

MAKALAH
ALGORITMA LANJUT
ALGORITMA BREADTH FIRST SEARCH DALAM DIGITAL
FORENSIK



Disusun Oleh :

11421018 Yudi Frandianto Saragih

11521019 Ignatius Simamora

11421028 Fanny Clara Sinaga

11421029 Prisilia Lumbantoruan

Institut Teknologi Del
Fakultas Vokasi
D4 Teknologi Rekayasa Perangkat Lunak
Laguboti
2023

BAB I

PENDAHULUAN

1. Latar Belakang

Dengan pesatnya perkembangan teknologi dan penggunaan serta perangkat digital lainnya, kejahatan digital juga semakin meningkat. Dalam konteks ini, bidang forensik digital menjadi sangat penting dalam membantu penyelidikan dan penyelesaian kasus-kasus kriminal yang melibatkan penggunaan teknologi informasi. Salah satu metode yang sangat berguna dalam analisis forensik digital adalah algoritma Breadth First Search (BFS). Dokumen ini bertujuan untuk mendalami penggunaan algoritma BFS dalam bidang forensik digital dengan fokus pada penemuan bukti elektronik. Algoritma BFS, yang awalnya dikembangkan untuk penelusuran graf, dapat diterapkan dalam analisis forensik digital untuk menemukan dan menganalisis jejak digital, file tersembunyi, dan hubungan antara entitas digital yang terlibat dalam suatu kejadian kriminal.

Laporan ini akan membahas secara rinci tentang algoritma BFS, prinsip-prinsip dasar forensik digital, serta aplikasi algoritma BFS dalam rangka penemuan bukti elektronik. Selain itu, laporan ini juga akan menggambarkan bagaimana algoritma ini dapat membantu dalam mengekstraksi informasi penting, menyusun jejak digital yang relevan, dan membantu rekonstruksi kejadian berdasarkan bukti-bukti digital yang ditemukan. Melalui penelitian ini, diharapkan akan terbuka wawasan baru tentang penerapan algoritma BFS dalam konteks forensik digital, sehingga dapat memberikan kontribusi yang signifikan dalam mempercepat dan memperkuat proses analisis forensik, serta meningkatkan akurasi dan keandalan dalam penyelidikan kasus kejahatan digital. Dengan demikian, laporan ini diharapkan dapat memberikan kontribusi nyata bagi pengembangan bidang forensik digital dan penggunaan teknologi dalam upaya penegakan hukum.

2. Landasan Teori

2.1. Pengertian Algoritma Breadth First Search Dan Cara Kerja Algoritma Breadth First Search

Breadth-first search adalah algoritma pencarian yang dilakukan secara melebar, algoritma ini mengunjungi simpul secara pre order, artinya mengunjungi suatu simpul kemudian mengunjungi simpul yang bertetangga dengan simpul tersebut terlebih dahulu. Selanjutnya, simpul yang belum dikunjungi juga dikunjungi dan bertetangga dengan simpul tersebut

dikunjungi juga. Cara kerja algoritma breadth-first search adalah pencarian awal akan dimulai dari simpul dasar lalu jika simpul solusi ditemukan maka pencarian akan selesai, namun ketika simpul solusi belum ditemukan maka simpul tetangga akan dimasukkan ke dalam antrian sampai saat ini ketika simpul belum juga ditemukan maka pencarian selesai tanpa hasil. Metode ini adalah salah satu metode yang cocok untuk menjelajahi struktur dalam bentuk graf atau hierarki.

2.2. Pengertian Digital Forensik

Menurut Marcella, digital forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan / penyaringan dan dokumentasi bukti digital dalam kejahatan komputer. Sedangkan menurut Budhisantoso, digital forensik merupakan kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum[3]. Maka dapat disimpulkan bahwa digital forensik adalah suatu aktivitas mengidentifikasi dan menganalisa data dari sistem komputer untuk pengambilan dokumentasi bukti digital yang dapat digunakan sebagai alat bukti untuk mengungkap kasus kejahatan dalam penegakan hukum.

