Jurnal Informatika Terpadu

https://journal.nurulfikri.ac.id/index.php/JIT
ISSN ONLINE : 2460-8998

ANALISA KINERJA APLIKASI DIGITAL FORENSIK *AUTOPSY* UNTUK PENGEMBALIAN DATA MENGGUNAKAN METODE *NIST SP 800-86*

Dedek Julian[1], Tata Sutabri[2]

[1,2]Magister Teknik Informatika, Universitas Bina Darma
Palembang, Sumatera Selatan, Indonesia 30111
dedek.julian99@gmail.com, tata.sutabri@binadarma.ac.id

Abstract

One example of digital crime that often occurs is data theft, such as transaction information, and important company data. The thief will delete files to remove traces so that it is necessary to search for and restore data that has been deleted to be used as digital evidence. This activity is usually called digital. forensics. Paid digital forensic applications are sold at quite expensive prices, so one alternative is Autopsy, which is an open source based investigation application that can restore data. This research aims to analyze the performance of the autopsy application in returning 70 files including documents, videos and images as digital evidence based on the crime case scenario of data theft with formatted flash disks. NIST SP 800-86 was chosen as the research method because it has simple stages and is in accordance with the research theme. The stages in this method start from collecting evidence, analyzing the contents of the flash disk with the autopsy application, searching for and returning the found files, to validating the files with hash compare. The analysis report shows that the autopsy application succeeded in returning 81.42% of the data that had been deleted and could be used as evidence based on the crime case scenario that had been created. The files that were successfully returned were 10 DOCX, 10 XLSX, 10 PDF, 6 TXT, 1 MP3, 10 MP4, and 10 PNG.

Keywords: *Autopsy, Cyber Digital, Digital Proof, Forensics, NIST*

Abstrak

Salah satu kasus kejahatan digital yang kerap terjadi adalah pencurian data, seperti informasi transaksi, hingga data penting milik perusahaan, pelaku pencurian akan menghapus berkas untuk menghilangkan jejak sehingga perlu dilakukan pencarian dan pengembalian data yang telah dihapus untuk dijadikan bukti digital, kegiatan ini biasa disebut digital forensik. Aplikasi digital forensik berbayar dijual dengan harga yang cukup mahal, sehingga salah satu alternatifnya adalah *autopsy*, yang merupakan aplikasi investigasi berbasis *open source* dan dapat melakukan pengembalian data. Penelitian ini bertujuan untuk menganalisis kinerja aplikasi *autopsy* dalam melakukan pengembalian 70 berkas dengan jenis dokumen, video dan gambar sebagai bukti digital berdasarkan pada skenario kasus kejahatan pencurian data dengan *flashdisk* yang telah diformat. *NIST SP 800-86* dipilih sebagai metode penelitian karena memiliki tahapan yang sederhana dan sesuai dengan tema penelitian, tahapan dalam metode tersebut dimulai dari pengumpulan barang bukti, melakukan analisa isi *flashdisk* dengan aplikasi *autopsy*, mencari dan mengembalikan berkas temuan, hingga memvalidasi berkas dengan *hash compare*. Laporan hasil analisis menunjukkan bahwa aplikasi *autopsy* berhasil mengembalikan sebanyak 81,42% dari data yang telah dihapus dan dapat dijadikan bukti berdasarkan skenario kasus kejahatan yang telah dibuat, berkas yang berhasil dikembalikan yaitu 10 *DOCX*, 10 *XLSX*, 10 *PDF*, 6 *TXT*, 1 *MP3*, 10 *MP4*, dan 10 *PNG*.

Kata kunci: *Autopsy*, Bukti Digital, Forensik, Kejahatan Digital, NIST

1. PENDAHULUAN

Era teknologi informasi membawa banyak perubahan, diantaranya merupakan dampak baik yaitu kemudahan serta kenyamanan untuk terus produktif dengan memanfaatkan teknologi. Namun tak dapat dipungkiri bahwa dampak negatif juga ikut bertumbuh, seperti kasus kejahatan digital atau *cyber crime*, yang merupakan tindak kejahatan dunia maya seperti pembajakan program komputer, kegiatan *cracking*, *carding*, penyebaran hal berbau pornografi, pembobolan bank, dan berbagai kejahatan yang lainnya [1]. *Cyber crime* sendiri semakin populer seiring dengan perkembangan teknologi, bahkan kerap kali dampak negatif tersebut terus dilakukan melalui berbagai cara yang tidak terduga. Untuk itu, diperlukan pengamanan teknologi

