AKUISISI BARANG BUKTI DIGITAL PADA MEDIA PENYIMPANAN FLASHDISK MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF JUSTICE (NIJ)

Hayyan Idhofi, Gufron Zaida Muflih
Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen
Jalan Raya Kutoarjo km 5 Jatisari, Kebumen, Indonesia
hayyanidhofi24@gmail.com

ABSTRAK

Maraknya kasus korupsi Dana BOS yang melibatkan teknologi digital menjadi permasalahan serius di dunia pendidikan. Berdasarkan data ICW 2023, tercatat 791 kasus korupsi dengan kerugian Rp28,4 triliun, di mana pelaku memanfaatkan media penyimpanan portable dan steganografi untuk menyembunyikan bukti. Penelitian ini bertujuan mengidentifikasi dan mengumpulkan bukti digital dalam kasus korupsi dana BOS, menganalisis serta memulihkan data dari flash disk, dan mengeksplorasi penggunaan steganografi. Metode yang digunakan adalah framework NIJ dengan lima tahapan: identification, collection, examination, analysis, dan reporting, didukung oleh tools Recuva untuk pemulihan data dan Steghide untuk analisis steganografi. Hasil penelitian menunjukkan tingkat keberhasilan recovery data mencapai 95% pada penghapusan standar, 78% pada secure delete (1 pass), 45% pada DOD Standard (3 pass), 89% pada format quick, dan 32% pada format low level. Analisis steganografi berhasil mengekstrak file "Laporan_dana_BOS.docx" dari gambar "Depan_Sekolah.jpg", mengungkap bukti transfer dana ke rekening pribadi. Penelitian menyimpulkan bahwa framework NIJ efektif dalam akuisisi dan analisis bukti digital, dengan rekomendasi peningkatan keamanan dana BOS, standardisasi SOP investigasi, pelatihan tim forensik, dan penelitian lanjutan tentang deteksi dini penyalahgunaan dana.

Kata kunci : *Digital Forensik, Framework NIJ, Recovery Data, Steganografi, Flasdisk*

1. PENDAHULUAN

Kejahatan merupakan fenomena sosial yang berkembang seiring dengan dinamika masyarakat. Dalam berbagai bentuknya, kejahatan tidak hanya mencakup tindakan kekerasan dan kriminalitas konvensional, tetapi juga kejahatan yang bersifat sistemik dan merugikan kepentingan publik, seperti korupsi. Korupsi merupakan ancaman serius yang telah merusak berbagai sektor di Indonesia, termasuk Pendidikan [1].

Praktik ini tidak hanya merugikan keuangan negara tetapi juga menghambat perkembangan kualitas pendidikan. Berdasarkan data *Indonesia Corruption Watch* (ICW) tahun 2023, tercatat 791 kasus korupsi dengan 1.695 tersangka, mengakibatkan potensi kerugian negara sebesar Rp28,4 triliun. Seiring dengan perkembangan teknologi, modus operasi pelaku semakin canggih, termasuk penggunaan perangkat digital untuk menyimpan, menyamarkan, dan menghilangkan bukti kejahatan**.**

Kasus korupsi Dana Bantuan Operasional Sekolah (BOS) yang terungkap menunjukkan bagaimana teknologi dimanfaatkan untuk melancarkan aksi korupsi. Contoh kasus terjadi di beberapa sekolah di Jawa Barat, seperti di SMAN 5 Sukabumi, di mana kepala sekolah dan bendahara melakukan manipulasi laporan pertanggungjawaban dan tidak menggunakan dana BOS sesuai peruntukan, menyebabkan kerugian negara sebesar Rp519,72 juta. Kasus serupa juga terjadi di SMAN 3 Depok, di mana dana BOS dan dana Peningkatan Manajemen Mutu Sekolah (PMMJ) tahun 2015-2016 digunakan di luar Rencana Kerja Sekolah (RKS), menyebabkan kerugian sebesar Rp2,7 miliar. Selain itu, SMAN 6 Cimahi melaporkan indikasi penyalahgunaan dana BOS dengan pembuatan laporan fiktif tanpa bukti pengeluaran yang jelas. [2].

Dalam beberapa kasus, pelaku memanfaatkan aplikasi edit PDF untuk memanipulasi laporan penggunaan dana, mulai dari mengubah angka dalam dokumen pertanggungjawaban hingga menghapus beberapa rincian transaksi agar tidak terdeteksi dalam audit. Misalnya, dalam kasus SMAN 2 Depok dan SMAN 4 Depok, laporan keuangan yang telah dimanipulasi digunakan untuk menutupi pengeluaran yang tidak sesuai peruntukan, seperti pengembangan perpustakaan dengan dana ratusan juta rupiah meskipun sekolah sedang tidak beroperasi akibat pandemi. Tidak jarang, dokumen hasil manipulasi ini juga dicetak ulang dan dipresentasikan sebagai laporan resmi guna meyakinkan pihak berwenang bahwa penggunaan dana sudah sesuai aturan. Modus seperti ini semakin memperumit investigasi dan menunjukkan bagaimana teknologi dapat dimanfaatkan untuk menyembunyikan jejak korupsi dalam pengelolaan dana BOS.

Salah satu media yang sering digunakan adalah perangkat pemyimpanan portable flash disk, yang dimanfaatkan untuk menyimpan dokumen keuangan atau bukti transaksi illegal [3].

Flash disk dipilih karena ukurannya yang kecil, ringan, dan mudah dibawa ke mana saja, sehingga memudahkan pelaku dalam menyimpan atau memindahkan data tanpa menarik perhatian. Selain itu, flash disk juga dapat dengan mudah disembunyikan atau bahkan dihancurkan jika diperlukan, membuatnya menjadi alat yang ideal untuk menghilangkan jejak transaksi ilegal sebelum penyelidikan dilakukan.

