Hardisk Dengan Metode DoD 5220.22 dan Gutmann," *eProceedings Eng.*, vol. 1, no. 1, pp. 607–613, 2014, [Online]. Available: http://libraryeproceeding.telkomuniversity.ac.id/index.php/engineering/article/view/2830/4521

[8] 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.

[9] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Natl. Inst. Stand. Technol.*, 2006.

[10] K. E. Purnama, C. Rozikin, and A. A. Ridha, "ANALISIS FORENSIC CITRA DIGITAL MENGGUNAKAN TEKNIK ERROR LEVEL ANALYSIS DAN METADATA BERDASARKAN METODE NIST," 2023.

[11] Aidil Wijaya Kusuma, Erick Irawadi Alwi, and Ramdaniah Ramdaniah, "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)," *Cyber Secur. dan Forensik Digit.*, vol. 7, no. 1, pp. 18–24, 2024, doi: 10.14421/csecurity.2024.7.1.4345.

[12] F. Yudha, "USB ANALISYS TOOL UNTUK INVESTIGASI FORENSIKA DIGITAL," *Teknoin*, vol. 21, no. 4, pp. 200–206, 2015.

[13] L. Susanti and A. Akrom, "Analisis Efektivitas File Carving dalam Forensik Digital pada Flashdisk Dengan Tools Autopsy dan FTK Imager," *J. Locus Penelit. dan Pengabdi.*, vol. 4, no. 9, pp. 8978–8989, 2025, doi: 10.58344/locus.v4i9.4857.

[14] M. Syaiful Huda Mubarok, A. Ardiansyah, R. Novrianda Dasmen, V. Pranata, and M. A. Januarta, "Digital Analysis of Forensic Data Recovery on Flash Drive Using National Institute Of Justice (NIJ) Method," *J. Ilm. Inform.*, vol. 12, no. 01, pp. 75–79, 2024.

[15] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, pp. 89–94, 2020, doi: 10.32493/informatika.v5i1.4578.

[16] K. Eka Purnama, C. Rozikin, and A. Ali Ridha, "Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode NIST," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 2, pp. 1100–1107, 2023, doi: 10.36040/jati.v7i2.6660.