Diterima 26 Agustus 2023, Direvisi 14 September 2023, Diterima untuk publikasi 18 September 2023

informasi yang bertujuan untuk meyakinkan integritas, kelanjutan, dan kerahasiaan dari pengolahan data [2]. Sementara itu, setiap perusahaan mempunyai sistemnya masing-masing, sistem sendiri dapat diartikan sebagai jaringan kerja prosedur-prosedur yang saling berhubungan [3], salah satu sistem yang bergantung dengan teknologi biasa disebut sebagai sistem informasi, yang mengandung berbagai data untuk kepentingan perusahaan. Sehingga, hal-hal seperti mencuri data rahasia perusahaan juga dapat dikategorikan sebagai kasus kejahatan digital, karena melanggar aturan dari perusahaan, dan dapat merugikan perusahaan. Pencurian data yang dilakukan seorang kriminal dapat berupa identitas nasabah pada perusahaan perbankan [4], data tersebut digunakan untuk mengambil keuntungan pribadi pelaku, contoh kasus pencurian data lainnya seperti data konsumen dari anak perusahaan *Lion Air* yakni *Malindo Air* dan *Thai Lion Air* yang juga mengalami kebocoran sebanyak 21 juta data penumpang [5]. Pencurian data seperti ini dapat diantisipasi dengan meningkatkan keamanan sistem, dan apabila telah terjadi mesti dilakukan investigasi untuk mengusut pelaku kejahatan tersebut.

Dalam mengungkapkan kasus kejahatan digital, maka diperlukan bukti-bukti digital sebagai acuan di ranah hukum, sementara untuk menghindari kejahatan sejenis ini maka diperlukan tindakan seperti menjaga perangkat dalam mode isolasi [6]. Sebuah teknik yang menerapkan analisis dan penyidikan komputer sehingga memungkinkan seorang penyidik mendapatkan barang bukti digital dari komputer biasa disebut sebagai komputer forensik atau digital forensik [7]. Terdapat dua jenis teknik pengangkatan barang bukti atau forensik, yakni *dead forensic* yang membutuhkan data yang disimpan secara permanen dalam perangkat media penyimpanan, biasanya *harddisk*, dan *live forensic* melibatkan data berjalan pada sistem atau data volatile yang biasanya tersimpan pada *RAM* atau transit pada jaringan [8]. Analisis forensik akan memberikan detail untuk membantu para penyelidik dan lembaga investigasi memecahkan dan menghubungkan kasus-kasus dengan kejahatan yang dilaporkan. Salah satu kegiatan dalam digital forensik yang sering dilakukan adalah *file recovery* atau pemulihan file, yang mana berkas yang telah dihapus oleh pengguna dapat dikembalikan agar bisa diolah lebih lanjut, sebagaimana dijelaskan dalam penelitian [9] bahwa proses *delete*/menghapus suatu berkas bukan berarti menghilangkan data tersebut secara permanen dari media penyimpanan, akan tetapi kegiatan tersebut dapat diartikan sebagai pemberitahuan kepada komputer bahwa ruang yang ditempati data tersebut telah tersedia untuk ditimpa/diisi oleh data yang lain. Sehingga masih memungkinkan untuk dilakukan pengembalian berkas yang telah dihapus dari media penyimpanan meskipun telah diformat.

Untuk dapat melihat apakah berkas yang telah dipulihkan masih bersifat utuh dan merupakan berkas yang sama dengan file asli, maka perlu dilakukan suatu langkah validasi dengan cara mencocokkan *file hash* dari berkas yang asli dengan berkas yang telah dipulihkan. Hingga saat ini, salah satu algoritma *hash* yang paling populer adalah *Message-Digest 5* atau *MD5*, yang merupakan suatu fungsi *hash* kriptografi dan digunakan untuk melakukan pemeriksaan integritas *file* dalam berbagai situasi [10]. Untuk menjalankan aktivitas validasi *hash* tersebut dapat dilakukan dengan memanfaatkan penggunaan aplikasi *hash compare* dari *securityxploded*. Komparasi *hash* ini akan dijalankan setelah semua berkas berhasil dipulihkan.