Selain itu, teknologi steganografi digunakan untuk menyembunyikan data dalam file digital, sehingga sulit dideteksi oleh penyidik [4].

Steganografi digital menjadi teknik yang semakin populer di kalangan pelaku korupsi karena kemampuannya menyembunyikan informasi sensitif dalam file-file yang tampak tidak mencurigakan. Teknik ini memungkinkan pelaku menyisipkan dokumen-dokumen bukti transaksi ilegal, daftar penerima suap, atau laporan keuangan yang dimanipulasi ke dalam file gambar, audio, atau video tanpa meninggalkan jejak yang mudah terdeteksi. Misalnya, sebuah file spreadsheet berisi rincian transfer dana ilegal dapat disisipkan ke dalam file foto kegiatan sekolah tanpa mengubah tampilan visual foto tersebut. Bahkan dalam beberapa kasus, pelaku menggunakan teknik steganografi berlapis, di mana file yang sudah disembunyikan kemudian dienkripsi lagi untuk menambah lapisan keamanan. Tidak jarang, pelaku juga menggunakan perangkat lunak penghapus data permanen untuk menghilangkan bukti sebelum penyelidikan dilakukan [5].

Kondisi ini menunjukkan perlunya metode investigasi digital yang lebih efektif untuk mengungkap kejahatan korupsi [6].

Untuk menghilangkan jejak, pelaku sering menggunakan software penghapus data seperti Eraser, yang mampu menghapus file secara permanen dengan menimpa data beberapa kali menggunakan pola acak. Teknik ini membuat proses pemulihan data menjadi sangat menantang, bahkan dengan menggunakan tools recovery modern. Namun, dengan menggunakan tools forensik seperti Recuva, investigator masih memiliki kesempatan untuk memulihkan file-file yang telah dihapus, termasuk file yang telah diproses dengan software penghapusan data.

Dalam konteks ini, digital forensik memainkan peran penting dalam mengidentifikasi, menganalisis, dan memulihkan bukti digital yang telah dihapus atau disamarkan. Teknik ini memungkinkan penyidik memperoleh kembali data dari berbagai media penyimpanan, termasuk flash disk, yang sering digunakan dalam tindak pidana korupsi [7].

Salah satu pendekatan yang banyak digunakan adalah framework National Institute of Justice (NIJ), yang memberikan panduan sistematis dalam investigasi forensik digital untuk memastikan akurasi dan legalitas bukti yang dikumpulkan [8].

Berbagai penelitian terdahulu telah membahas teknik pemulihan data dan investigasi forensik digital dalam kasus pencurian dan penghapusan data di media penyimpanan. [9] membandingkan efektivitas EaseUS Data Recovery Wizard dan Recuva, di mana EaseUS lebih unggul dalam memulihkan file yang rusak atau terinfeksi virus, sementara Recuva sering menghasilkan data yang kurang terstruktur. [10] menguji lima aplikasi pemulihan data menggunakan metode National Institute of Standards and Technology (NIST) dalam skenario pencurian data melalui flash disk dan menemukan bahwa Autopsy memiliki tingkat keberhasilan lebih tinggi dibandingkan dengan Recuva, Puran, EaseUS, dan Stellar.

Sementara itu, [11] menerapkan metode National Institute of Justice (NIJ) untuk menganalisis pemulihan file yang telah dihapus, di mana Autopsy terbukti lebih efektif dibandingkan Belkasoft Evidence Center, terutama dalam mengembalikan file digital penting seperti dokumen dan gambar.

Penelitian lain oleh [12] juga menggunakan metode NIST dan menemukan bahwa FTK Imager lebih cepat dalam analisis, sementara Autopsy lebih unggul untuk investigasi yang membutuhkan kedalaman analisis lebih lanjut.

Selain itu, [13] meneliti pemulihan data pada smartphone dengan metode NIJ dan menemukan bahwa EaseUS Data Recovery berhasil mengembalikan 100% data yang dihapus, lebih baik dibandingkan Wondershare Dr. Fone yang hanya mencapai tingkat keberhasilan 63%. Temuan dari berbagai penelitian ini memperkuat pentingnya penerapan metode NIJ dan NIST dalam investigasi forensik digital, khususnya dalam mendeteksi serta memulihkan bukti digital yang berkaitan dengan manipulasi dan penghapusan data dalam kasus korupsi dana BOS.

Penelitian ini bertujuan untuk mengidentifikasi dan mengumpulkan bukti digital dalam kasus korupsi, menganalisis serta memulihkan data dari perangkat pemyimpanan portable flash disk, serta mengeksplorasi penggunaan steganografi dalam penyembunyian bukti dengan menerapkan framework NIJ dan tools forensik.

2. TINJAUAN PUSTAKA

2.1. Digital Forensik

Digital forensik merupakan bagian dari ilmu forensik yang secara khusus menangani investigasi, analisis, serta pemulihan berbagai bukti yang berhubungan dengan pelanggaran hukum atau tindakan kriminal yang melibatkan perangkat atau media digital. Bidang ini melibatkan beragam teknik dan metode untuk mengenali, mengumpulkan, menganalisis, serta menjaga keutuhan bukti digital agar dapat digunakan secara sah dalam proses peradilan [14].

2.2. Steganografi

Steganografi adalah bentuk seni yang mengekstrak data atau informasi dari media digital untuk mencegah akses yang tidak sah dan menjaga kerahasiaan. Penggunaan steganografi dapat berdampak signifikan pada analisis forensik digital. Ini melibatkan penggunaan inspeksi visual atau analisis forensik digital tradisional. Analisis forensik harus menggunakan berbagai teknik steganografi untuk mengekstrak data. Saat menggunakan steganografi untuk mengekstrak data digital, prosesnya menjadi lebih rumit. Kemampuan untuk mengekstrak data melalui steganografi meningkatkan potensi untuk

mengekstrak data digital menggunakan metode ini. Namun, ini juga dapat membatasi privasi data [15].

