Paraben E3 Universal v3.8 Cobalt Edition

Test Results for Cloud Data Extraction Tool

February 2024

Science and Technology

February 2024

Test Results for Cloud Data Extraction Tool:
Parben E3 Universal v3.8 Cobalt Edition

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, 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 U.S. 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 Paraben E3 Universal v3.8 Cobalt Edition for extracting supported cloud-based application data.

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 three 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 testing environment and cloud based applications used for testing. Section 3 provides an overview of the test case results reported by the tool.

Test Results for Mobile Device Acquisition Tool

Tool Tested: E3 Universal Cobalt Edition

Software Version: v3.8

Supplier: Paraben Corporation

WWW: paraben.com

1 Results Summary

Paraben E3 Universal v3.8 Cobalt Edition was tested for its ability to extract and report data from supported cloud-based applications.

Except for the following anomalies, the tool acquired and reported all supported cloud-based application data.

Note that tools tested are reporting what is contained within cloud-based applications. Cloud-based applications often modify data (e.g., compressing the file, changing the file name) which results in an inconsistent file names, file sizes and/or hashes compared to the original file uploaded by a user.

Social Media and Messaging data (Facebook):

Note, as per above graphic and vidoes files uploaded to Facebook will be returned as jpg and mp4 files.

NOTE: Some social media applications will compress files as they are uploaded, resulting in inconsistent file size, file names and hash values compared to the original uploaded data files, resulting in different file sizes and hashes. This is reported "as expected" behavior and highlighted with an asterisk.

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 cloud-based data applications used for testing.

2.1 Execution Environment

Paraben E3 Universal v3.8 Cobalt Edition was installed on Windows 10 Pro version 10.0.19042.1586.

2.2 Cloud-based Application Data

Paraben E3 Universal v3.8 Cobalt Edition was measured by analyzing acquired data from supported cloud-based application data. Table 1 defines the data objects and elements used for testing tools capable of extracting and reporting cloud-based application data.

Service	Artifact Group - Artificats
Social Media: Facebook Facebook Messenger Instagram	**Facebook** ***Account Profile:*** *Username, Email, Password, Token,* *User Info: Phone, DOB, Education, Family members, etc.* ***Contacts:*** *Name, Facebook ID, Interaction Status (Friend, Family)* *Work Place, Contact Info: Phone, DOB, Education,* *Family members, etc.* ***Messages:*** *Participants (To,From), Message content, Last Modified Date* *Attachment Filename, Attachment File Content, File Size, Hash* ***Calls:*** *Participants (To,From), Creation Date, Duration* ***Posts:*** *Author Name, Participants Names, Type: Comment, Posts* *Post Content, Create Date, Attachment Filename,* *Attachment File Content* ***Comments:*** *Creation Date, Participant Name (From), Comment Text Content* ***Files:*** *Filename, File Content, File Type: Audio, Graphic,Video* *Create Date, Hash* **Facebook Messenger** ***Messages:*** *Participants (To,From), Message content, Last Modified Date* *Attachment Filename, Attachment File Content, File Size, Hash* ***Calls:*** *Participants (To,From), Creation Date, Duration*

Service	Artifact Group - Artificats
	Instagram ***Account Profile:*** *Username, Profile Picture, Password, Token* ***Contacts:*** *Name, Profile Picture, Bio, Interaction Status (Friend, Family), Phone Number, Email, Date of Last Contact, # of times contacted* ***Chats/Messages:*** *Participants (To,From), Createion Date, Last Activity Date, Attachment Filename, Attachment File Content* ***Posts:*** *Author, Body of Post, Particpants, Creation Date, Last Modified Date, Reactions (Likes, Comments), # of Likes, Attachment Filename, Attachment File Content*
Messaging: Discord	**Discord** ***Account Profile:*** *Username, Email, Password, Token,* *User Info: About / Bio* ***Contacts:*** *Friends* ***Messages:*** *Participants (To,From), Message content, Last Modified Date* *Attachment Filename, Attachment File Content, File Size, Hash* ***Calls:*** *Participants (To,From), Creation Date, Duration*

Table 1: Cloud-based Appliation Data

3 Test Results

This section provides the test cases results reported by the tool. Section 3.1 identifies the cloud-based service and data artifacts within each service used for testing Paraben E3 Universal v3.8 Cobalt Edition.

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

As Expected: the CDX tool returned expected test results.

Partial: the CDX tool returned some of data.

Not As Expected: the CDX tool failed to return expected test results.

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

3.1 Cloud Data Extraction

Cloud-based application data were acquired and analyzed with Paraben E3 Universal v3.8 Cobalt Edition. All test cases – pertaining to the acquisition of supported cloud-based application data – were successful with the exception of the anomalies reported in Table 2 below as well as in Section 1: Results Summary.

> **NOTE: Some social media applications will compress files as they are uploaded, resulting in inconsistent file size, file names and hash values compared to the original uploaded data files, resulting in different file sizes and hashes. This is reported "as expected" behavior and highlighted with an asterisk.**

Cloud Data Extraction
Paraben E3 Universal v3.8 Cobalt Edition

Social Media Services and Messaging Services

Test Cases:	Facebook – Facebook Messenger	Instagram	Discord
Connectivity: Invalid Credentials	*As Expected*	*As Expected*	*As Expected*
Valid Credentials	*As Expected*	*As Expected*	*As Expected*
Account Profile: Username	*As Expected*	*As Expected*	*As Expected*
Email	*As Expected*	*As Expected*	*As Expected*
Password, Token	*As Expected*	*As Expected*	*As Expected*
User Information, Profile Pic	*As Expected*	*As Expected*	*As Expected*
Contacts (friends, followers): Name, ID	*As Expected*	*As Expected*	*As Expected*
Bio, Profile Pic	*As Expected*	*As Expected*	*As Expected*
Interaction Status (Friend, Family, Follower)	*As Expected*	*As Expected*	*As Expected*
Personal Information (Work place, family members)	*As Expected*	*As Expected*	*Not As Expected*
Contact Info (phone, email)	*As Expected*	*As Expected*	*As Expected*
Messages/Chats/DMs: Participants (To, From)	*As Expected*	*As Expected*	*As Expected*
Message Content	*As Expected*	*As Expected*	*As Expected*
Date (Creation, Modified)	*As Expected*	*As Expected*	*As Expected*
Attachment Filename	*As Expected*	**As Expected*	*As Expected*
Attachment Content	*As Expected*	*As Expected*	*As Expected*
File Size	**As Expected*	**As Expected*	*As Expected*
Hash	**As Expected*	**As Expected*	*As Expected*
Calls: Participants (To, From)	*NA*	*NA*	*As Expected*
Date	*NA*	*NA*	*As Expected*
Duration	*NA*	*NA*	*As Expected*
Posts/Comments: Participant Names	*As Expected*	*As Expected*	*As Expected*

Test Cases:	Facebook – Facebook Messenger	Instagram	Discord
Direction (incoming, outgoing)	*As Expected*	*As Expected*	*As Expected*
Posts/Comment Content, # of likes/shares	*NA*	*As Expected*	*As Expected*
Posts/Comment Creation Date	*As Expected*	*As Expected*	*As Expected*
Attachment Filename	**As Expected*	**As Expected*	*As Expected*
Attachment File Content	*As Expected*	*As Expected*	*As Expected*
Files: Filename	**As Expected*	**As Expected*	*As Expected*
File Content	*As Expected*	*As Expected*	*As Expected*
Create Date	*NA*	*NA*	*As Expected*
Hash	**As Expected*	**As Expected*	*As Expected*

Table 2: Social Media and Messaging Services