January 2023

Test Results for Mobile Device Acquisition Tool:
Cellebrite Physical Analyzer v7.58.0.66

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), the National Institute of Justice, and the National Institute of Standards and Technology's (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 Cyber Crime Center, U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, and 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 Web site (https://www.cftt.nist.gov/).

Test results from other tools can be found on the DHS S&T sponsored digital forensics web page, http://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 identifies the mobile devices used for testing. Section 3 lists testing environment, the internal memory data objects used to populate the mobile devices. Section 4 provides an overview of the test case results reported by the tool.

Test Results for SQLite Data Recovery Tool

Tool Tested: Physical Analyzer

Software Version: v7.58.0.66

Supplier: Cellebrite, Inc.

Address: 7 Campus Drive, Suite 210, Parsippany, NJ 07054

Phone: (415) 361-4077

WWW: cellebrite.com

1 Results Summary

Cellebrite Physical Analyzer v7.58.0.66 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.

SQLite Header Parsing:

- PRAGMA journal mode = WAL, PERSIST, and OFF are not reported.
- PRAGMA encoding = UTF8, UTF16LE, UTF16BE are not reported.
- PRAGMA page_size = 1024, 4096, 8192 are not reported.
- PRAGMA Foreign keys = OFF is not reported.

SQLite Schema Data Reporting:

- BLOB data containing *pdf* files are not displayed.

For more test result details see section 3.

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

Cellebrite Physical Analyzer v7.58.0.66 was installed on Windows 10 Pro version 10.0.19044.2130.

2.2 SQLite Data

Cellebrite Physical Analyzer v7.58.0.66 was measured by its ability to report recovered SQLite database information. SQLite versions 3.19.0 (Android) and 3.32.3 (iOS) were used when creating the SQLite databases. These versions are the most current versions running on Android and iOS. Table 1 below defines the SQLite data tested per each test case.

Test Case	Data
SFT-01: SQLite Header Parsing	*Page Size (4096, 1024, 8192)* *Journal Mode Information (WAL, PERSIST, OFF)* *Number of Pages* *UTF-8* *UTF-16LE* *UTF-16BE*
SFT-02: SQLite Schema Reporting	*Table Names* *Column Names per Table* *Row Information per Table*
SFT-03: SQLite Recoverable Rows	*Source filename* *Row Status: Deleted* *Row Status: Modified*
SFT-04: SQLite Data Element Metadata	*Source filename* *Row Status: Deleted* *Row Status: Modified*
SFT-05: SQLite Schema Data Reporting	*Primary Key* *Int* *Float* *Text* *BLOB (bmp, gif, heic, jpg, pdf, png, tiff)* *Boolean*
SFT-06: Recovered Row Metadata	*Source Filename* *Row Status: Deleted* *Row Status: Modified*
SFT-07: SQLite Recovered Data Information	*File Offset, length* *Table name associated with Row*

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.

Cellebrite Physical Analyzer v7.58.0.66 was tested for its ability to report recovered SQLite database information.

The *Test Cases* column in sections 3.1 are 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 data.

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

Not Applicable (NA): the tool does not provide support.

3.1 SQLite Data Recovery

SQLite data recovery was testing with Cellebrite Physical Analzyer v7.58.0.66.

All test cases were successful with the exception of the following:

- Header information (Page Size, Journal Mode Type, Number of Pages, Encoding Type) is not reported.
- The source filename (db, journal, wal) for deleted and modified records is not reported.
- Graphic files (.pdf) embedded in a BLOB are not displayed.

See Table 2 below for more details.

SQLite Data Recovery
Cellebrite Physical Analyzer v7.58.0.66

Test Cases:	WAL	PERSIST	OFF
SFT-01: **Header Parsing** Page Size	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-01: **Header Parsing** Journal Mode Info	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-01: **Header Parsing** Number of Pages	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-01: **Header Parsing** UTF-8	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-01: **Header Parsing** UTF-16LE	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-01: **Header Parsing** UTF-16BE	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-01: **Header Parsing** Hash Value (MD5, SHA)	*As Expected*	*As Expected*	*As Expected*
SFT-02: **Schema Reporting** Table Name	*As Expected*	*As Expected*	*As Expected*
SFT-02: **Schema Reporting** Column Name	*As Expected*	*As Expected*	*As Expected*

Test Cases:	WAL	PERSIST	OFF
SFT-02: Schema Reporting Number of Rows	*As Expected*	*As Expected*	*As Expected*
SFT-03: Recoverable Rows Deleted	*As Expected*	*As Expected*	*As Expected*
SFT-03: Recoverable Rows Modified	*As Expected*	*As Expected*	*As Expected*
SFT-04: Data Element Metadata Reporting (Source filename) Deleted	*NA*	*NA*	*NA*
SFT-04: Data Element Metadata Reporting (Source filename) Modified	*NA*	*NA*	*NA*
SFT-05: Schema Data Reporting Primary Key	*NA*	*NA*	*NA*
SFT-05: Schema Data Reporting Int	*NA*	*NA*	*NA*
SFT-05: Schema Data Reporting Float	*NA*	*NA*	*NA*
SFT-05: Schema Data Reporting Text	*NA*	*NA*	*NA*
SFT-05: Schema Data Reporting BLOB Data: .bmp	*As Expected*	*As Expected*	*As Expected*
SFT-05: Schema Data Reporting BLOB data: .gif	*As Expected*	*As Expected*	*As Expected*
SFT-05: Schema Data Reporting BLOB Data: .heic	*As Expected*	*As Expected*	*As Expected*
SFT-05: Schema Data Reporting BLOB data: .jpg	*As Expected*	*As Expected*	*As Expected*
SFT-05: Schema Data Reporting BLOB data: .pdf	*Not As Expected*	*Not As Expected*	*Not As Expected*
SFT-05: Schema Data Reporting BLOB data: .png	*As Expected*	*As Expected*	*As Expected*
SFT-05: Schema Data Reporting	*NA*	*NA*	*NA*

Test Cases:	WAL	PERSIST	OFF
Boolean			
SFT-06: Recovered Row Metadata Source Filename	*As Expected*	*As Expected*	*As Expected*
SFT-06: Recovered Row Metadata Status: Modified	*NA*	*NA*	*NA*
SFT-06: Recovered Row Metadata Status: Deleted	*As Expected*	*As Expected*	*As Expected*
SFT-07: Recovered Data Info File Offset	*NA*	*NA*	*NA*
SFT-07: Recovered Data Info Recovered Row - Table Name	*NA*	*NA*	*NA*

Table 2: SQLite Data Recovery