Salah satu metode yang umum digunakan untuk melakukan analisis forensik adalah metode dari NIST *(National Institute of Standards and Technology)*, yaitu *NIST SP 800-86*, NIST sendiri merupakan suatu lembaga yang mengembangkan standar, panduan, dan persyaratan minimum untuk menyediakan keamanan informasi yang cukup bagi tiap aset serta pihak yang mempunyai kemampuan 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 [11]. Salah satu penelitian yang menerapkan metode ini adalah [9], yang melakukan uji coba pengembalian data, dimana hasil tertinggi yang diperoleh yaitu 100% untuk 20 dokumen, dan 90% untuk berkas dengan tipe gambar. Penelitian lain seperti [6], juga menerapkan metode *NIST* untuk pengembalian data dengan hasil yaitu *FTK Imager* memperoleh nilai 100% dan *Autopsy* memperoleh nilai 70%. Sementara itu, penelitian yang dilakukan oleh Riadi, dkk. [12] menerapkan metode yang lain, yaitu *National Institute of Justice* dalam melakukan pengembalian data dari *SSD* yang di implementasi *shadow defender* dengan aplikasi *X-ways forensics*, keberhasilan restorasi *file* hanya 28,7%. Sementara penelitian lainnya [13] menerapkan metode yang sama dalam melakukan pengembalian data menggunakan aplikasi *MOBILedit, Wondershare dr Fone*, dan *Belkasoft* dengan salah satu kesimpulannya menyatakan bahwa aplikasi forensik yang digunakan tidak cukup baik untuk mengembalikan data gambar, video dan berkas dokumen. Metode *NIJ* menerapkan 5 tahapan penelitian, sementara metode *NIST SP 800-86,* menerapkan langkah yang lebih sederhana yaitu dalam 4 tahapan, sehingga metode *NIST SP 800-86* dipilih karena merupakan metode yang dikembangkan langsung oleh lembaga pengembang standar dan panduan teknologi terutama, metode tersebut juga dapat diterapkan dengan lebih sederhana hanya dalam 4 tahapan, lebih singkat dan cocok dengan tema penelitian seperti yang pernah diterapkan juga dalam penelitian-penelitian sebelumnya.

Selain pemilihan metode yang tepat, penggunaan aplikasi yang sesuai juga dapat mendukung jalannya proses pemulihan data dengan lebih baik, aplikasi yang dapat digunakan untuk melakukan analisis forensik dan pengembalian data juga beragam, mulai dari yang berbayar hingga yang bersifat *open source*, seperti *Autopsy*. Meskipun bersifat *open source*, kinerja dari *tools* ini dapat

bersaing dengan aplikasi lain yang sejenis dengan harga tinggi. Seperti jika digunakan untuk menggali aktivitas transaksi dompet digital, *autopsy* dapat mengungguli aplikasi *Belkasoft Evidence Center*, dengan temuan sebanyak 8 aktivitas transaksi, sementara *Belkasoft Evidence Center* dengan temuan sebanyak 7 aktivitas transaksi [14]. Pada penelitian sebelumnya yang telah dilakukan oleh [15], dilakukan perbandingan untuk mengukur kinerja dari 3 aplikasi forensik untuk pengembalian data dengan media *SSD* yaitu *Autopsy, Belkasoft, dan Testdisk*, hasil akhir penelitian menunjukkan bahwa *Persentase recovery TRIM disable* dengan menggunakan aplikasi *Autopsy* dan *Testdisk* adalah 100% sehingga dapat menemukan barang bukti dan menjaga integritas dari barang bukti tersebut. Pada penelitian tersebut dapat dilihat bahwa aplikasi *autopsy* mempunyai potensi yang baik terutama untuk kategori kegiatan *data recovery* dengan media *SSD*.

Untuk itu, penelitian ini akan melakukan analisa kinerja dari aplikasi *autopsy* dalam mencari dan mengembalikan data yang telah dihapus dari media penyimpanan berupa *flashdisk*. Instrumen penilaian akan dilakukan dengan melihat seberapa banyak *file* yang dapat dikembalikan dengan aplikasi tersebut dan dinyatakan identik oleh aplikasi *Hash Compare*. Dalam penelitian sebelumnya, seperti [9] dilakukan uji coba menggunakan *file type JPG, PNG, DOCX*, dan *PDF*, maka pada penelitian ini akan dilengkapi dengan total 70 berkas sebagai bahan uji coba, yaitu berkas dengan ekstensi *DOCX, XLSX, MP3, MP4, TXT, PDF* dan *PNG* masing-masing sebanyak 10 berkas. Penelitian juga akan dilakukan dengan menerapkan metode *NIST SP 800-86*.