2.3. *Recovery Data*

Pemulihan data adalah proses mengambil kembali data yang hilang, terhapus, atau tidak dapat diakses. Hal ini dapat dilakukan untuk memulihkan file penting guna menyelidiki tindak kejahatan, atau menganalisis bukti digital. Teknik pemulihan umum mencakup pemindaian untuk menemukan sisa-sisa file yang dihapus, memulihkan data dari metadata sistem file, dan menggunakan alat perambah data untuk mengekstrak data mentah. Keberhasilan pemulihan data bergantung pada faktor-faktor seperti media penyimpanan, jenis kehilangan data, dan teknik yang digunakan. Tujuan utama pemulihan data adalah mengambil kembali informasi yang berguna dari sumber data digital yang rusak, terhapus, atau tidak dapat diakses [16].

2.4. *Eraser*

Eraser adalah alat penghapusan data yang menghapus data secara permanen dari media penyimpanan elektronik. Berbeda dengan penghapusan biasa yang hanya menghapus referensi file, penghapusan data menggunakan algoritma untuk menimpa data berkali-kali untuk memastikan data tidak dapat dipulihkan [17].

Keunggulan utama data eraser adalah dapat diverifikasi dan memberikan jaminan bahwa data sensitif telah benar-benar dihapus secara permanen [18].

Eraser menggunakan berbagai standar seperti metode US DoD 5220.22-M untuk menimpa data 3-7 kali, sehingga pemulihan menjadi tidak mungkin. Pada metode dasarnya (3 pass) menimpa data dengan angka nol (0x00), lalu angka satu (0xFF), dan data acak, sementara versi 7 pass yang lebih aman menambahkan 4 pass verifikasi tambahan. Eraser dapat digunakan untuk menghapus secara aman seluruh drive atau file/folder tertentu, membantu memastikan kepatuhan terhadap peraturan perlindungan data dengan menghapus data secara permanen.

2.5. *Recuva*

Recuva adalah salah satu alat forensik digital yang dikembangkan oleh Piriform Ltd untuk memulihkan file yang terhapus dari media penyimpanan yang terhubung melalui USB [19].

Recuva dapat memindai dan mendeteksi data yang hilang pada flash drive, hard drive eksternal, dan perangkat penyimpanan lainnya. Perangkat lunak ini menggunakan algoritma pemindaian canggih untuk menganalisis struktur sistem file dan dapat memulihkan data dari berbagai media penyimpanan, termasuk NTFS, FAT, dan exFAT [20].

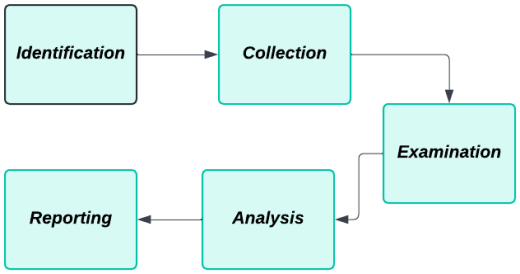
Keunggulan Recuva adalah antarmuka yang mudah dipahami, kemampuan menampilkan pratinjau file sebelum dipulihkan, dan indikator status pemulihan [21].

3. METODE PENELITIAN

3.1. Metode National Institute Of Justice

Tahapan penelitian yang dilakukan menggunakan pendekatan metodologi teknik statik forensik berdasarkan acuan NIJ (Natinal Institute of Justice). Framework National Institute of Justice (NIJ) digunakan sebagai panduan dalam melakukan investigasi forensik karena menyediakan langkah-langkah yang sistematis dan terstruktur [22].

Hal ini penting dilakukan mengingat tujuan utama dari digital forensik adalah untuk mengumpulkan bukti yang dapat diterima di pengadilan dan mengidentifikasi pelaku kejahatan.



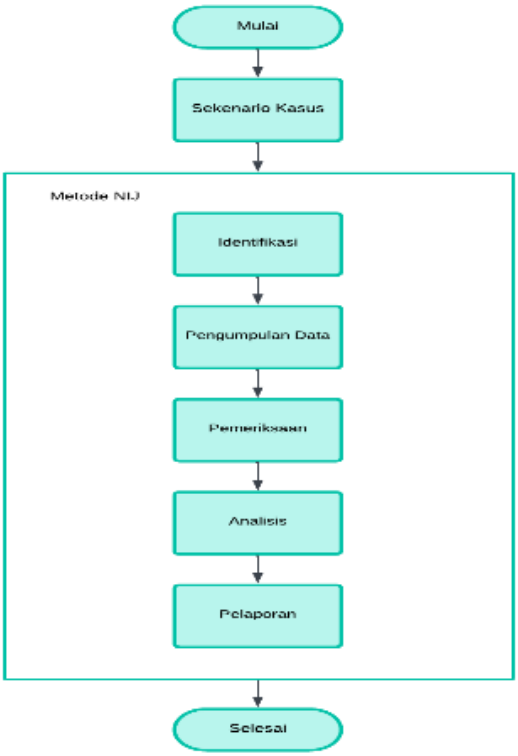
Gambar 1. Tahapan metode NIJ

Framework NIJ membantu investigator dalam memastikan setiap tahapan proses forensik terdokumentasi dengan baik dan menjaga integritas bukti digital yang ditemukan. Tahapan menggunakan metode NIJ terbagi menjadi lima yaitu, *identification, collection, examination, analysis, dan reporting.*

a. Tahap pertama adalah *identification*, yaitu mempersiapkan tim untuk melakukan investigasi.
b. Menemukan file dan membuat salinan dari objek fisik yang menyimpan bukti digital merupakan langkah kedua yaitu *collection* dalam proses pengumpulan dan akuisisi.
c. Setelah itu, langkah ketiga adalah *examination*. Bukti digital yang dikumpulkan dianalisis baik secara manual maupun otomatis.
d. Tahap keempat adalah *analysis*; pada tahap ini, bukti digital yang ditemukan selama penyelidikan diperiksa secara mendalam, dan analisis dilakukan untuk mencari bukti yang kuat.
e. *Reporting* adalah tahap kelima. Laporan ini berisi hasil analisis dari proses investigasi, deskripsi alat yang digunakan, penjelasan metode penyelidikan, serta tindakan lanjutan setelah analisis terhadap bukti digital yang diperoleh.

