Digital Transformation Technology (Digitech) | e-ISSN : 2807-9000
Volume 3, **Number** 1, Maret 2023
https://doi.org/10.47709/digitech.v3i1.2727

Perbandingan Kinerja Aplikasi Pengembalian Data Untuk Digital Forensik Dengan Metode National Institute of Standards and Technology

Dedek Julian[1*], Adi Wijaya[2], Tata Sutabri[3]
[1,2,3]Universitas Bina Darma, Indonesia
[1]dedek.julian99@gmail.com, [2]adiw1201@gmail.com, [3]tata.sutabri@binadarma.ac.id

Histori Artikel:
Diajukan: 15 Agustus 2023
Disetujui: 16 Agustus 2023
Dipublikasi: 17 Agustus 2023

Kata Kunci:
Pengembalian data; bukti digital; forensik; nist; kejahatan digital;

Abstrak
Kejahatan digital seperti pencurian data perusahaan dapat diantisipasi dengan meningkatkan keamanan sistem, sementara untuk kasus yang sudah terjadi, harus dilakukan analisis dan investigasi dalam mengungkapkan bukti-bukti kejahatan digital atau yang disebut sebagai digital forensik. Penelitian ini menguji coba 5 aplikasi pengembalian data untuk mendapatkan kembali bukti digital dari skenario kasus kejahatan pencurian data melalui flashdisk yang telah diformat, 5 aplikasi tersebut adalah autopsy, recuva, stellar, puran dan easus. Metode yang digunakan adalah metode National Institute of Standards and Technology (NIST), dengan tahapan dimulai dari collection, examination, analysis dan reporting. Tahapan tersebut dilaksanakan dengan barang bukti berupa flashdisk yang telah di isi 6 file sebagai bukti digital yang perlu dicari. Hasil akhir penelitian menunjukkan bahwa tools autopsy berhasil mengembalikan sebanyak 83% dari file yang di uji coba, sementara aplikasi recuva, puran dan easus sebanyak 66%, dan aplikasi stellar sebanyak 33%.

PENDAHULUAN

Menjadi lebih produktif dan merasakan kenyamanan penggunaan teknologi merupakan dampak positif yang dibawa oleh era teknologi. Namun disisi lain, dampak negatif yang dibawa oleh era teknologi juga terus ikut bertumbuh, contohnya adalah maraknya kasus kejahatan digital atau *cyber crime,* yang merupakan suatu tindak kejahatan dunia maya seperti misalnya pembajakan program, kegiatan *cracking*, *carding*, penyebaran konten dengan tema pornografi, pembobolan bank, dan berbagai kejahatan yang lainnya (Bellini and Sutabri 2023). *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 informasi yang bertujuan untuk meyakinkan integritas, kelanjutan, dan kerahasiaan dari pengolahan data (Sutabri 2012b). Dalam dunia korporat, masing-masing perusahaan mempunyai aturan dan sistem nya sendiri-sendiri, dimana sistem yang dimaksud dapat diartikan sebagai jaringan kerja prosedur-prosedur yang saling berhubungan (Sutabri 2012a), salah satu jenis sistem yang bergantung dengan teknologi biasa disebut sebagai sistem informasi, sistem informasi mengandung berbagai data untuk kepentingan perusahaan. Sehingga, melakukan hal-hal yang dapat merugikan perusahaan seperti seperti mencuri data rahasia perusahaan juga dapat dikategorikan sebagai suatu tindak kejahatan digital, karena melanggar aturan dari perusahaan tersebut, dan dapat merugikan perusahaan.

Pencurian data sendiri dapat berupa berbagai macam hal seperti misalnya pencurian identitas nasabah pada perusahaan perbankan (Sulisrudatin 2014), 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 (Thalib and Maswari 2021). Pencurian data seperti ini dapat dicegah dengan meningkatkan keamanan dari sistem perusahaan, dan apabila telah terjadi mesti dilakukan investigasi untuk mengusut pelaku kejahatan tersebut. Dalam mengungkapkan kasus kejahatan digital, maka diperlukan bukti-bukti digital sebagai acuan diranah hukum, sementara untuk menghindari kejahatan sejenis ini maka diperlukan tindakan seperti menjaga perangkat dalam mode isolasi (Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia 2020).