2. METODE PENELITIAN

Metode yang digunakan untuk melakukan penelitian ini yaitu *National Institute of Standard and Technology (NIST) SP 800-86*, dengan tahapan dan skenario kasus kejahatan sebagai berikut:

2.1 Tahapan Penelitian

Tahapan dalam metode *NIST SP 800-86* dapat dilihat pada Gambar 1 berikut ini.

Gambar 1. Tahapan Metode *NIST 800-86*

Berdasarkan gambar di atas, metode ini akan melalui 4 langkah, yakni dimulai dari *collection, examination, analysis,* hingga *reporting* [16]. Dengan penjelasan lebih lanjut sebagai berikut:

a) *Collection*, tahapan koleksi ini disebut juga tahap persiapan, koleksi yang dimaksud merupakan pengumpulan barang bukti dan peralatan yang akan digunakan untuk mengumpulkan data digital, proses ini mengikuti langkah pengamanan integritas data. Dalam kasus ini, pengumpulan barang bukti dilakukan dengan mengumpulkan *flashdisk*.
b) *Examination*, yakni tahap pengambilan data atau penggalian artefak dalam rangka menemukan data pada barang bukti menggunakan aplikasi *autopsy*.
c) *Analysis*, merupakan tahapan analisa dan melakukan evaluasi terhadap data yang didapatkan pada tahapan sebelumnya.
d) *Reporting*, adalah tahapan terakhir dalam metode ini yaitu proses pelaporan hasil analisis dari tahapan-tahapan sebelumnya untuk diambil kesimpulan.

2.2 Skenario Kasus Kejahatan

Selanjutnya untuk memperjelas kondisi penelitian, dibuatlah suatu skenario kejahatan yang berkaitan dengan pencurian data perusahaan dan dengan menggunakan media penyimpanan berupa *flashdisk drive*, skenario kejahatan digital yang telah dirancang tersebut secara sederhana dapat dilihat seperti Gambar 2 di bawah ini.

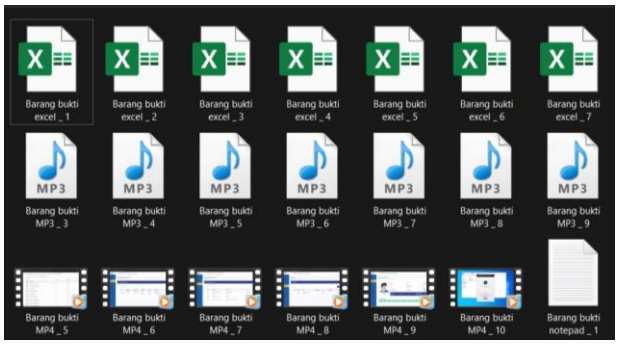
Gambar 2. Skenario Kasus Kejahatan

Tahapan-tahapan yang terjadi pada skenario tersebut secara lebih terperinci adalah sebagai berikut.

a) Pelaku masuk ke ruang atasan dan menggunakan komputer atasan tanpa seizin nya.
b) Pelaku kemudian menyalin data penting seperti foto, video, dokumen, dll. yang totalnya berjumlah 70 berkas dan dengan *file type* yaitu *png, docx, xlsx, pdf, txt, mp3, dan mp4.*
c) Pelaku tertangkap *CCTV* yang memperlihatkan aksinya masuk ke ruang atasan dengan membawa *flashdisk*.
d) Pelaku pun dicurigai telah mencuri data-data penting perusahaan yang ada di komputer atasan dengan melalui media *flashdisk*.
e) Setelah di wawancara, pelaku tidak mengatakan yang sebenarnya dan hanya berkata bahwa ia masuk ke ruangan untuk menemui atasan, tetapi karena tidak disana, ia kemudian hanya pergi.
f) *Investigator* kemudian memutuskan untuk mencari bukti dengan *flashdisk* tersebut, namun *flashdisk* yang diterima dalam kondisi telah diformat sehingga tidak ditemukan berkas apapun.
g) *Investigator* lalu melakukan akuisisi dan *recovery data* untuk melihat jejak data yg pernah disimpan oleh pelaku dan memastikan kebenaran yang ingin diungkap.

h) *Investigator* selanjutnya memastikan kembali bahwa data yang dikembalikan masih utuh dengan membandingkan *file hash* dari berkas yang telah di *recovery* dengan berkas asli yang masih disimpan.