3.2. Tahapan Penelitian

Penelitian ini melibatkan beberapa tahapan yang saling terkait untuk memastikan bahwa proses pemulihan bukti kejahatan pada USB dilakukan secara sistematis, seperti yang ditunjukkan pada Gambar 2 di bawah:



Gambar 2. Flowchart tahapan penelitian

Berikut adalah langkah-langkah yang diambil dalam penelitian ini:

a. Mulai
Pada tahap awal, peneliti melakukan persiapan dengan menetapkan tujuan dan cakupan penelitian. Fokus dari penelitian ini adalah pada pemulihan bukti digital yang relevan dengan tindak kejahatan, khususnya data yang terdapat atau pernah tersimpan di perangkat flashdisk.

b. Skenario Kasus
Peneliti merumuskan skenario kasus untuk memberikan konteks pada penyelidikan. Misalnya, kasus ini mungkin melibatkan dugaan adanya data penting yang sengaja dihapus atau disembunyikan pada flashdisk untuk mengaburkan jejak kejahatan. Skenario ini membantu dalam menentukan jenis data dan teknik recovery yang perlu diterapkan.

c. Identifikasi
Tahapan identifikasi bertujuan untuk menemukan elemen-elemen penting yang perlu dianalisis dalam flashdisk. Di sini, peneliti menentukan jenis bukti yang mungkin terkait dengan kasus, seperti file yang dihapus, dokumen tersembunyi, atau jejak aktivitas yang dapat dijadikan bukti.

d. Pengumpulan Data
Setelah mengidentifikasi elemen penting, peneliti mulai melakukan pengumpulan data dari perangkat flashdisk. Pengumpulan data ini dilakukan menggunakan perangkat lunak forensik untuk menyalin atau meng-clone isi flashdisk secara menyeluruh tanpa mengubah informasi asli. Data yang dikumpulkan termasuk file yang mungkin masih tersimpan, serta data yang sudah dihapus namun dapat dipulihkan.

e. Pemeriksaan
Pada tahap pemeriksaan, peneliti mengecek integritas dan validitas data yang berhasil dikumpulkan. Pemeriksaan ini melibatkan verifikasi bahwa data tersebut benar-benar sesuai dengan yang ada di flashdisk dan belum mengalami perubahan. Selain itu, peneliti juga mencari file tersembunyi atau data yang dienkripsi, karena file semacam itu sering kali mengandung informasi penting yang mungkin disembunyikan dengan sengaja.

f. Analisis
Dalam tahap ini, data yang berhasil dipulihkan dari flashdisk dieksplorasi lebih lanjut. Sebagian data yang ditemukan tidak dapat langsung dianalisis karena berada dalam bentuk terenkripsi atau tersembunyi. Peneliti kemudian melakukan proses ekstraksi untuk membuka atau mendekripsi data tersebut. Dengan menggunakan teknik dekripsi dan alat forensik khusus, peneliti mencoba mengakses isi sebenarnya dari data terenkripsi tersebut. Setelah data berhasil diekstraksi, analisis dilanjutkan untuk mencari pola, metadata, atau informasi penting lainnya yang mendukung skenario kasus.

g. Pelaporan
Hasil analisis dan seluruh proses investigasi disusun dalam bentuk laporan forensik yang sistematis. Laporan ini memuat detail proses pemulihan, metode ekstraksi, serta temuan-temuan penting yang relevan dengan kasus. Laporan akhir ini diharapkan dapat digunakan sebagai bukti yang sahih dalam penyelidikan lebih lanjut atau di pengadilan.

h. Selesai
Setelah semua tahapan selesai, penelitian dinyatakan selesai. Laporan forensik yang lengkap disiapkan dan siap untuk dipresentasikan atau dipublikasikan, sehingga dapat menjadi referensi dalam kasus serupa atau sebagai bukti dalam proses hukum.

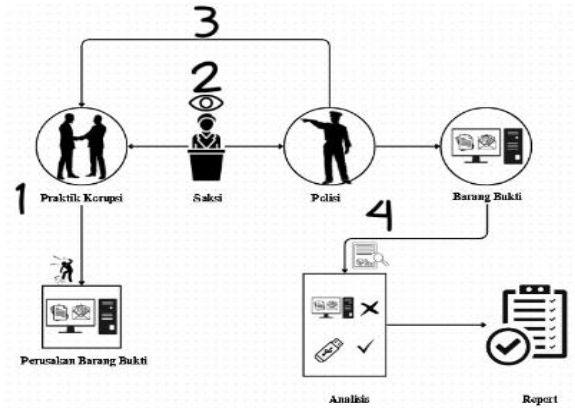
3.3. Kebutuhan *Hardware* dan *Software*

Guna mendukung jalannya proses dalam investigasi kasus kejahatan forensik digital, diperlukan alat bantu berupa perangkat keras dan perangkat lunak:

Tabel 1. Alat dan bahan

No	Nama	Keterangan
1	Laptop Acer Aspire 4752	Windows 10, 64 Bit, 8 GB RAM
2	Flashdisk 16 GB	Objek Penelitian
3	Tools Recuva, Eraser, dan Steghide	Tools

