# Analisis Komparatif Performa FTK IMAGER dan AUTOPSY dalam Forensik Digital pada Flashdisk

# Alur Proses


Gambar 1. Alur Proses Penelitian

# Tahapan dan proses-proses dalam metode NIST (National Institute of Standard and Technology)

a) Collection: Fase pertama dalam proses ini adalah untuk mengidentifikasi, memberi label, merekam, dan memperoleh data dari sumber yang mungkin dari data yang relevan, mengikuti pedoman dan prosedur yang menjaga integritas data.

b) Examination: Pemeriksaan melibatkan pemrosesan forensik dalam jumlah besar data yang dikumpulkan dengan menggunakan kombinasi metode otomatis dan manual untuk menilai dan mengekstraksi data yang menarik, sambil menjaga integritas data.

c) Analysis: Menganalisis hasil pemeriksaan, menggunakan metode dan teknik yang dapat dibenarkan secara hukum, untuk memperoleh informasi yang berguna yang menjawab pertanyaanpertanyaan yang menjadi dorongan untuk melakukan pengumpulan dan pemeriksaan.

d) Reporting: Pelaporan hasil analisis, yang dapat mencakup menggambarkan tindakan yang digunakan, menjelaskan bagaimana alat dan prosedur dipilih, menentukan tindakan apa yang perlu dilakukan (misalnya, pemeriksaan forensik sumber data tambahan, mengamankan kerentanan yang diidentifikasi, meningkatkan kontrol keamanan yang ada), dan memberikan rekomendasi untuk perbaikan kebijakan, pedoman, prosedur, alat, dan aspek lain dari proses forensik

Peningkatan penggunaan flashdisk atau perangkat USB cenderung masif karena berbagai aspek, salah satunya ukuran dan harga perangkat penyimpanan USB yang terjangkau. Namun, karena sifatnya yang portabel dan mudah dibawa-bawa, flashdisk juga seringkali digunakan dalam kejahatan digital. Penelitian dilakukan untuk pengimplementasian proses akuisisi data yang terhapus dari sebuah flashdisk menggunakan tools forensik Autopsy dan Forensic Toolkit Imager (FTK Imager) dan metode National Institute of Standard and Technology (NIST) serta validasi dengan pencocokan nilai hash. Hasil akuisisi menunjukan pada flashdisk yang dilakukan delete, FTK Imager memperoleh nilai 100%, sementara Autopsy memperoleh nilai 94,12%. Pada flashdisk yang dilakukan quick format FTK imager memperoleh nilai 0% dibandingkan Autopsy 97,06%. Sementara itu, pada flashdisk yang dilakukan format, FTK Imager dan Autopsy memperoleh nilai 0%. Hal ini disebabkan karena keduanya tidak berhasil menemukan file yang terhapus

# Forensik Komputer

- Proses forensik komputer melibatkan beberapa tahapan, termasuk **mengidentifikasi dan mengamankan bukti digital, menganalisis bukti** untuk mengungkap informasi yang mungkin relevan dengan penyelidikan, dan menyajikan temuan dalam cara yang jelas dan singkat. Para ahli forensik komputer dapat menggunakan berbagai alat dan teknik untuk **mengekstrak informasi dari perangkat digital**, termasuk **perangkat lunak pemulihan data**

# Pemulihan

- **Pemulihan data (recovery data)** merujuk pada proses memulihkan data yang hilang atau terhapus dari suatu perangkat penyimpanan seperti hard drive, USB drive, atau kartu memori. Data dapat hilang karena beberapa alasan seperti kerusakan perangkat keras, serangan virus atau malware, kesalahan manusia, atau kegagalan perangkat lunak.
- Proses pemulihan data dimulai dengan mengidentifikasi penyebab hilangnya data dan menentukan apakah data masih dapat dipulihkan. Namun, tidak semua data dapat dipulihkan dan proses pemulihan data dapat menjadi mahal tergantung pada tingkat kerusakan atau jenis data yang hilang