Skenario kasus kejahatan tersebut hampir sama dengan skenario kasus kejahatan pada penelitian [6], yaitu pelaku melakukan penggelapan dana perusahaan dan menyimpan bukti transaksi pada *DVD-R*, sehingga *DVD-R* tersebut menjadi barang bukti untuk di investigasi. Berkas yang disiapkan untuk menjadi bukti digital pada *flashdisk* berupa 70 berkas, yaitu berkas dengan ekstensi *DOCX*, *XLSX*, *MP3*, *MP4*, *TXT*, *PDF* dan *PNG*. Dengan nama berkas masing-masing adalah Barang bukti *word*, Barang bukti *excel*, Barang bukti *mp3*, Barang bukti *mp4*, Barang bukti *notepad*, Barang bukti *PDF* dan Barang bukti *png* yang masing-masingnya terdapat 10 berkas, seperti yang dapat dilihat pada Gambar 3 di bawah ini.



Gambar 3. Data yang Disiapkan sebagai Barang Bukti

Filetype yang dipilih terdapat 7 tipe untuk melihat sejauh mana kinerja dari aplikasi *autopsy* dalam mengembalikan data dengan tipe berbeda-beda. Dan dimasukkan tipe yang belum di uji coba pada penelitian sebelumnya [9] seperti *TXT*, *XLSX*, dan *MP3*. Setelah semua data tersebut dimasukkan ke *flashdisk*, data tersebut kemudian dihapus dengan melakukan *format disk* langsung terhadap media *flashdisk* sebagai suatu percobaan dalam menghilangkan bukti atau jejak digital. Sehingga, instrumen penilaian adalah untuk melihat seberapa banyak *file* yang dapat dikembalikan dengan aplikasi tersebut.

3. HASIL DAN PEMBAHASAN

Dalam melakukan proses analisis forensik, diperlukan adanya alat bantu sehingga pekerjaan dapat dilakukan dengan lebih baik, maka digunakanlah beberapa alat yang berupa perangkat keras serta aplikasi yang berupa perangkat lunak, yaitu seperti dijelaskan pada Tabel 1 di bawah ini.

Tabel 1. Alat dan Bahan

Nama	Spesifikasi	Keterangan
Laptop	*Acer Swift X, Windows 11*	Perangkat Keras
Flashdisk	*Sandisk*, Kapasitas 16GB	Perangkat Keras
Autopsy	Aplikasi	Perangkat Lunak

3.1 *Collection*

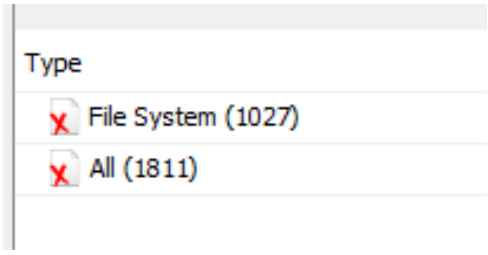
Barang bukti yang dikumpulkan pada tahapan ini yaitu perangkat *flashdisk* dengan merk *Sandisk Cruzer Blade CZ50 16GB*, dengan bentuk seperti pada Gambar 4 berikut.

Gambar 4. *Flashdisk* yang Digunakan

Sebelum menjalankan penelitian ini, kondisi *flashdisk* tersebut sebelumnya telah digunakan untuk kebutuhan sehari-hari yaitu dengan menyimpan berbagai macam berkas dalam berbagai jenis seperti video, musik, dokumen, dan lain sebagainya, sebelum akhirnya *flashdisk* tersebut digunakan untuk menyimpan berkas yang terkait dengan skenario kejahatan dalam penelitian ini

3.2 *Examination*

Untuk mendapatkan rekam jejak digital berupa berkas apa saja yang pernah disimpan ke dalam *flashdisk*, maka dilakukanlah proses akuisisi data dari perangkat *flashdisk* yang dilakukan dengan aplikasi *autopsy*, kegiatan tersebut memakan waktu yang cukup lama karena perlu menggali setiap data yang sebelumnya telah dihapus. Setelah proses selesai, aplikasi ini berhasil mendapatkan total 1811 data dan 1027 *file system* seperti pada Gambar 5 di bawah ini.

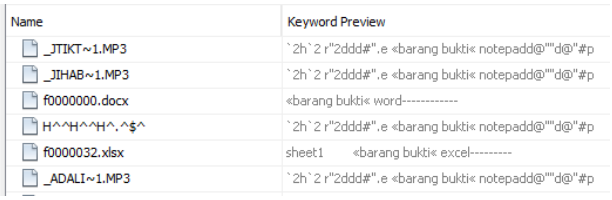


Gambar 5. Proses Akuisisi Data

Jika dikategorikan berdasarkan ekstensinya, ditemukan sebanyak 2118 berkas dengan jenis gambar, 17 berkas dengan jenis video, 353 dengan jenis audio, dan sebanyak 3 berkas dengan jenis arsip.