3.4. Skenario Kasus



Gambar 3. Skenario kasus

Untuk memperjelas sekaligus merekonstruksi kejadian yang melibatkan pelaku, saksi, dan korban, diperlukan penyusunan skenario kasus yang detail. Dalam penelitian ini, penulis akan memanfaatkan tools forensik digital dan menganalisis tingkat efektivitas alat tersebut dalam proses investigasi. Berikut skenario kasus yang digunakan:

a. Seorang oknum kepala sekolah bersekongkol dengan beberapa oknum guru untuk mengalihkan sebagian dana bos ke rekening pribadi. Pelaku kemudian mencoba menghilangkan barang bukti yang berupa file yang berisi nama oknum guru, jumlah transfer, dan bukti transfer ke rekening pribadi dengan cara memanfaatkan teknik steganografi untuk menyisipkan file tersebut ke dalam gambar biasa. Kemudian gambar yang telah di manipulasi di pindahkan ke flasdisk dari komputer sekolah.
b. Saksi mata yang juga rekan guru mengetahui tentang penyalahgunaan dana bos tersebut yang kemudian melaporkannya ke pihak berwajib.
c. Pihak berwajib melakukan penggledeahan terhadap kepala sekolah dan beberapa oknum guru, dan di dapatkan barang bukti berupa komputer dan flasdisk.
d. Barang bukti yang di dapatkan kemudian di analisis dan di dapatkan bukti file yang terstegano di dalam file gambar. Kemudian hasil temuan yang di dapat di laporkan untuk memperkuat hasil hukum.

4. HASIL DAN PEMBAHASAN

4.1. *Identification*

Dalam tahap identifikasi, persiapan tim investigasi menjadi langkah awal yang penting, melibatkan beberapa ahli forensik digital untuk memastikan bahwa proses akuisisi barang bukti digital pada flashdisk sesuai dengan framework National Institute of Justice (NIJ). Pada tahap ini juga menyiapkan peralatan yang digunakan selama tahap investigasi untuk mengumpulkan semua bukti, seperti flash drive yang ada untuk memastikan bahwa bukti tersebut asli. Ini dilakukan agar penyidik lebih mudah menyelesaikan kasus.

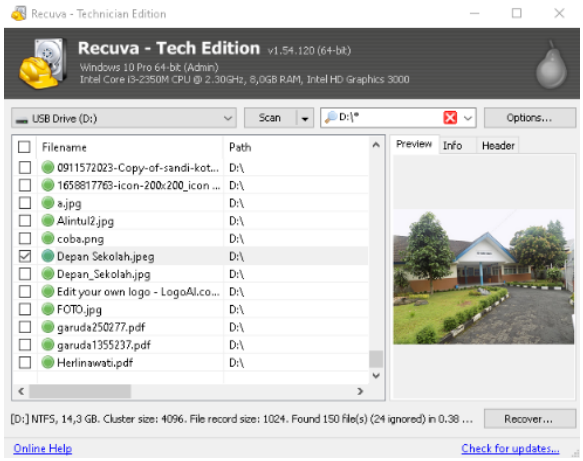
4.2. *Collection*

Pada tahap pengumpulan data (collection), dilakukan pemeriksaan terhadap barang bukti yang dikumpulkan untuk proses penyelidikan, termasuk jenis barang bukti,spesifikasi dan informasi lainnya.

Gambar 4. Barang bukti

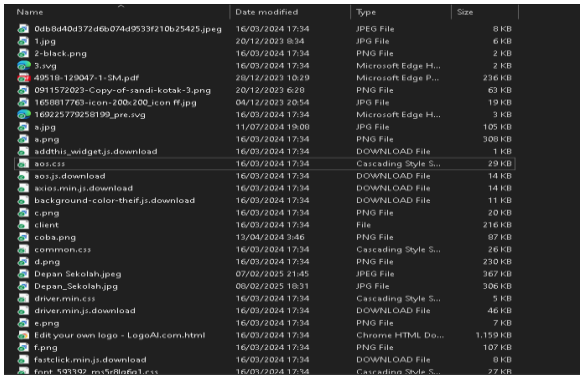
4.3. *Examination*

Dalam tahap pemeriksaan (examination) dilakukan akses terhadap isi flashdisk dan proses pemulihan data dilakukan untuk memastikan bahwa tidak ada informasi yang terhapus atau disembunyikan secara sengaja.



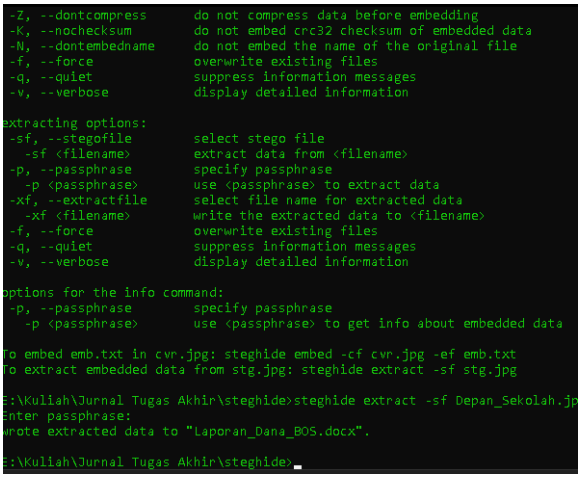
Gambar 5. Proses recovery flashdisk

Gambar 5 menampilkan proses pemulihan data yang dilakukan menggunakan tools Recuva. Dalam proses ini, Recuva digunakan untuk memindai sektor penyimpanan guna mendeteksi file yang masih dapat dipulihkan, baik yang telah dihapus secara sengaja maupun akibat kerusakan sistem. Selain itu, perangkat lunak ini memungkinkan identifikasi berbagai jenis file, termasuk dokumen, gambar, dan arsip, yang berpotensi memiliki keterkaitan dengan investigasi.