Terdapat suatu teknik yang menerapkan analisis dan penyidikan komputer sehingga memungkinkan seorang penyidik mendapatkan barang bukti digital dari komputer, teknik tersebut biasa disebut sebagai komputer forensik atau digital forensik (Andi Putra and Sutabri 2023). Komputer forensik atau *digital forensic* merupakan ilmu untuk memperoleh, mengambil, dan menyajikan data yang telah diproses secara elektronik, dan dapat diklasifikasikan lagi menjadi beberapa bagian disk forensic, system forensik, network forensik dan internet forensik (Hartanto, Utami, and Fatta 2011). Terdapat dua jenis teknik pengangkatan barang bukti atau forensik, yakni *dead forensic* yang membutuhkan data yang disimpan secara permanen dalam perangkat media penyimpanan, biasanya hardisk, dan *Live forensic* melibatkan data berjalan pada sistem atau data *volatile* yang biasanya tersimpan pada RAM atau transit pada jaringan (Yudhana, Riadi, and Anshori 2018). Analisis forensik

akan memberikan detail untuk membantu para penyelidik dan lembaga investigasi memecahkan dan menghubungkan kasus-kasus dengan kejahatan yang dilaporkan. Terdapat berbagai metode dalam melakukan digital forensik, dimana salah satu metode yang dapat digunakan adalah metode NIST (*National Institute of Standards and Technology*), yakni 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 (Nasirudin, Sunardi, and Riadi 2020).

Untuk memanfaatkan metode digital forensik, tetap diperlukan aplikasi atau tools yang mendukung jalannya proses analisis forensik dengan lebih baik, *tools* yang dapat digunakan untuk melakukan analisis forensik 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 menggungguli aplikasi Belkasoft Evidence Center, dengan temuan sebanyak 8 aktivitas transaksi, sementara Belkasoft Evidence Center dengan temuan sebanyak 7 aktivitas transaksi (Umar, Yudhana, and Fadillah 2022). Aplikasi lain yang juga dapat diandalkan khususnya untuk pengembalian data adalah *recuva* dan *puran file recovery* yang keduanya dapat bekerja dengan baik dalam memulihkan data yang telah dihapus (Handrizal 2017). Dalam rangka memastikan file yang dipulihkan masih utuh dan merupakan berkas yang sama dengan file asli, maka perlu dilakukan pengecekan dengan mencocokan *file hash* dari berkas yang asli dengan berkas yang dipulihkan, salah satu algoritma *hash* yang paling populer adalah Message-Digest 5 atau MD5, yang merupakan fungsi hash kriptografi dan digunakan untuk melakukan pemeriksaan integritas file dalam berbagai situasi (Lubis 2019). Salah satu cara untuk melakukan validasi hash dapat dengan menggunakan aplikasi *hash compare* dari securityxploded.

STUDI LITERATUR

Penelitian sebelumnya oleh (Pranoto, Riadi, and Prayudi 2020), dilakukan perbandingan kinerja aplikasi forensik yaitu Autopsy, Belkasoft, dan Testdisk, hasil akhir penelitian memperlihatkan bahwa Prosentase recovery TRIM disable dengan aplikasi Autopsy dan Testdisk adalah 100% sehingga dapat menemukan barang bukti dan menjaga integritas barang bukti. Disini terlihat bahwa aplikasi autopsy mempunyai potensi yang baik dalam kategori pengembalian data. Sementara di penelitian lain, oleh (Pratama, Carudin, and Yusup 2021), aplikasi Autopsy juga mengungguli aplikasi lain dalam proses file carving.

Pada penelitian yang dilakukan oleh (Simanjuntak 2017) ditemukan bahwa time left Recuva sebagai Software yang lebih baik dari Pandora Recovery, juga mempunyai fitur yang bagus. Sehingga aplikasi recuva dapat menjadi alternatif yang layak untuk pemulihan data. Penelitian lain oleh (Handrizal 2017), juga mendapatkan hasil bahwa aplikasi puran, undelete dan recuva dapat berkerja dengan baik dalam hal menemukan data yang sudah dihapus maupun dalam memulihkan data yang sudah dihapus tersebut.

Untuk itu, penelitian ini akan fokus untuk melakukan perbandingan kinerja dari 5 aplikasi, yaitu Autopsy, Recuva, Stellar, Puran dan Easus untuk melakukan tugas pengembalian data yang telah dihapus, serta pencocokan data yang telah di analisa dengan data asli, studi kasus yang digunakan adalah skenario kasus kejahatan berupa pencurian data perusahaan dengan menggunakan *flashdisk*, sehingga perlu dilakukan digital forensik untuk mendapatkan bukti digital berupa file berkas yang telah dihapus dari *flashdisk* tersebut.