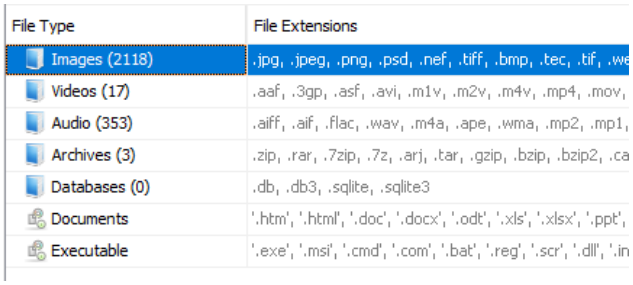
3.3 *Analysis*

Pada tahapan analisis dilakukan pencarian data berupa barang bukti, hal tersebut dapat dilakukan melalui pencarian dengan kata kunci atau dicari secara manual. Setelah dilakukan penelusuran, pencarian dengan kata kunci ‘barang bukti’ sesuai dengan nama berkas sebelum di format, dapat menampilkan beberapa berkas seperti yang dapat dilihat pada Gambar 6 berikut ini.



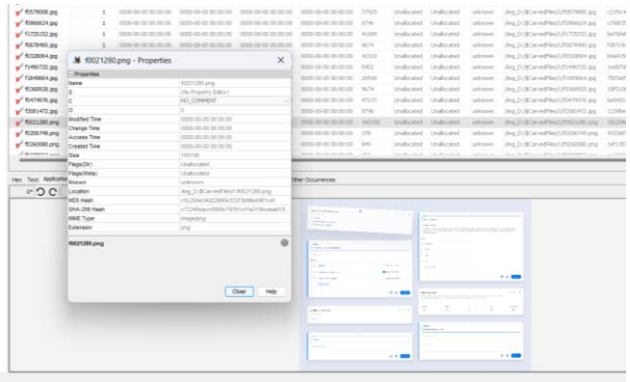
Gambar 6. Hasil Pencarian dengan Kata Kunci

Berkas yang ditemukan adalah berkas dengan ekstensi *docx*, *xlsx*, *txt* dan *mp3*. Berkas dengan ekstensi *docx*, dan *xlsx* dapat di temukan seluruhnya dan bisa di kembalikan dalam kondisi yang baik, sementara berkas dengan ekstensi *mp3* hanya ditemukan 1 berkas yang sesuai dan bisa dikembalikan dengan utuh. Berkas dengan ekstensi *txt* hanya ditemukan 6 berkas dan dapat dikembalikan secara utuh. *File* bukti dengan format lain yaitu *mp4*, *pdf*, dan *png* tidak ditemukan dengan metode ini, maka dilakukan metode pencarian manual yaitu dengan mencari berdasarkan tipe berkas. Melalui menu pencarian berdasarkan kategori seperti pada Gambar 7 di bawah.



Gambar 7. *Filter* Data berdasarkan Kategori

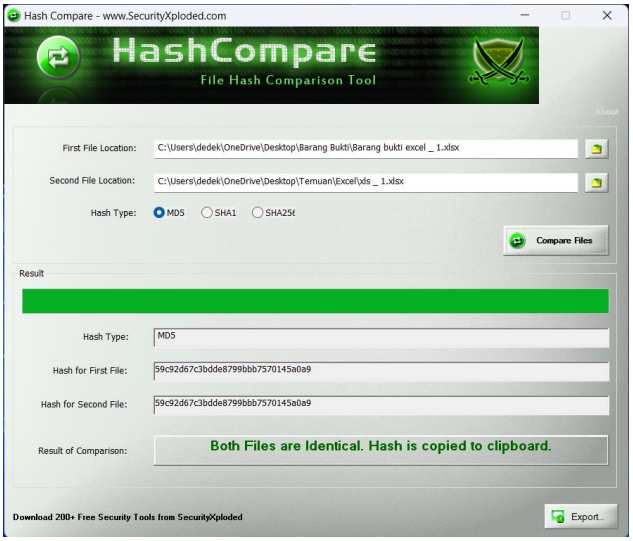
Untuk tipe berkas *MP4*, berhasil ditemukan dengan mudah karena hanya terdapat sedikit berkas dengan format *MP4* ketika diperiksa berdasarkan tipe berkas menggunakan menu *filter* kategori, selain dapat ditemukan, 10 berkas *MP4* yang dicari juga berhasil di-*recovery* dalam kondisi yang baik. 10 berkas dengan tipe PDF juga berhasil ditemukan dan dikembalikan melalui *filter Documents-PDF*. 10 berkas berjenis gambar dengan ekstensi *PNG* juga berhasil ditemukan dengan cara yang sama dan dapat di *recovery* dalam kondisi yang baik. Contohnya seperti pada Gambar 8 berikut ini.



