Performance Analysis of Forensic Programs on SQLite Corpus

Indra Jaya Kusuma

[1,2,3]Faculty of Informatics, Telkom University, Bandung
Jl. Telekomunikasi No.1, Bandung, Indonesia
e-mail : wolferker@students.telkomuniversity.ac.id

Abstract
Tujuan penelitian ini adalah untuk mengevaluasi performa berbagai program forensik pada korpus dengan program SQLite. Penulis mencoba mewakili beragam ukuran dan struktur basis data. Program-program forensik dijalankan pada berbagai versi SQLite. Namun, perlu diperhatikan bahwa karakteristik kinerja spesifik dari program-program tersebut dapat bervariasi tergantung pada karakteristik spesifik dari database yang sedang dianalisis dan versi SQLite tersebut. Secara keseluruhan, penelitian ini bertujuan untuk memberikan wawasan yang berharga tentang kinerja program-program forensik pada basis data SQLite dan dapat digunakan untuk menginformasikan pemilihan alat untuk analisis forensic.

Kata kunci : forensik, korpus, performa, analisis

Abstract
The goal of this study was to evaluate the performance of various forensic programs on a corpus of SQLite databases. Author is trying to represent a diverse range of database sizes and structures. The forensic programs were run on various SQLite version. However, it should be noted that the specific performance characteristics of the programs may vary depending on the specific characteristics of the database being analyzed and versions of said SQLite. Overall, this study aim to provide valuable insights into the performance of forensic programs on SQLite databases and can be used to inform the selection of tools for forensic analysis.

Keywords: forensic, corpus, performance, analysis

1. Introduction

Forensic analysis plays a crucial role in the field of digital forensics, as it allows for the identification and analysis of digital evidence from computers, mobile devices, and other electronic media. The use of forensic software is a common approach to facilitate this process, as it provides a range of tools and techniques to extract, analyze, and report on digital evidence. However, with the increasing number of forensic programs available, it is important to evaluate their performance in order to select the most suitable tool for a given task.

Developments in forensic research, tools, and process over the past decade have been very successful and many in leadership positions now rely on these tools on a regular basis frequently without realizing it.[1]

As such, SQLite is one of the popular tools to make use. For instance, the mobile messaging program WhatsApp, which has over 2.24 billion users on June 2022.[2] and is one of the most popular communication channels worldwide, uses SQLite as its storage format.

SQLite, however, is not just for mobile applications. For instance, SQLite is used by well-known web browsers like Firefox.[3] and Chrome.[4]. In addition to storing application data, SQLite is also used to store meta data, including bookmarks, history, and login information.

Therefore, it is crucial to extract all data connected to a SQLite database from the perspective of IT forensics. The acquisition of deleted SQLite data is challenging, even though the extraction of allocated database information is simple.

As such, there are a few tools that will be introduced in this paper. Firstly, SQLite Expert Professional. SQLite Expert Professional is its intuitive and user-friendly interface, which makes it easy to create, edit, and manage SQLite databases. The software offers a variety of visual tools and wizards that simplify the process of designing and modifying database schema, as well as importing and exporting data. Secondly, SQLite Doctor has advantages that make it an ideal choice for working with SQLite databases. it has a user-friendly interface that allows users to easily navigate through the various functions and tools available. SQLite Browser as a open-source software is actively developed and maintained by a dedicated team of contributors, ensuring that the software remains up-to-date and responsive to the needs of its users. SQLite Studio have an intuitive graphical interface, which allows users to view and modify database schema with ease, The software provides a variety of tools for advanced SQL queries and a built-in query builder. Lastly, SQLite DB Recovery is a specialized tool uses advanced algorithms that can scan even corrupt database file and extract as much data as possible.

The goal of this study was to evaluate the performance of various forensic programs on a corpus with the use of SQLite. SQLite itself is a widely used database management system(DBMS) that is commonly found in wide range of applications, including mobile devices, various operating services, web browsers, and IoT devices[5]. The datasets used in the analysis represented a diverse range of database sizes and structures.

1.1 Problem Identification

Within this studies, we focus testing several SQLite versions in order to compare the capabilities of each versions in order to identify whether those versions are able to process corpus correctly. The problems that will be discussed in this research are listed as :

A. How to perform forensic analysis on SQLite Corpus using SQLite Expert Professional?
B. How to perform forensic analysis on SQLite Corpus using SQLite Doctor?
C. How to perform forensic analysis on SQLite Corpus using SQLite Browser?
D. How to perform forensic analysis on SQLite Corpus using SQLite Studio?
E. How to perform forensic analysis on SQLite Corpus using SQLite DB Recovery?

1.2 Contributions

In this paper, We are using some of the corpus used in “A standardized corpus for SQLite database forensics” (Garfinkel et al) [6], which follows a standardized corpus. The main contribution of this research are the following :

A. Performing forensic analysis on SQLite Corpus using SQLite Expert Professional
B. Performing forensic analysis on SQLite Corpus using SQLite Doctor
C. Performing forensic analysis on SQLite Corpus using SQLite Browser
D. Performing forensic analysis on SQLite Corpus using SQLite Studio
E. Performing forensic analysis on SQLite Corpus using SQLite DB Recovery

1.3 Scope

A. The SQLite Corpus that will be analyzed is from the paper made by Garfinkel et.al. which follows a standardized corpus dataset.
B. The comprehension of analyzing SQLite Corpus using SQLite Expert Professional
C. The comprehension of analyzing SQLite Corpus using SQLite Doctor
D. The comprehension of analyzing SQLite Corpus using SQLite Browser
E. The comprehension of analyzing SQLite Corpus using SQLite Studio
F. The comprehension of analyzing SQLite Corpus using SQLite DB Recovery

1.4 Research Plan

The research plan is depicted by the following figure.

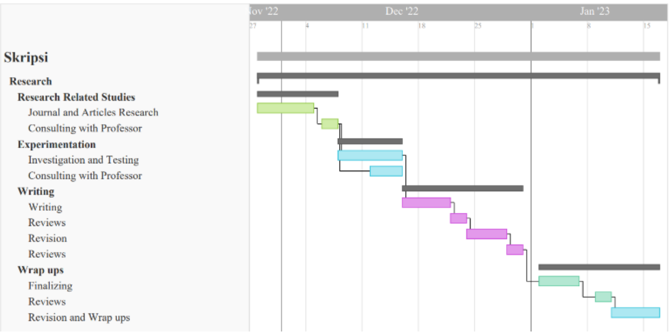

Figure 1. Research Plan Gantt Chart