METODE

Dalam melakukan penelitian ini, metode yang dipakai yaitu metode NIST (*National Institute of Standard and Technology*), dimana tahapan dalam metode ini terdapat 4 langkah, langkah tersebut dimulai dari *collection, examination, analysis*, hingga *reporting* (Riadi 2020). Metode ini akan digunakan bersamaan dengan 5 *tools* berbeda untuk mendapatkan perbandingan kinerja dari kelima aplikasi tersebut, yaitu aplikasi *autopsy, recuva, stellar, puran,* dan *easus*.

Fig. 1 Tahapan metode NIST

Berdasarkan gambar diatas, maka langkah-langkah analisis forensik dengan menggunakan metode NIST tersebut dapat dirincikan yaitu (1) *Collection*, tahapan ini dilakukan persiapan dengan melakukan pengumpulan

barang bukti dan peralatan yang akan digunakan untuk menganalisis data digital serta mencari bukti digital, proses ini mengikuti langkah pengamanan integritas data. (2) *Examination*, merupakan tahapan dalam pengambilan atau penggalian artefak sehingga dapat menemukan data pada barang bukti yang dilakukan dengan menggunakan 5 *tools,* yaitu *autopsy, recuva, stellar, puran* dan *easus*. (3) *Analysis*, yakni tahapan dilakukannya analisa dan evaluasi terhadap data yang telah ditemukan pada tahapan-tahapan sebelumnya. Di tahap ini juga akan dilakukan pengembalian data serta pencocokan *hash* berkas dari *flashdisk* dengan berkas asli untuk memastikan bahwa file tersebut memang benar adalah sama dan masih bersifat utuh. (4) *Reporting*, merupakan tahapan terakhir dalam metode ini dimana akan dilakukan proses pelaporan hasil analisis dari tahapan-tahapan sebelumnya untuk diambil kesimpulan.

Sebelum dilakukan penelitian, telah disiapkan beberapa data untuk menjadi bukti digital kasus kejahatan yang harus ditemukan dan dikembalikan pada *flashdisk,* yaitu berupa 6 file dengan ekstensi DOCX, XLSX, MP3, MP4, TXT, dan PNG. Dengan nama file seperti yang dapat dilihat pada gambar dibawah ini.

Fig. 2 Data yang disiapkan sebagai barang bukti

Setelah dimasukan ke *flashdisk*, data tersebut kemudian dihapus dengan memformat langsung *flashdisk* untuk menghilangkan bukti, sehingga kondisi *flashdisk* setelah di format adalah kosong tanpa ada nya file apapun.

PEMBAHASAN

Untuk melanjutkan proses pengembalian data, digunakanlah beberapa alat berupa perangkat keras dan perangkat lunak yaitu dengan keterangan seperti pada tabel dibawah ini.

Table 1
Alat dan Bahan

No	Nama	Spesifikasi	Keterangan
1	Laptop	Acer Swift X, Windows 11	Perangkat Keras
2	Flashdisk	Sandisk, 16 GB	Perangkat Keras
3	Autopsy	Aplikasi	Perangkat Lunak
4	Recuva	Aplikasi	Perangkat Lunak
5	Stellar	Aplikasi	Perangkat Lunak
6	Puran	Aplikasi	Perangkat Lunak
7	Easus	Aplikasi	Perangkat Lunak

A. Collection

Pada tahapan ini, dilakukan pengumpulan barang bukti, dan telah dikumpulkan sebuah barang bukti yang digunakan yakni *flashdisk* dengan merk Sandisk tipe Cruzer Blade CZ50 16GB.

Fig. 3 Flashdisk yang digunakan

Sebelum file barang bukti berupa 6 berkas seperti pada skenario kasus kejahatan disimpan dalam *flashdisk* ini, kondisi *flashdisk* tersebut sebelumnya telah digunakan dan pernah disimpan berbagai macam file, sebelum akhirnya disimpan berkas yang terkait dengan skenario kejahatan dalam penelitian ini.