Gambar 6. Hasil recovery

Setelah proses pemulihan data selesai dilakukan, sejumlah file berhasil dipulihkan dari perangkat penyimpanan. Di antara file-file tersebut, terdapat beberapa yang mencurigakan dan berpotensi memiliki keterkaitan dengan investigasi yang sedang berlangsung. Salah satu file yang menimbulkan kecurigaan adalah "Depan_Sekolah.jpg", yang perlu dianalisis lebih lanjut untuk memastikan apakah terdapat informasi tersembunyi di dalamnya. Selain itu, pemeriksaan metadata dan kemungkinan penerapan teknik steganografi atau enkripsi pada file-file tersebut menjadi langkah penting dalam mengungkap potensi penyalahgunaan data.

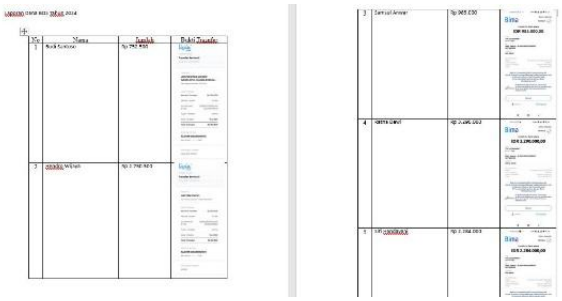


Gambar 7. Hasil ekstrak steganografi

Gambar 7 menunjukkan proses pengecekan file tersembunyi pada Depan_Sekolah.jpg dengan menggunakan tool Steghide. Dalam proses ini, dilakukan ekstraksi terhadap file tersebut, yang kemudian menghasilkan Laporan_dana_BOS.docx. File hasil ekstraksi ini memerlukan pemeriksaan lebih lanjut untuk mengidentifikasi isi serta kemungkinan adanya manipulasi atau informasi tersembunyi lainnya.

4.4. *Analysis*

Analisis terhadap file "Laporan_Dana_BOS.docx" yang berhasil diekstrak mengungkap informasi yang berpotensi menjadi bukti dalam penyelidikan lebih lanjut. Dokumen tersebut berisi daftar lengkap nama-nama penerima dana BOS, termasuk rincian jumlah dana yang ditransfer ke masing-masing penerima yang menjadi indikasi pengalihan dana ke rekening yang tidak terkait dengan institusi pendidikan. Temuan ini menunjukkan adanya penyalahgunaan dana BOS yang perlu dianalisis lebih lanjut untuk memastikan transparansi dan akuntabilitas dalam pengelolaannya.



Gambar 8. Isi dokumen Laporan_Dana_BOS.docx

Analisis lebih lanjut terhadap file "Depan_Sekolah.jpg" menggunakan tool Steghide mengungkapkan adanya file tersembunyi "Laporan_dana_BOS". Proses ekstraksi berhasil dilakukan tanpa kerusakan data, mengindikasikan penggunaan teknik steganografi LSB (Least Significant Bit) yang sophisticated. Penelitian [23] menunjukkan bahwa teknik steganografi LSB memungkinkan penyembunyian data hingga 10% dari ukuran file pembawa tanpa perubahan visual yang signifikan. Dalam kasus ini, pelaku memanfaatkan teknik tersebut untuk menyembunyikan dokumen sensitif yang berisi daftar transfer dana BOS ke rekening pribadi.

4.5. *Reporting*

Laporan ini menyajikan hasil investigasi forensik digital yang telah dilakukan terhadap barang bukti berupa flashdisk 16GB menggunakan framework National Institute of Justice (NIJ). Proses investigasi dimulai dengan melakukan recovery data menggunakan tools Recuva, yang berhasil memulihkan sejumlah file yang sebelumnya terhapus dari flashdisk tersebut. Di antara file-file yang berhasil dipulihkan, ditemukan sebuah file gambar bernama "Depan_Sekolah.jpg" yang mencurigakan. Analisis lebih lanjut menggunakan tool steganografi Steghide berhasil mengungkap bahwa file gambar tersebut menyembunyikan sebuah dokumen Word bernama "Laporan_dana_BOS.docx". Proses ekstraksi berhasil dilakukan tanpa ada kerusakan pada file, menunjukkan penggunaan teknik steganografi yang cukup sophisticated untuk menyembunyikan informasi sensitive.

Tabel 2. Temuan file

Aspek	Detail
Nama File Pembawa	Depan_Sekolah.jpg
File Tersembunyi	Laporan_dana_BOS.docx
Metode Penyembunyian	Steganografi LSB

Dokumen yang berhasil diekstrak mengandung informasi kritis terkait penyalahgunaan dana BOS, termasuk daftar nama-nama penerima transfer dan jumlah dana yang dialihkan ke rekening pribadi. Temuan ini mengindikasikan adanya upaya sistematis untuk mengalihkan dana BOS melalui serangkaian transfer yang tidak sesuai dengan prosedur standar pengelolaan keuangan sekolah.

Tabel 3. Temuan bukti

Kategori	Temuan
Jenis Pelanggaran	Pengalihan dana BOS
Modus Operasi	Transfer ke rekening pribadi
Bukti Digital	Dokumen transfer dan daftar penerima

Berdasarkan hasil investigasi, dapat disimpulkan bahwa telah terjadi upaya terencana untuk menyalahgunakan dana BOS dengan memanfaatkan teknologi digital untuk menyembunyikan bukti. Metodologi yang digunakan dalam investigasi ini telah mengikuti standar forensik digital yang ketat, memastikan integritas dan validitas bukti yang ditemukan.

