Jurnal Ilmu Komputer (JIK)
Volume 7, Nomor 1, Desember 2024: 66-71
E-ISSN: 2746-7163

Penerapan Tools Autopsy Untuk Recovery File Pada Windows

[1]Azril Ardiansyah, [2*]Deni Saptudin Djoha, [3]Muhammad Zikri Ardiansyah, [4]Emi Sita Eriana
Sistem Informasi, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
deni21djoha@gmail.com

ABSTRAK

Pemulihan data yang hilang pada sistem operasi Windows menjadi salah satu tantangan utama dalam bidang forensik digital. Autopsy, sebagai salah satu perangkat lunak sumber terbuka (open-source) yang populer dalam digital forensik, menawarkan solusi komprehensif untuk menganalisis dan memulihkan file yang terhapus atau rusak. Penelitian ini bertujuan untuk mengevaluasi kinerja dan efektivitas Autopsy dalam proses recovery file pada lingkungan Windows.
Studi ini dilakukan melalui simulasi skenario kehilangan data, di mana berbagai tipe file dihapus dari perangkat berbasis Windows, kemudian diupayakan pemulihannya menggunakan Autopsy. Hasil penelitian menunjukkan bahwa Autopsy memiliki kemampuan yang signifikan dalam mengidentifikasi dan memulihkan file, termasuk file yang telah terhapus permanen, namun keberhasilan pemulihan dipengaruhi oleh beberapa faktor, seperti jenis file, waktu penghapusan, dan aktivitas sistem setelah file dihapus.
Dengan demikian, Autopsy dapat menjadi alat yang efektif untuk profesional di bidang forensik digital dalam upaya pemulihan data, meskipun diperlukan penyesuaian lebih lanjut untuk situasi-situasi yang lebih kompleks.
Kata Kunci: Forensik Digital, Pemulihan Data, Autopsy, Recovery File, Windows.

ABSTRACT

Data recovery from lost data on Windows operating systems is one of the major challenges in digital forensics. Autopsy, as one of the popular open-source software in digital forensics, offers a comprehensive solution to analyze and recover deleted or corrupted files. This study aims to evaluate the performance and effectiveness of Autopsy in the file recovery process in a Windows environment.
This study was conducted through a simulation of a data loss scenario, where various types of files were deleted from a Windows-based device, then attempted to recover them using Autopsy. The results showed that Autopsy has significant capabilities in identifying and recovering files, including files that have been permanently deleted, but the success of recovery is affected by several factors, such as file type, deletion time, and system activity after the file was deleted.
Thus, Autopsy can be an effective tool for digital forensics professionals in data recovery efforts, although further adjustments are needed for more complex situations.
Keywords: *Digital Forensics, Data Recovery, Autopsy, File Recovery, Windows.*

PENDAHULUAN

Dalam era digital saat ini, data memiliki peran yang sangat penting dalam berbagai aspek kehidupan, baik dalam konteks pribadi, bisnis, maupun pemerintahan. Namun, kehilangan data karena kesalahan pengguna, kerusakan

perangkat keras, atau serangan siber menjadi tantangan serius yang dihadapi oleh banyak individu dan organisasi. Pemulihan data yang hilang, terutama pada sistem operasi Windows yang banyak digunakan, memerlukan alat dan metode yang efektif serta andal.

Salah satu perangkat lunak yang digunakan dalam upaya pemulihan data dan investigasi forensik digital adalah **Autopsy**. Autopsy adalah perangkat lunak sumber terbuka yang dirancang untuk melakukan analisis forensik digital pada berbagai sistem operasi, termasuk Windows. Dengan fitur-fitur canggih yang dimilikinya, Autopsy mampu melakukan proses recovery file, analisis jejak digital, serta memberikan laporan

A. TINJAUAN PUSTAKA

Tinjauan pustaka ini membahas konsep-konsep dasar terkait pemulihan data, forensik digital, serta peran perangkat lunak Autopsy dalam konteks recovery file pada sistem operasi Windows.

1.1 Forensik Digital

Forensik digital adalah disiplin ilmu yang berkaitan dengan identifikasi, pengumpulan, pelestarian, analisis, dan presentasi bukti digital yang ditemukan di perangkat elektronik. Tujuannya adalah untuk mendukung investigasi atau tuntutan hukum. Forensik digital mencakup beberapa area, seperti komputer, jaringan, perangkat seluler, dan penyimpanan data cloud. Dalam konteks pemulihan file, forensik digital berfokus pada bagaimana menemukan dan memulihkan data yang hilang atau terhapus.].

1.2 Pemulihan Data

Pemulihan data adalah proses mengembalikan informasi yang hilang, terhapus, atau tidak dapat diakses dari perangkat penyimpanan. Berbagai teknik pemulihan data tersedia, tergantung pada cara data tersebut hilang (seperti karena kesalahan pengguna atau kerusakan sistem). Salah satu metode utama dalam pemulihan data adalah penggunaan perangkat lunak yang dapat menelusuri jejak digital yang ditinggalkan oleh file yang telah dihapus. Di Windows, saat sebuah file dihapus, datanya tidak langsung hilang dari hard drive; sistem hanya menandainya sebagai "dapat ditimpa," sehingga recovery file masih memungkinkan sebelum data tersebut ditimpa oleh data baru..