Gambar 8. *File* bukti dengan Ekstensi PNG

Sementara itu, sisa berkas lainnya yang belum ditemukan seperti 4 berkas bukti dengan ekstensi *TXT*, dilakukan pencarian lebih lanjut dengan kata kunci '*barang bukti notepad*' sesuai dengan nama berkas sebelum dihapus, kata tersebut juga ada di dalam dokumen sehingga berkemungkinan ditemukan oleh aplikasi *autopsy*, pencarian dengan ekstensi menggunakan kata kunci *'*.txt'* juga tidak berhasil dalam menemukan berkas notepad dengan ekstensi *txt* ini. Hal tersebut bisa saja disebabkan karena terjadinya kerusakan pada *file* ketika dihapus sehingga aplikasi tidak dapat menemukan berkas tersebut. Hal tersebut juga dilakukan untuk berkas *MP3* yang hanya ditemukan 1 berkas saja.

Setelah selesai pada tahapan pencarian dan pengembalian data, selanjutnya dilakukan komparasi *file hash* dengan aplikasi *Hash Compare* seperti pada Gambar 9 berikut.



Gambar 9. Perbandingan *Hash* dengan aplikasi *Hash Compare*

Tahap ini merupakan tahapan validasi apakah berkas masih bersifat utuh dan sama dengan berkas asli barang bukti digital yang perlu ditemukan. *Hash compare* dijalankan dengan memilih opsi *MD-5 Hash*, hasil yang didapatkan memperlihatkan bahwa semua berkas dokumen *word*, *pdf* dan *excel* dengan ekstensi *DOCX*, *PDF* dan *XLSX*, ditemukan valid dan bersifat identik. 6 temuan berkas *notepad* ber-ekstensi *TXT* juga dinyatakan identik. Berkas media, yaitu 1 *MP3* dan 10 *MP4* juga ditemukan dalam kondisi utuh dengan keterangan bahwa berkas tersebut sama dengan berkas aslinya. 10 berkas gambar dengan format *PNG* juga berhasil dipulihkan dengan kondisi yang baik, dan dinyatakan valid sebagai berkas yang utuh dan sama dengan berkas aslinya. Dengan adanya validasi tersebut, maka temuan dapat dijadikan bukti digital untuk mengungkapkan kasus kejahatan seperti pada skenario yang dibuat.

3.4 *Reporting*

Setelah melalui semua tahapan analisis, maka didapatkan semua informasi yang telah diperoleh, informasi tersebut

kemudian dibuat dalam bentuk laporan. Tabel 2 berikut ini merupakan hasil pelaporan dari analisis forensik yang telah dilakukan.

Tabel 2. Hasil Tool *Autopsy*

Data	Ekstensi	Temuan	Komparasi Hash
Barang bukti *word*	*DOCX*	10 berkas	Semua berkas identik
Barang bukti *excel*	*XLSX*	10 berkas	Semua berkas identik
Barang bukti *mp3*	*MP3*	1 berkas	1 berkas identik
Barang bukti *mp4*	*MP4*	10 berkas	Semua berkas identik
Barang bukti *notepad*	*TXT*	6 berkas	6 berkas identik
Barang bukti *pdf*	*PDF*	10 berkas	Semua berkas identik
Barang bukti gambar	*PNG*	10 berkas	Semua berkas identik

Total temuan dalam penelitian adalah 57 berkas dari 70 berkas dalam skenario. Dan semua temuan telah divalidasi merupakan berkas yang sama dengan berkas aslinya, dengan temuan paling sedikit yaitu berkas dengan tipe *MP3* yang hanya berjumlah 1 berkas.