B. Examination

Untuk mendapatkan informasi lengkap rekam jejak digital berupa file apa saja yang pernah disimpan dalam flashdisk sebagai barang bukti, maka dilakukanlah proses akuisisi data dari perangkat flashdisk, yang dilakukan dengan tools autopsy, recuva, stellar, puran, dan easus, kegiatan pada tahapan ini memakan waktu yang cukup lama karena perlu menggali setiap data yang sebelumnya telah dihapus. Hasil akuisisi data dari masing-masing aplikasi mendapatkan hasil yang berbeda-beda yaitu sebagai berikut:

1. *Autopsy*, aplikasi ini berhasil menemukan sebanyak 2902 file yang pernah dimasukan ke dalam *flashdisk.*
2. *Recuva*, aplikasi ini berhasil menemukan sebanyak 1932 file.
3. *Stellar*, berhasil menemukan sebanyak 2011 file dalam 137 folder.
4. *Puran*, berhasil mendapatkan data sebanyak 2086 file.
5. *Easus*, berhasil menemukan sebanyak 2709 file berkas dari flashdisk.

Pada tahapan ini, didapatkan bahwa aplikasi Autopsy berhasil menemukan lebih banyak file dibandingkan aplikasi yang lain, yaitu sebanyak 2902 file.

C. Analysis

Pada tahapan analisis dilakukan pencarian data berupa barang bukti, hal tersebut dapat dilakukan melalui pencarian dengan kata kunci atau dicari secara manual. Pencarian dengan kata kunci dilakukan dengan memasukan input ‘barang bukti’ sesuai dengan nama file sebelum di format, serta dengan memasukan input format file, seperti ’*.mp3’, jika tidak ditemukan barulah dilakukan pencarian manual dengan memeriksa file yang ada. Langkah-langkah tersebut dilakukan pada kelima aplikasi yang digunakan.

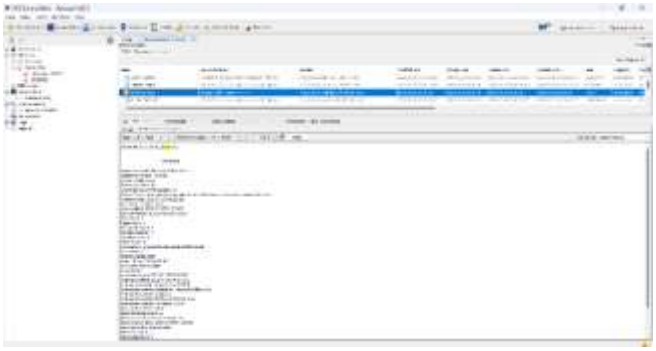

Fig. 4 Tampilan aplikasi autopsy

Aplikasi autopsy dapat memeriksa isi dari tiap berkas, sehingga hasil pencarian bukan hanya berdasarkan dari nama file atau ekstensi nya saja, melainkan juga berdasarkan metadata dari tiap-tiap file. Fitur ini mempermudah proses pencarian data. Selain itu, aplikasi autopsy juga telah disediakan fitur filter berdasarkan jenis berkas.

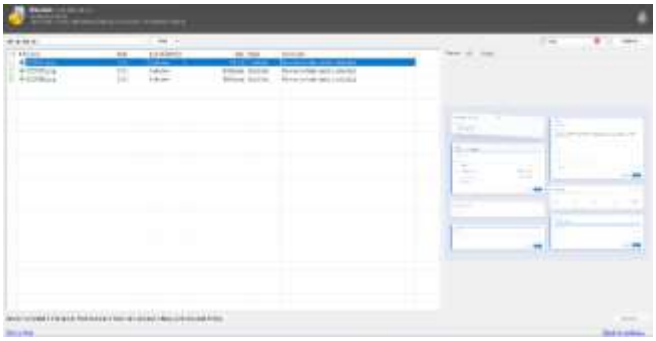

Fig. 5 Tampilan aplikasi recuva

Aplikasi recuva tentunya juga telah menyediakan fitur pencarian berdasarkan kata kunci ataupun ekstensi berkas untuk mempermudah pengguna dalam menemukan data, dengan tambahan fitur preview juga memberikan pengalaman pengguna yang baik.

Fig. 6 Tampilan aplikasi stellar

Sementara itu, pada aplikasi stellar, dapat dilakukan pencarian melalui folder-folder yang telah dikategorikan, pencarian dapat dilakukan dengan lebih mudah karena terdapat opsi preview sehingga isi dari file dapat dilihat secara langsung, selain itu, juga dapat dilakukan pencarian dengan fitur search.

