December 2023

Test Results for Cloud Data Extraction Tool:
Oxygen Forensic Detective v16.1.0.172 – Cloud Extractor v10.1.0.114

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the U.S. 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's Cyber Crime Center, the U.S. Internal Revenue Service's Criminal Investigation Division Electronic Crimes Program, and the DHS' 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, proving 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 Oxygen Forensic Detective v16.1.0.172 – Cloud Extractor v10.1.0.114 for extracting supported cloud-based application data.

Test results from other tools can be found on the DHS S&T-sponsored digital forensics webpage, 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: Oxygen

Software Version: Forensic Detective v16.1.0.172 – Cloud Extractor v10.1.0.114

Supplier: Oxygen

Address: 909 N. Washington St, Suite 300, Alexandria, VA 22314

Phone: +1(703) 888-2327

WWW: http://www.oxygenforensic.com/

1 Results Summary

Oxygen Forensic Detective v16.1.0.172 – Cloud Extractor v10.1.0.114 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 the 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.

Storage Services (Google Drive, One Drive):

- Authentication to "Google Drive" was successful. No data was extracted.
- Authentication to "One Drive" was not successful. No data was extracted.

Email Services (Gmail, Outlook):

- Authentication to "Gmail" was successful. The extraction ended with the following errors: "PM Thread: Error Retrieving Mail" and "PM Access violation at address in module iCloudExtractor.exe". No data was extracted.
- Authentication to "Outlook mail" was not successful. No data was extracted.

Productivity data (Google Contacts, iCloud Contacts):

- Individual "Contacts" profile pictures are not reported for "Google Contacts".
- The following data fields: phone, email, address, website for Google Contacts are each are correctly reported but are prefaced with a ":" that is not included in the uploaded data.
- The "Homepage/Website" for individual Contacts is not reported for "iCloud Contacts".

Social Media and Messaging data (Facebook):

- Direct messages (DMs) do not report txt, doc and pdf files.
- Facebook heart emoticons applied to a post are not reported.

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

Social Media and Messaging data (X):

- "Heart" emoticons applied to an X post were not reported.
- Note, as per above graphic and videos, files uploaded to X will be returned as jpg and mp4 files.

Social Media and Messaging data (WhatsApp):

- Biographical information from the owner and followers is not reported.
- Note, as per above graphic and videos, files uploaded to WhatsApp will be returned as jpg and mp4 files.

Social Media and Messaging data (Instagram):

- Bio information from the owner and followers is not reported.
- The number of "likes" and "shares" for posts are not reported.
- Note, as per above graphic and videos, files uploaded to Instagram will be returned as jpg and mp4 files.

Social Media and Messaging data (TikTok):

- Authentication to TikTok was not successful. No data was extracted.

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

Oxygen Forensic Detective v16.1.0.172 – Cloud Extractor v10.1.0.114 was installed on Windows 10 Pro version 10.0.19042.1586.

2.2 Cloud-based Application Data

Oxygen Forensic Detective v16.1.0.172 – Cloud Extractor v10.1.0.114 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
Storage Service: Google Drive iCloud One Drive	***Account Profile:*** *Profile picture, Username, Password, Token* ***Files:*** *Filename, File Content, File Size, Creation Date, Last Viewed Date, Hash*
Email Service: Gmail Outlook	***Account Profile:*** *Name, Username, Password, Token* ***Contacts:*** *Full Name, Email Address, Last Time Contacted Date, Number of Times Contacted, Last Viewed Date, File Content, File Type, File Size, Last Viewed Data* ***Email Data:*** *Direction (incoming, outgoing), Status (read, unread), Creation Date, Sender, Receiver email addresses, Subject, Email Body, Attachment Filename, Attachment File Content, File Size, Folder: Drafts, Inbox, Sent, Email Header, Hash*
Productivity Services: Google Calendar Google Contacts iCloud Contacts	**Google Calendar** ***Account Profile:*** *Username, Password, Token* ***Calendar Data:*** *Calendar Name, Event Description, Location of Event Start Date, End Date, Event Recurrance Date Range* **Google Contacts** ***Account Profile:*** *Email, Password, Token* ***Contact Data:*** *Profile Pic, Name, Company, Job Title, Email, Phone Number, Street Address, City, St, Zip, Birthday, Website, Notes*

Service	Artifact Group - Artificats
	<u>iCloud Contacts</u> ***Account Profile:*** *Email, Password, Token* ***Contact Data:*** *Profile Pic, Name, Company, Job Title, Email, Phone, Street Address, City, State/Country, Zip, Birthday, Website, Notes*
Social Media: Facebook Facebook Messenger X WhatsApp Instagram TikTok Diskcord	**<u>Facebook</u>** ***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* **<u>Facebook Messenger</u>** *Messages:* *Participants (To,From), Message content, Last Modified Date* *Attachment Filename, Attachment File Content, File Size, Hash* *Calls:* *Participants (To,From), Creation Date, Duration* **<u>X</u>** ***Account Profile:*** *Username, Email, Profile Picture, Password, Token* ***Contacts:*** *Name, Profile Picture, Bio, # of Followers, # of People Following* *Phone, Email, Date of Last Contact, # of Times Contacted* *Interaction Status (Follower)* ***Chats:*** *Participants (To,From), Direction (incoming, outgoing)* *Creation Date, Chat Text, Attachment Filename*