2.3. Tujuan Algoritma Breadth First Search dalam Digital Forensik

Sebelumnya, dalam hal ini algoritma BFS digunakan untuk menganalisis struktur data digital untuk membantu penyelidik memahami penyimpanan data dan diorganisir dalam struktur hierarkis seperti sistem file. Selain itu, algoritma ini bertujuan untuk mencari bukti digital, merekonstruksi riwayat aktivitas digital untuk membantu penyelidik melacak dan memahami peristiwa yang terjadi dalam lingkungan digital. Oleh karena itu BFS digunakan untuk menganalisis, mencari bukti, merekonstruksi, memulihkan, dan melindungi informasi digital penting untuk investigasi dan penegakkan hukum

3. Pengumpulan Data dan Preprocessing Data yang Dilakukan

3.1. Pengumpulan Data dalam Digital Forensik

Pengumpulan data dalam digital forensik adalah langkah kunci untuk mengumpulkan bukti digital yang dapat digunakan dalam penyelidikan atau peradilan. Berikut adalah langkah-langkah umum yang dilakukan dalam proses pengumpulan data dalam digital forensik:

1. Identifikasi dan Perencanaan: Identifikasi jenis bukti digital yang mungkin relevan untuk penyelidikan kemudian rencanakan pendekatan dan metode pengumpulan data berdasarkan jenis perangkat atau sistem yang akan diselidiki.
2. Pemeliharaan Keaslian (Preservation of Evidence): Pastikan untuk memelihara keaslian bukti digital. Jangan mengubah atau menghapus data yang ada pada perangkat atau sistem yang diselidiki serta gunakan metode yang memungkinkan pengambilan data tanpa mengubah isi dari perangkat atau media penyimpanan.
3. Identifikasi dan Amankan Lokasi: Tentukan lokasi fisik dan logis dari perangkat atau sistem yang akan diselidiki. Amankan dan jaga lokasi fisik agar tidak ada yang dapat mengakses atau merusak bukti digital.
4. Peralatan Pengumpulan Data: Gunakan peralatan forensik digital yang sesuai, seperti write-blocking devices, untuk memastikan data tidak berubah selama proses pengumpulan. Pilih perangkat lunak forensik yang sesuai untuk menduplikasi dan menganalisis data.
5. Duplikasi Data (Imaging): Duplikasi penuh (bit-for-bit) dari perangkat atau media penyimpanan adalah kunci. Ini menciptakan salinan yang identik dengan data asli. Pastikan bahwa duplikasi dilakukan dengan benar dan verifikasi keasliannya.
6. Catat Informasi Kontekstual: Catat informasi kontekstual seperti tanggal, waktu, lokasi, dan siapa yang terlibat dalam proses pengumpulan data. Dokumentasikan setiap langkah yang diambil selama proses pengumpulan.
7. Pengumpulan Data: Ambil data yang relevan sesuai dengan rencana pengumpulan yang telah dibuat. Ambil data secara menyeluruh termasuk data terhapus, log, dan metadata.
8. Validasi Data: Validasi integritas data setelah pengumpulan untuk memastikan bahwa duplikasi akurat dan tidak terjadi kerusakan data. Gunakan hash function untuk membandingkan nilai hash dari data asli dan duplikasi.
9. Pembuatan Laporan: Buat laporan forensik yang mencakup semua langkah yang diambil selama proses pengumpulan data. Sertakan temuan, analisis, dan bukti digital yang relevan.
10. Pengadilan: Jika proses forensik digital tersebut berkaitan dengan investigasi hukum atau peradilan, pastikan untuk mematuhi prosedur hukum yang berlaku dan persyaratan pengadilan.

Penting untuk diingat bahwa dalam setiap kasus digital forensik, integritas dan keaslian bukti harus dijaga dengan sangat hati-hati untuk memastikan keberlakuannya dalam proses hukum. Selalu konsultasikan dengan ahli forensik digital atau profesional hukum yang berpengalaman jika Anda tidak yakin atau jika bukti tersebut akan digunakan dalam konteks hukum.

3.2. Preprocessing Data dalam Digital Forensik

Preprocessing data dalam konteks forensik digital melibatkan serangkaian langkah untuk membersihkan, mengorganisir, dan mempersiapkan data agar dapat digunakan dengan efektif dalam analisis forensik. Berikut adalah beberapa langkah umum untuk preprocessing data pada data forensik:

1. Pengumpulan Data: Kumpulkan data forensik dari sumber-sumber yang relevan, seperti sistem file, log, rekaman memori, dan data jaringan.
2. Identifikasi dan Ekstraksi Metadata: Identifikasi dan ekstrak metadata yang terkait dengan entitas digital, seperti file atau aktivitas jaringan. Ini bisa mencakup waktu pembuatan, pemilik, ukuran, dan atribut lainnya.
3. Handling Missing Values: Tangani nilai-nilai yang hilang. Ini bisa terjadi pada data forensik karena berbagai alasan, dan dapat mempengaruhi analisis. Misalnya, pertimbangkan untuk mengisi nilai yang hilang atau menghapus entitas dengan nilai yang hilang, tergantung pada konteks dan dampaknya terhadap analisis.
4. Pembersihan Data: Bersihkan data dari noise, outlier, atau informasi yang tidak relevan. Hal ini dapat melibatkan penghapusan entitas atau aktivitas yang tidak mendukung tujuan analisis forensik Anda.
5. Encoding Kategori: Jika diperlukan, ubah variabel kategori menjadi bentuk yang dapat diolah oleh algoritma. Ini termasuk penggunaan one-hot encoding atau label encoding untuk entitas atau atribut kategori.
6. Scaling dan Normalisasi: Scaling atau normalisasi fitur-fitur yang relevan. Misalnya, jika Anda bekerja dengan data yang mencakup berbagai satuan (seperti waktu dan ukuran file), pastikan untuk menormalkan data sehingga mereka berada dalam skala yang serupa.
7. Deteksi dan Penanganan Outlier: Identifikasi dan tangani nilai-nilai outlier yang dapat mempengaruhi interpretasi atau analisis. Teknik statistik atau visualisasi dapat digunakan untuk mendeteksi outlier.

8. Pemrosesan Teks (Jika Diperlukan): Jika data forensik Anda mencakup teks, lakukan pemrosesan teks seperti tokenisasi, penghapusan stopwords, dan normalisasi teks.
9. Pemisahan Data: Pisahkan data menjadi set pelatihan dan pengujian jika Anda berencana untuk melatih model machine learning atau melakukan validasi.
10. Visualisasi Data: Gunakan visualisasi data untuk memahami distribusi, korelasi, dan trend dalam data. Ini dapat membantu dalam pengambilan keputusan saat merancang model atau analisis forensik.
11. Penggabungan Data (Opsional): Gabungkan data dari berbagai sumber jika diperlukan untuk mendapatkan gambaran yang lebih lengkap atau menyelidiki hubungan antar-entitas.
12. Pengamatan dan Verifikasi Data: Tinjau data secara menyeluruh untuk memastikan bahwa tidak ada informasi yang hilang atau proses yang diperlukan lebih lanjut sebelum melakukan analisis lebih lanjut.

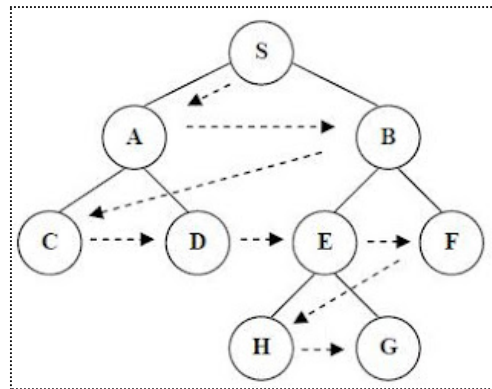
Setelah langkah-langkah preprocessing ini selesai, data forensik Anda akan lebih siap untuk analisis lebih lanjut, termasuk penggunaan algoritma forensik seperti BFS atau metode analisis forensik lainnya. Pastikan untuk selalu mempertimbangkan kebutuhan dan karakteristik unik dari data forensik yang Anda tangani.

BAB II

ARSITEKTUR DAN INTEGRASI ALGORITMA BFS

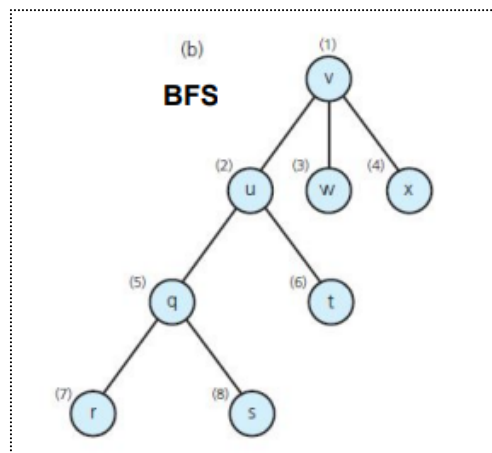
1. Definisi Algoritma BFS (*Breadth First Search*)

Algoritma BFS (*Breadth First Search*) dikenal juga dengan nama algoritma pencarian melebar adalah sebuah teknik umum yang digunakan untuk melakukan traversal pada graf. Secara ringkas, algoritma ini memiliki prosedur: traversal dimulai dari simpul, kunjungi semua simpul, kunjungi semua simpul yang bertetangga dengan simpul v terlebih dahulu, kunjungi simpul yang belum dikunjungi dan bertetangga dengan simpul – simpul yang tadi dikunjungi, demikian seterusnya. Pencarian dalam algoritma BFS dilakukan secara sistematis, artinya biasanya dikunjungi dalam satu arah, misalnya dari simpul paling kiri ke simpul paling kanan. Penelusuran simpul juga dilakukan dalam satu arah terlebih dahulu sebelum mengunjungi simpul pada arah yang lebih tinggi.