# Penghapusan Data Format, Quick Format, dan Delete

- Format: Proses penghapusan data pada perangkat penyimpanan digital dan pengaturan ulang file system pada perangkat tersebut. Dalam proses format, seluruh data pada perangkat akan dihapus, termasuk file sistem dan partisi
- Quick format: Proses penghapusan data pada perangkat penyimpanan digital dan pengaturan ulang file system pada perangkat tersebut, namun hanya menghapus file sistem dan partisi saja. Data pada sektor-sektor di dalam perangkat penyimpanan tetap ada dan dapat dipulihkan dengan perangkat lunak pemulihan data khusus
- Delete: Proses penghapusan file atau folder pada perangkat penyimpanan digital. Saat file atau folder dihapus menggunakan metode delete, data tersebut masih tetap ada pada perangkat penyimpanan, namun hanya file sistem yang menghapus akses ke data tersebut

# FTK Imager

- FTK Imager adalah perangkat lunak forensik yang digunakan untuk memperoleh gambar atau salinan forensik dari perangkat penyimpanan data, seperti
  - hard drive,
  - USB drive, dan kartu memori.
- Dapat digunakan untuk melakukan analisis forensik pada data yang terdapat pada perangkat penyimpanan tersebut.
- FTK Imager dikembangkan oleh AccessData, sebuah perusahaan yang menyediakan solusi forensik digital dan keamanan informasi. FTK Imager dapat digunakan oleh para profesional forensik, investigasi keamanan informasi, atau pengguna individu yang ingin memulihkan data yang hilang dari perangkat

# Autopsy

- Autopsy adalah perangkat lunak forensik sumber terbuka (open source) yang digunakan untuk analisis forensik pada perangkat lunak, perangkat keras, dan data digital.
- Autopsy dikembangkan oleh Basis Technology Corp dan diperbarui secara berkala oleh komunitas pengembang terbuka. Perangkat lunak ini dapat digunakan pada berbagai sistem operasi seperti Windows, Linux, dan MacOS.
- Autopsy sangat berguna bagi para profesional forensik, seperti penegak hukum, tim investigasi keamanan informasi, atau pengguna individu yang ingin melakukan analisis forensik pada perangkat lunak atau data digital. Autopsy juga menyediakan berbagai macam plugin untuk membantu para pengguna memperluas fungsi perangkat lunak sesuai dengan kebutuha

# Perbandingan FTK Imager dan Autopsy

Tabel 1. Perbandingan FTK Imager dan Autopsy

| Aspek | FTK Imager | Autopsy |
|---|---|---|
| Fitur | lebih fokus pada proses pengambilan dan pembuatan *image* forensik dari perangkat penyimpanan | lebih fokus pada analisis data digital dan memiliki fitur pencarian dan visualisasi data yang kuat |
| Tampilan | lebih sederhana dan mudah digunakan | lebih kompleks dengan banyak pilihan dan fitur yang lebih banyak |
| Ketersediaan | Windows | Windows, Linux, dan MacOS |
| Penggunaan | Cocok digunakan oleh para profesional forensik yang sudah terbiasa menggunakan perangkat lunak forensik | Mudah digunakan dan dapat digunakan oleh orang yang tidak memiliki latar belakang teknis yang kuat dalam forensik digital |

# Skenario

- Berikut ini beberapa skenario yang dilakukan pada penelitian ini.
  - a. Skenario 1: Flashdisk menyimpan 34 file barang bukti kejahatan, kemudian seseorang berusaha melakukan penghapusan pada file dengan melakukan **delete**.
  - b. Skenario 2: Flashdisk menyimpan 34 file barang bukti kejahatan, kemudian seseorang berusaha melakukan penghapusan pada file dengan melakukan **quick format**.
  - c. Skenario 3: Flashdisk menyimpan 34 file barang bukti kejahatan, kemudian seseorang berusaha melakukan penghapusan pada file dengan melakukan **format**