ITMS 538 Assignment 06c_s

Alan Palayil
Due Date: 12/06/2022

Database Forensics

During this lab, we must work with database files and use various tools to look over the various categories. In the lab, we have steps to install each of the tools in RADISH Windows 10 along with the initial set up. We use 'DB Browser for SQLite' and 'Notepad++' to refer with the other tools. I am writing a brief description of each tool along their strengths and weaknesses.

SQLite Forensic Explorer (SFE) is a commercial database forensic tool that gives users access to SQLite databases and allows for their analysis. It can extract and analyze SQLite database objects as well as the data that is associated with them, as well as reconstruct SQLite database files that have been deleted or corrupted. It's possible that the demo version has limited features because we're using it. The purpose of SQLite Forensic Explorer is to make it simple and quick for investigators to retrieve deleted SQLite database records and tables. Overwritten records can be viewed, but overwritten tables cannot be recovered, and it can partially recover deleted tables and records. In addition, it is unable to examine unallocated freeblock and freelist areas or detect deleted overflow pages.

SQLite Database Recovery (SDR) is a piece of software that helps users recover data from SQLite databases that have been damaged or corrupted. It can carry out a deep scan of an SQLite database to identify any corruption and retrieve data from the database. It can also view and export the recovered data in CSV, HTML, and XML, among other formats. Overwritten records can be viewed, but tables cannot be detected or recovered by the tool. However, it is unable to examine unallocated freeblock and freelist areas or detect deleted overflow pages.

Several Python plugins designed specifically for SQLite are included in the open-source digital forensics platform known as Autopsy. Data can be analyzed and recovered from SQLite databases with the help of these plugins. The recovered data can be exported in a variety of formats using Autopsy, including CSV, HTML, and XML. This device can be utilized to recuperate erased records, tables, and flood pages from SQLite information bases. Additionally, it helps recover unallocated freeblock and freelist areas. It does not support the recovery of tables and records that have been overwritten.

FQLite is a powerful forensic tool for SQLite databases that can be used to analyze and retrieve data. Users can analyze and extract data from SQLite databases with its many features. It can find and restore databases that have been deleted or damaged; and can export the recovered data in CSV, HTML, and XML formats, among others. It can be used to retrieve deleted SQLite database records and tables. It can also retrieve deleted overflow pages and overwritten records and tables. However, recovering unallocated freeblock and freelist areas is not supported.

Both SQLite Forensic Explorer and SQLite Database Recovery are intended to assist investigators in quickly and easily retrieving deleted SQLite database records and tables. However, unlike SQLite Database Recovery, SQLite Forensic Explorer does not allow for the recovery of unallocated areas of freeblocks and freelists. Both FQLite and Autopsy, which are Python plugins for SQLite, can recover deleted records, tables, and overflow pages from SQLite databases. FQLite, on the other hand, does support the recovery of overwritten records and tables, whereas

Autopsy (SQLite-specific Python plugins) does not. Lastly, neither FQLite nor Autopsy (SQLite-specific Python plugins) support recovering unallocated freeblock and freelist areas.

DB Forensic Tool Comparison

Category	Database	Database Forensic Tools			
		SQLite Forensic Explorer	***SQLite Database Recovery***	***Autopsy***	***FQLite***
Deleted Tables	0A-05.db	No	No	No	Yes
Overwritten Tables	0B-02.db	No	No	No	Yes
Deleted Records	0C-10.db	Partial	No	Partial	Yes
Overwritten records	0D-08.db	Yes	Yes	No	Yes
Deleted overflow pages	0E-02.db	No	No	Yes	Yes
Unallocated areas - freeblock	17-13-antifor.db	Yes	No	Yes	No
Unallocated areas - freelist	18-01-antifor.db	Yes	No	Yes	No

URL:
https://docs.google.com/spreadsheets/d/1nVOGM7NuDBaVMXAiFuSHPc4vkVJ5I36i8Ya2g07-TRc/edit?usp=sharing