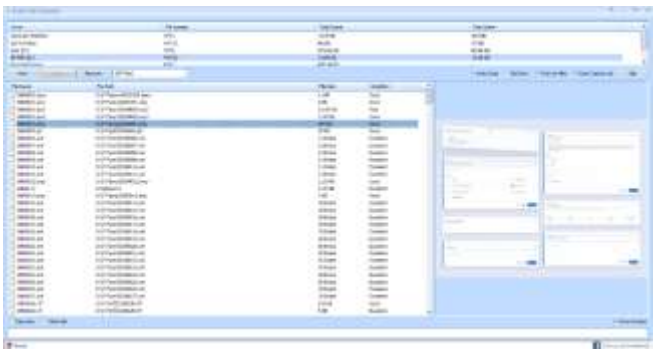

Fig. 7 Tampilan aplikasi puran

Untuk aplikasi puran, juga dilengkapi fitur yang hampir sama, yaitu fitur pencarian dengan beberapa filter serta preview. Mengembalikan berkas juga dapat dengan mudah dilakukan, baik salah satu ataupun banyak berkas sekaligus dengan fitur recover.

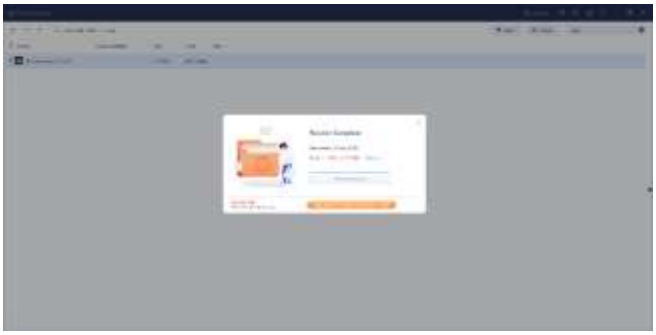

Fig. 8 Tampilan aplikasi easus

Aplikasi easus memberikan beberapa kategori folder untuk di eksplor, seperti Deleted, File Path Lost, File Name Lost, dll. juga dilengkapi fitur pencarian dengan filter untuk mempermudah dalam pencarian data, sedangkan pengembalian data dapat dilakukan secara terbatas untuk versi gratis.

Fig. 9 Tampilan aplikasi hash compare

Setelah dilakukan pengembalian data menggunakan masing-masing aplikasi, selanjutnya data yang dikembalikan dibandingkan dengan data asli untuk memeriksa apakah berkas masih utuh dan adalah sama dengan berkas asli.

D. Reporting

Setelah melalui tahapan analisis, berikut ini merupakan hasil pelaporan dari tahapan analisis forensik yang dilakukan dengan menggunakan 5 aplikasi pengembalian data.

Table 2
Hasil Tool Autopsy

Data	Ekstensi	Ditemukan	Kondisi	Hash Compare
Barang bukti word	DOCX	Ya	Baik	Valid
Barang bukti excel	XLSX	Ya	Baik	Valid
Barang bukti mp3	MP3	Ya	Tidak Baik	Tidak Valid
Barang bukti mp4	MP4	Ya	Baik	Valid
Barang bukti notepad	TXT	Tidak	-	-
Barang bukti png	PNG	Ya	Baik	Valid

Hasil akhir dari penggunaan aplikasi autopsy, file bukti dalam bentuk word, excel, mp4, dan png berhasil ditemukan dan dapat dipulihkan dengan baik, serta telah dilakukan hash comparison untuk melihat apakah file yang di temukan adalah file yang sama dengan file asli dan benar merupakan berkas yang sesuai dengan yang ditulis dalam skenario, sehingga dapat dijadikan barang bukti. File mp3 dapat ditemukan namun tidak berhasil di pulihkan dalam keadaan normal, melainkan dokumen dengan jenis musik tersebut sudah corrupt dan menyebabkan lagu yang diputar tidak utuh. Sementara itu, dokumen notepad dengan ekstensi txt tidak berhasil ditemukan.

Table 3
Hasil Tool Recuva

Data	Ekstensi	Ditemukan	Kondisi	Hash Compare
Barang bukti word	DOCX	Ya	Baik	Valid
Barang bukti excel	XLSX	Ya	Baik	Valid
Barang bukti mp3	MP3	Tidak	-	-
Barang bukti mp4	MP4	Ya	Baik	Valid
Barang bukti notepad	TXT	Tidak	-	-
Barang bukti png	PNG	Ya	Baik	Valid

Untuk hasil pengembalian data dari aplikasi recuva, file bukti dalam bentuk word, excel, mp4, dan png berhasil ditemukan, juga dapat dipulihkan dengan baik dan sesuai dengan yang ditulis dalam skenario dan dapat dijadikan barang bukti. Sementara itu, file mp3 dan txt tidak berhasil ditemukan.

