

November 2021

Test Results for SQLite Data Recovery Tool:
Magnet Forensics Axiom Examine v5.5.1.26621

Contents

| | |
|---------------------------------|---|
| Introduction..... | 1 |
| How to Read This Report | 1 |
| 1 Results Summary | 2 |
| 2 Testing Environment..... | 3 |
| 2.1 Execution Environment | 3 |
| 2.2 SQLite Data | 3 |
| 3 Test Results..... | 4 |
| 3.1 SQLite Data Recovery | 5 |

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology (NIST) Special Programs Office and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense's Cyber Crime Center, U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, as well as the DHS Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensics tools is based on well-recognized methodologies for conformance and quality testing. Interested parties in the computer forensics community can review and comment on the specifications and test methods posted on the CFTT Website (<https://www.cftt.nist.gov/>).

This document reports the results from testing Magnet Forensics Axiom Examine v5.5.1.26621 for SQLite data recovery, including: displaying recovered SQLite database information, and identifying, categorizing and reporting Write-Ahead Log (WAL), Rollback Journal data and sequence WAL journal data.

Test results from other tools can be found on the S&T-sponsored digital forensics webpage, <https://www.dhs.gov/science-and-technology/nist-cftt-reports>.

How to Read This Report

This report is divided into four sections. Section 1 identifies and provides a summary of any significant anomalies observed in the test runs. This section is sufficient for most readers to assess the suitability of the tool for the intended use. Section 2 lists testing environment and SQLite data objects used for testing. Section 3 provides an overview of the test case results reported by the tool.

Test Results for SQLite Data Recovery

Tool Tested: Axiom Examine
Software Version: v5.5.1.26621
Supplier: Magnet Forensics
Address: 2250 Corporate Park Drive, Suite 130
Herndon, VA 20171
Fax: 1-844-638-7884
WWW: magnetforensics.com

1 Results Summary

Magnet Forensics Axiom Examine v5.5.1.26621 was tested for its ability to report recovered SQLite database information. Except for the following anomalies, the tool was able to report and recover all supported data objects completely and accurately.

Axiom Examine v5.5.1.26621 is designed exclusively as an SQLite Viewer. Therefore, SQLite header parsing, data recovery, and other tests not supported by the tool are marked as Not Applicable (NA).

For more test result details see section 2.

2 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the selected test execution environment, and the data objects populated for SQLite data recovery.

2.1 Execution Environment

Magnet Forensics Examine v5.5.1.26621 was installed on Windows 10 Pro version 10.0.14393.

2.2 SQLite Data

Magnet Forensics Examine v5.5.1.26621 was measured by its ability to report recovered SQLite database information. SQLite versions 3.19.0 (Android) and 3.32.3 iPhone Operating System (iOS) were used when creating the SQLite databases. These versions are the most current versions running on Android and iOS. Table 2 below defines the SQLite data tested per each test case.

| Test Case | Data |
|---|---|
| SQLite Forensic Tool (SFT)-01: SQLite header parsing | <i>Page Size (4096, 1024, 8192)</i> |
| | <i>Journal Mode Information (Write-Ahead Log (WAL), PERSIST, OFF)</i> |
| | <i>Number of Pages</i> |
| | <i>UTF(Unicode Transformation Format)-8</i> |
| | <i>UTF-16 (Little Endian) LE</i> |
| | <i>UTF-16 (Big Endian) BE</i> |
| SFT-02: SQLite Schema Reporting | <i>Table Names</i> |
| | <i>Column Names per Table</i> |
| | <i>Row Information per Table</i> |
| SFT-03: SQLite Recoverable Rows | <i>Source filename</i> |
| | <i>Row Status: Deleted</i> |
| | <i>Row Status: Modified</i> |
| SFT-04: SQLite Data Element Metadata | <i>Source filename</i> |
| | <i>Row Status: Deleted</i> |
| | <i>Row Status: Modified</i> |
| SFT-05: SQLite Schema Data Reporting | <i>Primary Key</i> |
| | <i>Integer (Int)</i> |
| | <i>Float</i> |
| | <i>Text</i> |
| | <i>Binary Large Object (BLOB) (bmp, gif, heic, jpg, pdf, png, tiff)</i> |
| | <i>Boolean</i> |
| SFT-06: Recovered Row Metadata | <i>Source Filename</i> |
| | <i>Row Status: Deleted</i> |
| | <i>Row Status: Modified</i> |
| SFT-07: SQLite Recovered Data Information | <i>File Offset, length</i> |
| | <i>Table name associated with Row</i> |

Table 1: SQLite Data Objects

3 Test Results

This section provides the test case results reported by the tool. Section 3.1 identifies the PRAGMA journal mode (i.e., WAL, PERSIST, OFF), test cases, and associated data checked within individual test cases.

Magnet Forensics Axiom Examine v5.5.1.26621 was tested for its ability to report recovered SQLite database information.

The *Test Cases* column in section 3.1 is comprised of two sub-columns that define a particular test category, and individual sub-categories that are verified when testing. The results are as follows:

As Expected: the SQLite data recovery tool returned expected test results.

Partial: the SQLite data recovery tool returned some of the data.

Not As Expected: the SQLite data recovery tool failed to return expected test results.

Not Applicable (NA): the tool does not provide support, or the test assertion is optional.

3.1 SQLite Data Recovery

SQLite data recovery was testing with Magnet Forensics Axiom Examine v5.5.1.26621.

All test cases that are supported by the tool's functionality were successful.

See Table 2 below for more details.

| Axiom v5.5.1.26621 | | | | |
|---|----------------------------|---------------------|-------------|-------------|
| Test Cases – SQLite Data Recovery | | PRAGMA Journal Mode | | |
| | | WAL | PERSIST | OFF |
| SFT-01: Header Parsing | Page Size | NA | NA | NA |
| | Journal Mode Info | NA | NA | NA |
| | Number of Pages | NA | NA | NA |
| | UTF-8 | NA | NA | NA |
| | UTF-16LE | NA | NA | NA |
| | UTF-16BE | NA | NA | NA |
| | Hash Value (MD5, SHA) | As Expected | As Expected | As Expected |
| SFT-02: Schema Reporting | Table Name | As Expected | As Expected | As Expected |
| | Column Name | As Expected | As Expected | As Expected |
| | Number of Rows | As Expected | As Expected | As Expected |
| SFT-03: Recoverable Rows | Deleted | NA | NA | NA |
| | Modified | NA | NA | NA |
| SFT-04: Data Element Metadata Reporting (Source filename) | Deleted | NA | NA | NA |
| | Modified | NA | NA | NA |
| SFT-05: Schema Data Reporting | Primary Key | NA | NA | NA |
| | Int | NA | NA | NA |
| | Float | NA | NA | NA |
| | Text | NA | NA | NA |
| | BLOB Data: .bmp | As Expected | As Expected | As Expected |
| | BLOB data: .gif | As Expected | As Expected | As Expected |
| | BLOB Data: .heic | NA | NA | NA |
| | BLOB data: .jpg | As Expected | As Expected | As Expected |
| | BLOB data: .pdf | NA | NA | NA |
| | BLOB data: .png | As Expected | As Expected | As Expected |
| Boolean | NA | NA | NA | |
| SFT-06: Recovered Row Metadata | Source Filename | As Expected | As Expected | As Expected |
| | Status: Modified | NA | NA | NA |
| | Status: Deleted | NA | NA | NA |
| SFT-07: Recovered Data Info | File offset | NA | NA | NA |
| | Recovered Row - Table Name | NA | NA | NA |

Table 2: SQLite Data Recovery