Gambar 1. Contoh Penyelesaian dengan Algoritma BFS

Dalam implementasinya, algoritma BFS memerlukan matriks ketetanggaan $A = [a_{ij}]$ yang berukuran $n \times n$, antrean q untuk menyimpan simpul yang telah dikunjungi, dan tabel boolean dikunjungi.



Gambar 2. Pohon Pencarian Algoritma BFS

2. Penerapan Algoritma BFS dalam digital forensik

Digital forensik adalah bidang yang berkaitan dengan identifikasi, pengumpulan, analisis, dan interpretasi informasi elektronik untuk mendukung penyelidikan atau pengadilan. Algoritma BFS (Breadth-First Search) dapat diterapkan dalam konteks digital forensik untuk mengeksplorasi dan menganalisis struktur data, seperti sistem file atau jaringan komputer.

Arsitektur Digital Forensik:

1. Pengumpulan Bukti (Acquisition):

- Mendapatkan salinan atau snapshot dari media digital yang akan dianalisis (hard drive, USB drive, dll.).
- Memastikan bahwa proses pengumpulan tidak merusak atau mengubah data asli.

2. Identifikasi dan Preservasi (Identification and Preservation):

- Mengidentifikasi jenis data yang ada dan memilih metode preservasi yang sesuai.
- Memastikan integritas dan keaslian data yang disimpan.

3. Analisis (Analysis):

- Menganalisis data untuk mengidentifikasi bukti digital yang relevan.
- Memahami struktur data yang mungkin terlibat (file system, database, dll.).

4. Rekonstruksi dan Restorasi (Reconstruction and Restoration):

- Merekonstruksi kejadian atau aktivitas yang mungkin telah terjadi.
- Memulihkan data yang mungkin telah dihapus atau diubah.

5. Riwayat (Timeline Analysis):

- Membangun timeline dari aktivitas digital untuk membantu dalam pemahaman kronologi kejadian.

Algoritma BFS dalam Digital Forensik:

Algoritma BFS dapat digunakan dalam beberapa konteks dalam analisis forensik, terutama untuk eksplorasi struktur data tertentu, seperti sistem file. Dalam analisis Sistem File:


- Menjelajahi struktur sistem file menggunakan BFS untuk mengidentifikasi file, direktori, dan hubungan hirarki antar mereka.
- Mencari tanda-tanda aktivitas mencurigakan, seperti pembuatan atau penghapusan file secara tiba-tiba.

Algoritma BFS memungkinkan eksplorasi secara sistematis dari suatu struktur data, membantu mengungkap pola dan hubungan yang mungkin tidak terlihat secara langsung. Dalam konteks digital forensik, ini dapat membantu dalam pengumpulan bukti dan analisis yang lebih efektif.

2.1. Implementasi Algoritma BFS dalam pencarian file

Pada penerapan algoritma yang akan dibangun, user dapat mengetahui jenis file yang ada pada tanggal yang dimaksudkan file tersebut rusak atau diretas.

1.Pencarian Berdasarkan Tanggal

Search by Date: 


- No files found for the selected date.

2.Hasil Pencarian

- WhatsApp Image 2023-11-27 at 16.15.26 (1).jpeg - 2023-11-29 13:22:52 [Download](#)
- WhatsApp Image 2023-11-27 at 16.15.26 (1).jpeg - 2023-11-29 13:22:56 [Download](#)

3.File dapat di download dan di upload

Welcome to File Management System

Choose a file: No file chosen
Search by Date: 

- WhatsApp Image 2023-11-27 at 16.15.26 (1).jpeg - 2023-11-29 13:22:52 [Download](#)
- WhatsApp Image 2023-11-27 at 16.15.26 (1).jpeg - 2023-11-29 13:22:56 [Download](#)

2.2. Implementasi Algoritma BFS dalam Melakukan *Digital Trace Detection*

Dalam hal ini Implementasi BFS dalam *Digital Trace Detection* adalah :

- Database Interactions:
Menggunakan SQLAlchemy untuk berinteraksi dengan database SQLite (files.db), mencatat setiap file yang diunggah.gm
- File Uploads:

Jejak file dapat ditemukan di dalam direktori yang ditentukan. Informasi file juga disimpan dalam database.

- Date and Time Stamps:

Tanggal dan waktu unggah dicatat, memungkinkan pencarian berdasarkan

Melalui analisis forensik digital, jejak digital ini dapat digunakan untuk melacak aktivitas pengguna, file yang diunggah, dan interaksi dengan sistem. Ini dapat mendukung deteksi atau penyelidikan keamanan