BAB I

PENDAHULUAN

1.1 Latar Belakang

Identifikasi tipe *file* adalah tugas yang sangat kompleks bagi pemeriksa forensik digital (Karampidis & Papadourakis, 2017). Analisis terhadap ekstensi *file* diperlukan untuk membantu dalam upaya mendeteksi manipulasi suatu *file* menggunakan metode modifikasi yang bertujuan menyembunyikan isi dari wujud sebenarnya (Hegarty & Haggerty, 2016). Apabila ekstensi suatu *file* diubah dari ekstensi aslinya maka aplikasi yang biasa digunakan untuk menjalankan *file* tidak bisa mengidentifikasi. Permasalahan tersebut keamanan yang harus diperbaiki dalam proses pertumbuhan teknologi saat ini dikarenakan para pelaku kejahatan sering memanipulasi keaslian suatu *file* (Ardiansyah dkk., 2020).

Penelitian yang berhubungan dengan modifikasi *file* pernah dilakukan sebelumnya: mengubah ekstensi *file* untuk mengelabui sistem operasi. Penelitian ini dilakukan oleh Michael Yip, mencoba mengubah ekstensi *file* gambar dari .jpg ke .doc yang memberikan bukti bahwa betapa mudahnya mengelabui *operating system* untuk menampilkan jenis *file* yang salah hanya dengan mengubah ekstensi *file* dan bagaimana melakukan pemeriksaan *signature file* menggunakan alat bantu *HexEdit* untuk mengetahui orisinalitas ekstensi suatu *file*. Pemeriksaan secara manual terhadap *signature file* dengan menggunakan *HexEdi*t untuk mengetahui ekstensi *file* yang sesuai memerlukan waktu yang lama (Yip, 2008).

Implementasi yang lebih komprehensif diperlukan untuk mendukung proses komputer forensik terhadap identifikasi *file.* Analisis *signature file* dapat dimanfaatkan untuk mendeteksi tindak kejahatan yang memanfaatkan teknik manipulasi pada ekstensi *file* untuk menyembunyikan bentuk aslinya. Agar sistem operasi modern dapat mengenali data sebagai *file* terkait, informasi seperti ekstensi *file* atau *signature file* harus ada. Dengan menetapkan jenis *file* secara otomatis, proses manual akan berkurang secara signifikan (E. Daniel, 2014).

Penelitian ini memperkenalkan aplikasi *File Signature Analyzer 2.0* sebuah alat yang dirancang untuk melakukan analisis terhadap *file-file* dengan mempertimbangkan metadata seperti ekstensi, *signature* dan *mimetype*. Fokus utama dari pembuatan aplikasi ini adalah kemampuannya untuk secara otomatis mengidentifikasi jenis ekstensi *file*. Sebelumnya, telah dibuat aplikasi File Signature Analyzer 1.0 yang mendukung analisis 150 ekstensi file, namun memiliki keterbatasan dalam proses unggah *file* hanya mendukung satu *file* dalam satu sesi analisis. Aplikasi terbaru, *File Signature Analyzer 2.0*, telah ditingkatkan untuk mendukung hingga 196 ekstensi *file* dan 269 signature, serta memungkinkan pengguna untuk mengunggah hingga 5 *file* sekaligus dalam satu sesi analisis.

1.2 Rumusan Masalah

Berdasarkan latar belakang sebelumnya, maka rumusan masalah dari penelitian adalah bagaimana menganalisa dan menentukan orisinalitas ekstensi *file* secara otomatis?

1.3 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah, maka tujuan penelitian ini adalah Menganalisa orisinalitas ekstensi *file* dan menentukan ekstensi *file* secara otomatis menggunakan aplikasi *File Signature Analyzer* 2.0.

1.4 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Bagi Penulis

   Implementasi studi kasus mengenai teknologi yang akan diterapkan pada *File Signature Analyzer* 2.0.

2. Bagi Pengguna

   Membantu untuk mempermudah proses identifikasi keaslian dari suatu *file*. Bila diperlukan bisa digunakan oleh pihak yang berwajib untuk mempermudah dalam proses penyelidikan digital forensik terkhusus mengenai identifikasi orisinalitas *file*.

1.5 Batasan Masalah

Batasan masalah penelitian ini sebagai berikut:

1. Penelitian ini tidak membahas stuktur file sistem secara mendalam.
2. Penelitian ini tidak membahas forensik secara mendalam namun hanya pada studi kasus mendeteksi file berdasarkan signature.
3. Aplikasi *File Signature Analyzer* 2.0 mendukung 196 ekstensi file dan 269 signature.

4. Pengujian aplikasi *File Signature Analyzer* 2.0 dilakukan secara lokal komputer dengan menggunakan sampel file yang didapatkan dari: *https://filesamples.com/*.