Table 4
Hasil Tool Stellar

Data	Ekstensi	Ditemukan	Kondisi	Hash Compare
Barang bukti word	DOCX	Tidak	-	-
Barang bukti excel	XLSX	Tidak	-	-
Barang bukti mp3	MP3	Tidak	-	-
Barang bukti mp4	MP4	Ya	Baik	Valid
Barang bukti notepad	TXT	Tidak	-	-
Barang bukti png	PNG	Ya	Baik	Valid

Aplikasi stellar berhasil menemukan file bukti dalam bentuk mp4 dan png dan dapat dipulihkan dengan baik Sementara file bukti dengan bentuk word, excel, dan dokumen notepad dengan ekstensi txt tidak berhasil ditemukan.

Table 5
Hasil Tool Puran

Data	Ekstensi	Ditemukan	Kondisi	Hash Compare
Barang bukti word	DOCX	Ya	Baik	Valid
Barang bukti excel	XLSX	Ya	Baik	Valid
Barang bukti mp3	MP3	Tidak	-	-
Barang bukti mp4	MP4	Ya	Baik	Tidak Valid
Barang bukti notepad	TXT	Tidak	-	-
Barang bukti png	PNG	Ya	Baik	Valid

Dengan menggunakan aplikasi puran, file bukti dalam bentuk word, excel, mp4, dan png berhasil ditemukan, akan tetapi terdapat perbedaan hash pada file mp4 sehingga tidak bisa disebut sebagai berkas yang sama meskipun dapat dikembalikan dan memberikan output yang sesuai dengan file asli. Sementara itu, file musik dengan ekstensi mp3 dan dokumen notepad dengan ekstensi txt tidak berhasil ditemukan.

Table 6
Hasil Tool Easus

Data	Ekstensi	Ditemukan	Kondisi	Hash Compare
Barang bukti word	DOCX	Ya	Baik	Valid
Barang bukti excel	XLSX	Ya	Baik	Valid
Barang bukti mp3	MP3	Tidak	-	-
Barang bukti mp4	MP4	Ya	Tidak Baik	Tidak Valid
Barang bukti notepad	TXT	Tidak	-	
Barang bukti png	PNG	Ya	Baik	Valid

Hasil pengembalian data dengan aplikasi easus didapatkan bahwa file bukti dalam bentuk word, excel, mp4, dan png berhasil ditemukan, namun file video dengan format mp4 tidak dapat diputar karena telah menjadi corrupt. Sementara itu, dokumen notepad dengan ekstensi txt tidak berhasil ditemukan.

Table 7
Hasil Analisa Perbandingan

Aplikasi	Data Dikembalikan	Persentase
Autopsy	5 / 6	83%
Recuva	4 / 6	66%
Stellar	2 / 6	33%

Puran	4 / 6	66%
Easus	4 / 6	66%

Dari analisa yang telah dikumpulkan sebelumnya, dapat disimpulkan bahwa aplikasi autopsy dapat mengembalikan data sebanyak 83% dari skenario kasus kejahatan yang telah dibuat, sementara itu aplikasi lain yaitu recuva, puran, dan easus hanya mengembalikan sebanyak 66% dan aplikasi stellar sebanyak 33%.

KESIMPULAN

Berdasarkan hasil penelitian, dengan skenario kasus kejahatan yang dibuat, yaitu pencurian data melalui media flashdisk drive, penggunaan metode NIST dan 5 aplikasi yang diuji coba yaitu autopsy, recuva, stellar, puran, dan easus dapat diandalkan untuk melakukan analisis forensik, khususnya untuk tugas pengembalian data. Dari hasil penelitian juga dapat dilihat aplikasi autopsy berhasil menemukan sebanyak 5 dari 6 file bukti skenario kejahatan, atau jika dibuat dalam bentuk persentase, terdapat 83% file yang berhasil ditemukan dan dikembalikan, yaitu file DOCX, XLSX, MP3, MP4, dan PNG. Sementara dokumen notepad dengan ekstensi TXT tidak berhasil ditemukan. Hasil tersebut mengalahkan kinerja dari aplikasi lain dengan persentase temuan dan pengembalian data yang lebih rendah, yaitu recuva, puran, dan easus hanya mengembalikan sebanyak 66% dan aplikasi stellar sebanyak 33%.