Gambar 1. Berikut adalah gambar dari dari interface Autopsy

Autopsy memiliki beberapa fitur unggulan yang mendukung proses pemulihan file, seperti:

1. File Recovery Module: Modul ini memungkinkan pengguna untuk mencari file yang terhapus, meskipun file tersebut telah dihapus secara permanen dari sistem.
2. Timeline Analysis: Fitur ini membantu pengguna memahami urutan waktu dari aktivitas sistem, yang dapat memberikan petunjuk kapan file terhapus.
3. Keyword Search: Autopsy memungkinkan pengguna mencari file berdasarkan kata kunci tertentu yang terkait dengan isi atau nama file.
4. Metadata Extraction: Fitur ini digunakan untuk mengidentifikasi karakteristik file seperti ukuran, tanggal pembuatan, dan perubahan terakhir.

1.3 Perangkat Lunak Autopsy

Autopsy adalah perangkat lunak open-source yang digunakan dalam analisis forensik digital. Dikembangkan pertama kali oleh Brian Carrier, perangkat ini memanfaatkan berbagai modul dan fitur yang memungkinkan investigasi digital secara menyeluruh, termasuk pencarian file yang terhapus, penelusuran aktivitas sistem, serta analisis metadata file.

METODE

Penelitian ini menggunakan pendekatan eksperimental untuk mengevaluasi kinerja perangkat lunak Autopsy dalam proses pemulihan file pada sistem operasi Windows.Langkah-langkah yang dilakukan dalam penelitian ini meliputi pengumpulan data, simulasi kehilangan data, penggunaan perangkat lunak Autopsy, serta analisis hasil pemulihan. Metode penelitian ini dibagi menjadi beberapa tahapan sebagai berikut:

2.1 Tahap Persiapan

Pada tahap ini, dilakukan persiapan perangkat keras dan perangkat lunak yang akan digunakan dalam penelitian, yaitu:

1. **Perangkat keras**: Sebuah komputer dengan spesifikasi standar yang menjalankan sistem operasi Windows.

2. **Perangkat lunak**: Autopsy versi terbaru, serta berbagai jenis file (dokumen, gambar, video, dll.) yang akan digunakan dalam simulasi kehilangan data.

Tahapan persiapan ini juga mencakup instalasi Autopsy dan pengaturan lingkungan Windows untuk mensimulasikan berbagai skenario penghapusan file.

2.2 Simulasi Kehilangan Data

Untuk mensimulasikan kehilangan data, beberapa file dengan berbagai format (misalnya: .docx, .jpg, .mp4, .pdf) akan disimpan di komputer, kemudian dihapus menggunakan metode berikut:

1. **Penghapusan standar**: File dihapus melalui Recycle Bin dan kemudian dikosongkan.
2. **Penghapusan permanen**: File dihapus menggunakan kombinasi tombol "Shift + Delete" untuk langsung menghilangkannya tanpa melalui Recycle Bin.

Kedua metode penghapusan ini bertujuan untuk menguji efektivitas Autopsy dalam memulihkan file dari skenario yang berbeda.

2.3 Penggunaan Autopsy untuk Pemulihan File

Setelah data dihapus, Autopsy digunakan untuk memindai sistem dan mencari file yang telah dihapus. Langkah-langkah penggunaan Autopsy adalah sebagai berikut:

1. **Pembuatan Kasus Baru**: Membuat proyek kasus baru di dalam Autopsy dan memilih media penyimpanan (hard disk) yang akan dipindai.
2. **Pemindaian Disk**: Autopsy melakukan pemindaian menyeluruh terhadap media penyimpanan untuk menemukan file yang dihapus atau hilang.
3. **Pencarian dan Pemulihan File:** Setelah pemindaian selesai, Autopsy menampilkan daftar file yang ditemukan. File-file yang telah dihapus dianalisis dan diupayakan untuk dipulihkan.

2.4 Pengukuran Keberhasilan Pemulihan

Keberhasilan pemulihan file diukur berdasarkan beberapa indikator berikut:

1. **Jumlah file yang berhasil dipulihkan**: Berapa banyak file yang dapat ditemukan dan dikembalikan ke keadaan semula.
2. **Kualitas file yang dipulihkan:** Apakah file yang dipulihkan dapat dibuka dan digunakan tanpa kerusakan.
3. **Waktu pemulihan**: Waktu yang dibutuhkan Autopsy untuk menemukan dan memulihkan file.

Setiap hasil pemulihan akan dianalisis untuk menentukan faktor-faktor yang mempengaruhi keberhasilan, seperti tipe file, metode penghapusan, dan durasi setelah penghapusan.

2.5 Analisis Data

Data yang diperoleh dari proses pemulihan dianalisis menggunakan metode deskriptif kuantitatif. Jumlah file yang berhasil dipulihkan, kualitas file,

serta waktu pemulihan akan dibandingkan antara berbagai skenario penghapusan. Selain itu, dilakukan evaluasi terhadap kekuatan dan keterbatasan Autopsy dalam proses pemulihan file, terutama dalam skenario yang lebih kompleks.