4.6. *Skenario Percobaan Multiple Recovery*

Untuk memvalidasi efektivitas metode recovery dan ekstraksi data, dilakukan serangkaian percobaan dengan berbagai skenario. Percobaan dilakukan sebanyak lima kali dengan kondisi yang berbeda untuk menguji konsistensi dan reliabilitas metode yang digunakan.

Tabel 4. Hasil Percobaan Multiple Recovery

No	Skenario	Metode Penghapusan	Tingkat Keberhasilan Recovery	Kualitas Data
1	Penghapusan Standard	Delete Manual	95%	Sempurna
2	Penghapusan dengan Eraser (1 pass)	Secure Delete	78%	Baik
3	Penghapusan dengan Eraser (3 pass)	DOD Standard	45%	Moderate
4	Format Quick	Format Standar	89%	Baik
5	Format Full	Format Low Level	32%	Poor

Hasil percobaan menunjukkan bahwa efektivitas recovery data sangat bergantung pada metode penghapusan yang digunakan. Penelitian [24] mengkonfirmasi bahwa penggunaan software secure deletion seperti Eraser dengan multiple passes dapat secara signifikan mengurangi kemungkinan pemulihan data. Namun, dalam kasus ini, tim investigasi berhasil memulihkan file target karena pelaku hanya menggunakan metode penghapusan standar.

5. KESIMPULAN DAN SARAN

Penelitian ini mendemonstrasikan keefektifan framework National Institute of Justice (NIJ) dalam proses akuisisi dan analisis barang bukti digital pada media penyimpanan flashdisk. Melalui implementasi tahapan-tahapan framework NIJ yang meliputi identification, collection, examination, analysis, dan reporting, investigasi berhasil mengungkap kasus penyalahgunaan dana BOS yang disembunyikan menggunakan teknik steganografi. Proses recovery data menggunakan tool Recuva berhasil memulihkan file-file yang telah dihapus, termasuk file "Depan_Sekolah.jpg" yang kemudian dianalisis menggunakan Steghide dan mengungkap dokumen tersembunyi "Laporan_dana_BOS.docx". Hasil pengujian multiple recovery menunjukkan variasi tingkat keberhasilan yang signifikan tergantung pada metode penghapusan yang digunakan, dengan tingkat keberhasilan tertinggi mencapai 95% pada penghapusan standar, sementara format low level hanya mencapai 32% dengan kualitas data yang rendah. Teknik steganografi LSB yang digunakan pelaku terbukti sophisticated namun masih dapat dideteksi dan diekstrak tanpa kerusakan data, membuktikan efektivitas tools forensik yang digunakan dalam investigasi. Dokumen yang berhasil diekstrak mengandung bukti-bukti kuat berupa daftar transfer dana BOS ke rekening pribadi, mengonfirmasi adanya upaya sistematis dalam penyalahgunaan dana pendidikan.

Pengembangan Metodologi dan Tools, Direkomendasikan untuk mengembangkan metodologi forensik yang lebih komprehensif dengan mengintegrasikan berbagai tools forensik terbaru. Penelitian selanjutnya sebaiknya mempertimbangkan penggunaan tools forensik yang lebih advanced untuk mengantisipasi teknik-teknik penyembunyian data yang lebih sophisticated, serta melakukan validasi silang dengan menggunakan multiple tools untuk meningkatkan akurasi temuan.

Peningkatan Keamanan Sistem Perlu adanya implementasi sistem keamanan yang lebih ketat dalam pengelolaan dana BOS, termasuk penggunaan sistem monitoring real-time, audit trail yang komprehensif, dan mekanisme verifikasi bertingkat untuk setiap transaksi keuangan. Institusi pendidikan sebaiknya menerapkan kebijakan yang lebih strict dalam hal manajemen dan pengawasan penggunaan media penyimpanan data yang berkaitan dengan informasi keuangan.

Pengembangan SOP Investigasi, Disarankan untuk mengembangkan Standard Operating Procedure (SOP) yang lebih detail dan terstandarisasi dalam penanganan kasus-kasus serupa, termasuk protokol untuk penanganan berbagai jenis media penyimpanan dan teknik steganografi. SOP ini harus mencakup prosedur untuk memastikan chain of custody dan integritas bukti digital selama proses investigasi.

Pelatihan dan Edukasi, Perlu diadakan program pelatihan berkala untuk tim investigasi forensik digital mengenai teknik-teknik terbaru dalam recovery data dan analisis steganografi. Selain itu, edukasi tentang keamanan digital dan manajemen data sensitif juga perlu diberikan kepada personel yang terlibat dalam pengelolaan dana BOS.

Penelitian Lanjutan, Direkomendasikan untuk melakukan penelitian lanjutan yang fokus pada

pengembangan metode deteksi dini untuk mencegah penyalahgunaan dana melalui teknik-teknik digital. Penelitian tersebut sebaiknya mencakup analisis pattern recognition untuk mengidentifikasi anomali dalam transaksi keuangan dan pengembangan sistem early warning untuk mencegah penyalahgunaan dana serupa di masa mendatang.

DAFTAR PUSTAKA

[1] D. S. Wibawa, M. Agustian, and M. T. Warmiyati, "Pendidikan Anti Korupsi sebagai Tindakan Preventif Perilaku Koruptif," *Muqoddima Jurnal Pemikiran dan Riset Sosiologi*, vol. 2, no. 1, pp. 1–18, Jun. 2021, doi: 10.47776/mjprs.002.01.01.

[2] D. R. Mauludi, "Bentuk Penanggulangan Tindak Pidana Korupsi Dana BOS Oleh Tenaga Kependidikan Di Lingkungan Sekolah Berdasarkan Perspektif Kriminologi," *Al Daulah : Jurnal Hukum Pidana dan Ketatanegaraan*, pp. 119–143, Jun. 2023, doi: 10.24252/ad.vi.38157.

