May 2021

Test Results for Forensic Media Preparation Tool:
ATRIO Version 4.0

Federated Testing Suite for Forensic Media Preparation

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security Science and Technology Directorate (DHS 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 Cyber Crime Center, U.S. Internal Revenue Service 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/).

This document reports the results from testing the forensic media preparation function of ATRIO Version 4.0 using the CFTT Federated Testing Test Suite for Forensic Media Preparation, Version 5.

Federated Testing is an expansion of the CFTT program to provide forensic investigators and labs with test materials for tool testing and to support shared test reports. The goal of Federated Testing is to help forensic investigators to test the tools that they use in their labs and to enable sharing of tool test results. CFTT's Federated Testing Forensic Tool Testing Environment and included test suites can be downloaded from http://www.cftt.nist.gov/federated-testing.html and used to test forensic tools. The results can be optionally shared with CFTT, reviewed by CFTT staff, and then shared with the community.

Test results from other tools can be found on DHS's computer forensics web page, https://www.dhs.gov/science-and-technology/nist-cftt-reports.

How to Read This Report

This report is organized into the following sections:

1. **Tool Description:** The tool name, version, and developer information are listed.
2. **Testing Organization:** Contact information and approvals.
3. **Results Summary:** This section identifies any significant anomalies observed in the test runs. This section provides a narrative of key findings identifying where the tool meets expectations and provides a summary of any ways the tool did not meet expectations. The section also provides any observations of interest about the tool or about testing the tool including any observed limitations or organization imposed restrictions on tool use.
4. **Test Environment & Selected Test Configurations:** Description of hardware and software used in tool testing, the test drives used, and a list of the applicable test configurations from the Federated Testing Forensic Media Preparation Test Suite.
5. **Test Results by Test Configuration:** Automatically generated test results that identify anomalies.
6. **Appendix: Additional Details:** Additional administrative details for each test configuration such as, who ran the test, when the test was run, computer used, etc.

Federated Testing Test Results for Forensic Media Preparation Tool: ATRIO Version 4.0

1. Tool Description

Tool Name: ATRIO
Tool Version: 4.0
Tool Developer: ArcPoint Forensics, info@arcpointforensics.com

2. Testing Organization

Organization conducting test: ArcPoint Forensics
Contact: info@arcpointforensics.com
Report date: 28 April 2021
Authored by: Cesar Quezada

This test report was generated using CFTT's Federated Testing Forensic Tool Testing Environment, see Federated Testing Home Page.

3. Results Summary

The tool met expectations with no anomalies.

4. Test Environment & Selected Test Configurations

This section describes the test hardware and software, test configurations, and test drives used in testing.

4.1 Test Hardware and Software

Hardware: Intel NUC

Firmware Version: 0038

Operating System: Kali 2021.1

4.2 Defined Test Configurations

The following table describes each defined configuration of test drive and wipe method.

The columns are as follows:

- **Config:** The test configuration ID.
- **Drive Type:** The drive size category and interface type.
- **Host Interface:** The type of connection used to connect the test drive to the test computer.
- **Connection:** Either *direct* or *bridge*. Indicates if the test drive was connected to the test computer directly or via a bridge. If connected via a bridge, the bridge description is included.
- **Hidden Sectors:** Indicates the presence and type of hidden sectors.
- **Wipe Method:** The selected method for wiping a drive.

Config	Drive Type	Host Interface	Connection	Hidden Sectors	Wipe Method
001	Big USB (any type) > 2TB	USB3	Direct	None	Overwrite

4.3 Test Drive Information and Layouts

The following table describes the test drive and its layout for each test configuration.

- **Config:** The test configuration ID.
- **Drive Type:** The drive size category and interface type.
- **Manufacturer/Model:** The drive manufacturer and model.
- **Drive Size:** The drive size in sectors and Mega/Giga bytes.
- **Hidden Sectors:** The size in sectors of any hidden area and the type of hidden area.

Config	Drive Type	Manufacturer/Model	Drive Size	Hidden Sectors
001	Big USB (any type) > 2TB	Samsung	976,773,168 (465GB)	0

5. Test Results by Test Configuration

This section has two subsections: a summary of the test results and detailed results for each test configuration.

5.1 Results Summary

The following table reports the overall result for each tested configuration. An entry of *Anomaly* in the Results column means that some sectors were not wiped. An entry of *As Expected* in the Results column means that all sectors were completely overwritten or erased.

Config	Drive Type	Host Interface	Connection	Hidden Sectors	Wipe Method	Results
001	Big USB (any type) > 2TB	USB3	direct	None	Overwrite	As Expected

5.2 Test Result Details by Configuration

This section presents the detailed analysis of each test configuration. Each analysis is presented as a table of sector runs for sectors as identified as either *unchanged*, *overwritten*, or *shifted*. A successful test result is for all sectors to be overwritten.

The columns of the tables of sector runs are as follows:

- **Result Type:** Category of result, either *overwritten* or *unchanged*. Sectors that have been relocated (still with original content) are classified as *shifted* and are considered as a variation on *unchanged*.
- **N Sectors:** The number of sectors in the category.
- **N Runs:** The number of sector runs in the category.
- **Start LBA:** For each sector run, this is the LBA of the first sector of the run.
- **End LBA:** For each sector run, this is the LBA of the last sector of the run.
- **Run Length:** For each sector run, the number of sectors in the run.

5.2.1 Test Result Details for Configuration 001

Expected Results: Configuration 001, all sectors overwritten

Result Type	N Sectors	N Runs	Start LBA	End LBA	Run Length
overwritten (hex fill)	976,773,168	1	0	976,773,167	976,773,168

6. Appendix: Additional Details

6.1 Test Configuration Administrative Details

For each test configuration run, the tester, the test computer, and the date the test was run are listed.

Config	Tester	Host	Date
001	CQ	ATRIO	Wed Apr 28 23:41:18 2021

OS: Linux Version 4.13.0-37-generic
Federated Testing Version 5, released 3/12/2020