4. KESIMPULAN

Berdasarkan hasil akhir dari penelitian dengan skenario kasus kejahatan yang telah dibuat yaitu pencurian data melalui media *flashdisk drive*, penggunaan metode *NIST SP 800-86* dan aplikasi *autopsy* dapat diandalkan untuk melakukan analisis forensik khususnya untuk melakukan pemulihan atau pengembalian data, pada kasus ini aplikasi tersebut dapat membantu merestorasi 57 dari total 70 berkas berdasarkan skenario kasus kejahatan, sehingga kinerja aplikasi tersebut dinilai 81,42%, karena berhasil menemukan dan mengembalikan 10 berkas *DOCX*, 10 berkas *XLSX*, 10 berkas *PDF*, 6 berkas *TXT*, 1 berkas *MP3*, 10 berkas *MP4*, dan 10 berkas *PNG*. Dengan fitur yang cukup banyak dan sifat aplikasi yang berbasis *open source*, aplikasi *autopsy* mempunyai keunggulan tersendiri dibandingkan aplikasi lain yang sejenis, terutama pada harga aplikasi yang gratis dan dapat digunakan oleh siapa saja.

DAFTAR PUSTAKA

[1] Y. Bellini and T. Sutabri, "Sistem Pakar Mendeteksi Tindak Pidana Cyber Crime untuk Penanganan Komputer Forensik Menggunakan Backward Chaining," *JDTI*, vol. 6, no. 1, p. 42, Mar. 2023, doi: 10.32502/digital.v6i1.5619.

[2] T. Sutabri, *Konsep Sistem Informasi*. Andi, 2012. [Online]. Available: https://books.google.co.id/books?id=uI5eDwAAQBAJ

[3] T. Sutabri, *Analisis Sistem Informasi*. Andi, 2012. [Online]. Available: https://books.google.co.id/books?id=ro5eDwAAQBAJ

[4] N. Sulisrudatin, "Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit," *jihd*, vol. 9, no. 1, Jun. 2014, doi: 10.35968/jh.v9i1.296.

[5] E. F. Thalib and K. L. Maswari, "Perlindungan Hukum terhadap Data Pribadi Perusahaan Akibat Penyalahgunaan Data Digital Oleh Karyawan Perusahaan," *Prosiding Seminar Nasional FH UNMAS Denpasar : Urgensi dan Implikasi RUU Perlindungan Keamanan Kerahasiaan Data Diri Berbasis Digitalisasi*, vol. 1, no. 1, pp. 55–66, Oct. 2020.

[6] I. Riadi, A. Fadlil, and M. I. Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *RESTI*, vol. 4, no. 5, pp. 820–828, Oct. 2020, doi: 10.29207/resti.v4i5.2224.

[7] Y. Andi Putra and T. Sutabri, "Analisis Penyadapan pada Aplikasi Whatsapp Dengan Menggunakan Metode Sinkronisasi Data," *Blantika*, vol. 2, no. 1, pp. 11–20, Feb. 2023, doi: 10.57096/blantika.v2i1.8.

[8] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *ITJRD*, vol. 3, no. 1, pp. 13–21, Aug. 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[9] D. T. Yuwono, A. Fadlil, and S. Sunardi, "Performance Comparison of Forensic Software for Carving Files using NIST Method," *Jurnal Teknologi dan Sistem Komputer*, vol. 7, no. 3, pp. 89–92, Jul. 2019, doi: 10.14710/jtsiskom.7.3.2019.89-92.

[10] S. U. Lubis, "Implementasi Metode MD5 untuk Mendeteksi Orisinalitas File Audio," *KOMIK*, vol. 3, no. 1, Nov. 2019, doi: 10.30865/komik.v3i1.1620.

[11] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *JIUP*, vol. 5, no. 1, p. 89, Mar. 2020, doi: 10.32493/informatika.v5i1.4578.

[12] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ)," *ELINVO*, vol. 3, no. 1, pp. 70–82, Jul. 2018, doi: 10.21831/elinvo.v3i1.19308.

[13] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *JURTI*, vol. 3, no. 1, p. 87, Jun. 2019, doi: 10.30872/jurti.v3i1.2292.

[14] R. Umar, A. Yudhana, and M. N. Fadillah, "Perbandingan Tools Forensik Pada Aplikasi Dompet Digital," *JIKO*, vol. 6, no. 2, p. 242, Sep. 2022, doi: 10.26798/jiko.v6i2.621.

[15] W. Pranoto, I. Riadi, and Y. Prayudi, "Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics," *ITJRD*, vol. 4, no. 2, Feb. 2020, doi: 10.25299/itjrd.2020.vol4(2).4615.

[16] I. Riadi, Sunardi, and Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 7, no. 1, pp. 197–204, Jan. 2020, doi: 10.25126/jtiik.202071921.