REFERENSI

Andi Putra, Yusuf, and Tata Sutabri. 2023. "ANALISIS PENYADAPAN PADA APLIKASI WHATSAPP DENGAN MENGGUNAKAN METODE SINKRONISASI DATA." *Blantika : Multidisciplinary Journal* 2(1):11–20. doi: 10.57096/blantika.v2i1.8.

Bellini, Yustida, and Tata Sutabri. 2023. "Sistem Pakar Mendeteksi Tindak Pidana Cyber Crime untuk Penanganan Komputer Forensik Menggunakan Backward Chaining." *Jurnal Digital Teknologi Informasi* 6(1):42. doi: 10.32502/digital.v6i1.5619.

Handrizal, Handrizal. 2017. "Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik." *J-SAKTI (Jurnal Sains Komputer dan Informatika)* 1(1):84. doi: 10.30645/j-sakti.v1i1.31.

Hartanto, Anggit Dwi, Ema Utami, and Hanif Al Fatta. 2011. "PENERAPAN TEKNIK KOMPUTER FORENSIK UNTUK PENGEMBALIAN DAN PENGAHAPUSAN BERKAS DIGITAL." *Jurnal Teknologi* 4.

Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia. 2020. "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)." *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)* 4(5):820–28. doi: 10.29207/resti.v4i5.2224.

Lubis, Sapria Ulandari. 2019. "IMPLEMENTASI METODE MD5 UNTUK MENDETEKSI ORISINALITAS FILE AUDIO." *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)* 3(1). doi: 10.30865/komik.v3i1.1620.

Nasirudin, Nasirudin, Sunardi Sunardi, and Imam Riadi. 2020. "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express." *Jurnal Informatika Universitas Pamulang* 5(1):89. doi: 10.32493/informatika.v5i1.4578.

Pranoto, Wisnu, Imam Riadi, and Yudi Prayudi. 2020. "Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics." *IT JOURNAL RESEARCH AND DEVELOPMENT* 4(2). doi: 10.25299/itjrd.2020.vol4(2).4615.

Pratama, Arvin Kynan, Carudin Carudin, and Dadang Yusup. 2021. "Analisis Perbandingan Perangkat Lunak Forensik Digital untuk File Carving dalam Mengungkap Barang Bukti Digital." *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)* 6(2):109–20. doi: 10.32528/justindo.v6i2.5101.

Riadi, Imam. 2020. "PERBANDINGAN TOOL FORENSIK DATA RECOVERY BERBASIS ANDROID MENGGUNAKAN METODE NIST."

Simanjuntak, Pastima. 2017. "ANALISIS PERBANDINGAN APLIKASI PANDORA RECOVERY DAN RECUVA TERHADAP PENGEMBALIAN DATA WINDOWS."

Sulisrudatin, Nunuk. 2014. "ANALISA KASUS CYBERCRIME BIDANG PERBANKAN BERUPA MODUS PENCURIAN DATA KARTU KREDIT." *JURNAL ILMIAH HUKUM DIRGANTARA* 9(1). doi: 10.35968/jh.v9i1.296.

Sutabri, Tata. 2012a. *Analisis Sistem Informasi*. Andi.

Sutabri, Tata. 2012b. *Konsep Sistem Informasi*. Andi.

Thalib, Emmy Febriani, and Ketut Laksmi Maswari. 2021. "PERLINDUNGAN HUKUM TERHADAP DATA

PRIBADI PERUSAHAAN AKIBAT PENYALAHGUNAAN DATA DIGITAL OLEH KARYAWAN PERUSAHAAN."

Umar, Rusydi, Anton Yudhana, and Muhammad Noor Fadillah. 2022. "PERBANDINGAN TOOLS FORENSIK PADA APLIKASI DOMPET DIGITAL." *JIKO (Jurnal Informatika dan Komputer)* 6(2):242. doi: 10.26798/jiko.v6i2.621.

Yudhana, Anton, Imam Riadi, and Ikhwan Anshori. 2018. "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist." *IT JOURNAL RESEARCH AND DEVELOPMENT* 3(1):13–21. doi: 10.25299/itjrd.2018.vol3(1).1658.