[3] F. G. P. Zamsari and T. Wahyono, "Forensic Investigation of Digital Evidence on Flash Disk with Forensic Process Method Based on NIST," *Jurnal Ecotipe (Electronic, Control, Telecommunication, Information, and Power Engineering)*, vol. 11, no. 1, pp. 88–96, Apr. 2024, doi: 10.33019/jurnalecotipe.v11i1.4489.

[4] Siaulhak, S. Kasma, and Suparman, "Sistem Pengiriman File Menggunakan Steganografi Pengolahan Citra Digital Berbasis Matriks Laboratory," 2023.

[5] A. Kynan Pratama, C. Carudin, and D. Yusup, "Jurnal Sistem dan Teknologi Informasi Analisis Perbandingan Perangkat Lunak Forensik Digital untuk File Carving dalam Mengungkap Barang Bukti Digital," vol. 6, no. 2, 2021, [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

[6] R. Hidayat *et al.*, "The Comparative Study Analysis Logical Files Recovery And Low Level Files Recovery Using Digital Forensic Methods," vol. 5, no. 2, pp. 149–154, 2022, doi: 10.31943/teknokom.

[7] J. Matondang and I. Maulana, "Analisis Perbandingan Perangkat Lunak Forensik Digital File Carving Menggunakan NIST," *INNOVATIVE: Journal Of Social Science Research*, vol. 3, pp. 2154–2165, 2023.

[8] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ," *IT Journal Research and Development*, vol. 5, no. 2, pp. 118–134, Aug. 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.

[9] A. Putra and M. Donni Lesmana Siahaan, "Comparative Analysis Of Data Recovery Using Easeus Data Recovery Wizard And Recuva Applications", [Online]. Available: http://infor.seaninstitute.org/index.php/infokum/index

[10] D. Julian, A. Wijaya, T. Sutabri, and H. Artikel, "Perbandingan Kinerja Aplikasi Pengembalian Data Untuk Digital Forensik Dengan Metode National Institute of Standards and Technology," *Digital Transformation Technology (Digitech) | e*, vol. 3, no. 1, 2023, doi: 10.47709/digitech.v3i1.2727.

[11] R. N. Dasmen, A. Rahman, A. D. Putra, and M. Saputra, "Analisis Digital Forensik Recovery File yang Terhapus Menggunakan Tools Autopsy Dengan Metode National Institute Of Justice," *Jurnal Ilmiah Komputasi*, vol. 23, no. 2, Jun. 2024, doi: 10.32409/jikstik.23.2.3553.

[12] F. G. P. Zamsari and T. Wahyono, "Forensic Investigation of Digital Evidence on Flash Disk with Forensic Process Method Based on NIST," *Jurnal Ecotipe (Electronic, Control, Telecommunication, Information, and Power Engineering)*, vol. 11, no. 1, pp. 88–96, Apr. 2024, doi: 10.33019/jurnalecotipe.v11i1.4489.

[13] S. Marcellino, H. B. Seta, and W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute Of Justice (NIJ)," 2023.

[14] R. Novrianda Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial Digital Forensics Deleted Cyber Crime Evidence on Social Media Instant Messaging," 2021.

[15] A. U. Albab and D. Darmaji, "Pengamanan Pesan Menggunakan Kombinasi Kriptografi dan Steganografi Audio Berbasis Transformasi Wavelet Diskrit," J. Sains dan Seni ITS, vol. 11, no. 3, 2023, doi: 10.12962/j23373520.v11i3.81479.

[16] M. F. Abdillah, "Analisis Perbandingan Data Recovery Menggunakan Tools Forensik Berbasis Open Source Pada Linux," 2022.

[17] "Keamanan Data: Pengertian, Jenis, dan Tujuannya - Mekari Sign." Accessed: Oct. 30, 2024. [Online]. Available: https://mekarisign.com/id/blog/keamanan-data-adalah/

[18] "What is Data Erasure?" Accessed: Oct. 30, 2024. [Online]. Available: https://www.privacyengine.io/resources/glossary/data-erasure/

[19] V. Rajani, A. Maziar, K. N. M. Man, J. W. Hell, and Q. Yuan, "Age-dependent contributions of nmda receptors and l-type calcium channels to long-term depression in the piriform cortex," *Int J Mol Sci*, vol. 22, no. 24, 2021, doi: 10.3390/ijms222413551.

[20] P. Cronin, X. Gao, H. Wang, and C. Cotton, "Time-Print: Authenticating USB Flash Drives

with Novel Timing Fingerprints," *Proc IEEE Symp Secur Priv*, vol. 2022-May, pp. 1002–1017, 2022, doi: 10.1109/SP46214.2022.9833595.

[21] "Review Software Pemulihan Data Gratis Recuva [2022]." Accessed: Oct. 30, 2024. [Online]. Available: https://recoverit.wondershare.co.id/free-data-recovery/recuva-free-data-recovery-review.html

[22] R. A. Ramadhan and D. Mualfah, "Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh," *IT Journal Research and Development*, vol. 5, no. 2, pp. 183–192, 2020, doi: 10.25299/itjrd.2021.vol5(2).5750.

[23] M. Dalal and M. Juneja, "Steganography and Steganalysis (in digital forensics): a Cybersecurity guide," *Multimed. Tools Appl.*, vol. 80, no. 4, pp. 5723–5771, 2021, doi: 10.1007/s11042-020-09929-9.

[24] I. P. A. E. Pratama, "Computer Forensic using Photorec for Secure Data Recovery Between Storage Media : a Proof of Consept," *Int. J. Sci. Technol. Manag.*, 2020, [Online]. Available: hhttps://ijstm.inarah.co.id