2.6 Pelaporan Hasil

Hasil analisis kemudian disusun dalam bentuk laporan yang memuat temuan-temuan utama mengenai efektivitas Autopsy dalam pemulihan file pada Windows. Pelaporan juga mencakup saran untuk penggunaan perangkat ini dalam situasi praktis. Melalui metode ini, diharapkan penelitian dapat memberikan gambaran yang komprehensif mengenai performa Autopsy dan memberikan panduan praktis bagi pengguna yang ingin memanfaatkan alat ini untuk pemulihan data.

HASIL

Penelitian ini berhasil mengevaluasi kinerja Autopsy dalam pemulihan file yang dihapus pada sistem operasi Windows melalui simulasi berbagai skenario kehilangan data. Hasil penelitian ini didasarkan pada pemulihan beberapa jenis file yang sengaja dihapus, baik melalui metode penghapusan standar maupun penghapusan permanen. Pembahasan ini meliputi hasil pemulihan, faktor-faktor yang mempengaruhi keberhasilan pemulihan, serta evaluasi keseluruhan dari penggunaan Autopsy.

3.1 Hasil Pemulihan File

Pemulihan file yang dilakukan dengan Autopsy menghasilkan beberapa temuan kunci terkait efektivitas perangkat lunak ini:

1. **Jumlah File yang Dipulihkan**: Dari total 100 file yang dihapus dalam berbagai format (.docx, .jpg, .mp4, .pdf), Autopsy berhasil memulihkan sekitar 85% file yang dihapus melalui metode penghapusan standar (Recycle Bin) dan 60% file yang dihapus secara permanen (Shift + Delete).

3.2 Faktor-Faktor yang Mempengaruhi Keberhasilan Pemulihan

Berdasarkan hasil pemindaian dan pemulihan, terdapat beberapa faktor yang mempengaruhi keberhasilan Autopsy dalam memulihkan file:

1. **Metode Penghapusan**: File yang dihapus melalui Recycle Bin lebih mudah dipulihkan karena mereka belum benar-benar dihapus dari hard disk; sistem hanya menandainya untuk dihapus di kemudian hari. Sebaliknya, file yang dihapus menggunakan metode permanen lebih sulit untuk dipulihkan, terutama setelah waktu tertentu.

3.3 Kelebihan Autopsy dalam Proses Pemulihan

Autopsy terbukti menjadi alat yang andal untuk pemulihan data dengan beberapa kelebihan yang menonjol:

1. **Antarmuka Pengguna yang Mudah**: Autopsy menyediakan antarmuka pengguna yang intuitif, sehingga memudahkan pengguna dalam

melakukan pemindaian dan pemulihan file tanpa memerlukan banyak pengetahuan teknis

KESIMPULAN

Penelitian ini berhasil mengevaluasi kemampuan perangkat lunak Autopsy dalam pemulihan file yang dihapus pada sistem operasi Windows. Hasil penelitian menunjukkan bahwa Autopsy dapat memulihkan sekitar 85% file yang dihapus melalui metode penghapusan standar dan 60% file yang dihapus secara permanen. Saran yang dapat di pertimbangkan, **Penggunaan Segera Setelah Penghapusan**: Pengguna disarankan untuk segera menggunakan Autopsy setelah kehilangan data untuk meningkatkan kemungkinan pemulihan. Semakin lama pengguna menunggu, semakin besar kemungkinan data tersebut tertimpa oleh data baru.

DAFTAR PUSTAKA

Eriana, E. S., & Subariah, R. (2022). Mengembangkan Sistem Keamanan Jaringan Komputer Pada Laboratorium Komputer STMIK Pranata Indonesia menggunakan Metode Forensik. *Unpampress*.

Eriana, E. S., & Sulastri, T. (2021). Pemanfaatan Teknologi Digital dalam Mendukung Kinerja Sistem Informasi Manajemen. *Journal of Applied Science and Technology*.

Eriana, E. S., Djoha, D. S., & Ardiansyah, M. Z. (2019). Penerapan Tools Autopsy untuk Recovery File pada Windows. *JATI*, 1-10.

Murphy, R., & Jackson, D. (2022). Forensic Data Recovery Techniques and Best Practices. *International Journal of Forensic Sciences*, 154-168.

N. Iman, et al. (2019). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia. *IncomTech: Jurnal Telekomunikasi dan Komputer*, 188–191.

Neshenko, P., & Kondratenko, V. (2020). Advanced Digital Forensics: Tools and Technologies for Effective Data Recovery. *International Journal of Digital Forensics and Cybersecurity*, 35-49.

Pugu, M. R., Riyanto, S., & Haryadi, R. N. (2024). *Metodologi Penelitian; Konsep, Strategi, dan Aplikasi*. PT. Sonpedia Publishing Indonesia.

Suthar, S., & Patel, K. (2021). Digital Forensic Investigation: Tools and Techniques for Forensic Data Recovery and Analysis. *Journal of Computer Science and Technology*, 284-301.