Service	Artifact Group - Artificats
	Attachment File Content ***Tweets/Posts:*** *Author, Direction (Incoming, Outgoing), Create Date,* *Text of Tweet/Post, # of re-Tweets, # of Likes,* *Type (Tweet, Comment, Post)* ***Files:*** *Filename, File Content, File Attachment, Creation Date* **<u>WhatsApp</u>** ***Account Profile:*** *Username, Password, Token* ***Contacts:*** *Name, Email, Phone Number* ***Messages:*** *Participants (To,From), Createion Date, Attachment Filename,* *File Content* ***Call Logs:*** *Participants (To, From), Creation Date, Duration,* *Status (Received, Missed), Location (Longtitude, Latitude)* **<u>Instagram</u>** ***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	**<u>Discord</u>** ***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 Oxygen Forensic Detective v16.1.0.172 – Cloud Extractor v10.1.0.114.

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 Compliance Data eXchange (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 Oxygen Forensic Detective v16.1.0.172 – Cloud Extractor v10.1.0.114. All test cases pertaining to the acquisition of supported cloud-based application data were successful with the exception of the anomalies reported in Section 1 Results Summary.

See Tables 2-6 below for more details.

> **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.**

Storage Services

Test Cases:	Google Drive	iCloud	One Drive
Connectivity: Invalid Credentials	*As Expected*	*As Expected*	*Not As Expected*
Valid Credentials	*As Expected*	*As Expected*	*Not As Expected*
Account Profile: Username	*As Expected*	*As Expected*	*NA*
Email	*As Expected*	*As Expected*	*NA*
Password, Token	*As Expected*	*As Expected*	*NA*
User Information, Profile Pic	*As Expected*	*As Expected*	*NA*
Files: Filename	*Not As Expected*	*As Expected*	*NA*
File Content	*Not As Expected*	*As Expected*	*NA*
File Size	*Not As Expected*	*As Expected*	*NA*
Creation Date	*Not As Expected*	*As Expected*	*NA*
Last Viewed Date	*Not As Expected*	*As Expected*	*NA*
Hash	*Not As Expected*	*As Expected*	*NA*

Table 2: Storage Services

Email Services

Test Cases:	Gmail	Outlook
Connectivity: Invalid Credentials	*As Expected*	*Not As Expected*
Valid Credentials	*As Expected*	*Not As Expected*
Account Profile: Username	*Not As Expected*	*NA*
Email	*Not As Expected*	*NA*
Password, Token	*Not As Expected*	*NA*
User Information, Profile Pic	*Not As Expected*	*NA*
Contacts: Name	*Not As Expected*	*NA*
Email Address	*Not As Expected*	*NA*
Date-Time Contacted/# of Times Contacted	*Not As Expected*	*NA*
Email Data: Direction (incoming, outgoing)	*Not As Expected*	*NA*
Status (read, unread)	*Not As Expected*	*NA*
Creation Date	*Not As Expected*	*NA*
Sender, Receiver Email Address	*Not As Expected*	*NA*
Subject	*Not As Expected*	*NA*
Email Body	*Not As Expected*	*NA*
Attachment Filename	*Not As Expected*	*NA*
Attachment File Content	*Not As Expected*	*NA*
Folder: Drafts, Inbox, Sent	*Not As Expected*	*NA*
Email Header	*Not As Expected*	*NA*
Hash	*Not As Expected*	*NA*

Table 3: Email Services

Productivity Services (Calendar)

Test Cases:	Google Calendar
Connectivity: Invalid Credentials	*As Expected*
Valid Credentials	*As Expected*
Account Profile: Username	*As Expected*
Email	*As Expected*
Password, Token	*As Expected*
User Information, Profile Pic	*As Expected*
Calendar Data: Calendar Name	*As Expected*
Event Description	*As Expected*
Location of Event	*As Expected*
Start Date	*As Expected*
End Date	*As Expected*
Recurrence Date Range	*As Expected*

Table 4: Productivity Calendar Services

Prodcutivity (Contacts)

Test Cases:	Google Contacts	iCloud Contacts
Connectivity: Invalid Credentials	*As Expected*	*As Expected*
Valid Credentials	*As Expected*	*As Expected*
Account Profile: Username	*As Expected*	*As Expected*
Email	*As Expected*	*As Expected*
Password, Token	*As Expected*	*As Expected*
User Information, Profile Pic	*As Expected*	*As Expected*
Contacts: Name	*As Expected*	*As Expected*
Contact Photo	*Not As Expected*	*As Expected*
Phone Number	*As Expected*	*As Expected*
Email	*As Expected*	*As Expected*
Address, City, St, Zip	*As Expected*	*As Expected*
Contact Website	*As Expected*	*Not As Expected*
Job Title	*As Expected*	*NA*
Bio / Notes	*As Expected*	*As Expected*

Table 5: Productivity Contact Services

Note: QR code had to be used to authenticate to Discord.

Social Media Services

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

Test Cases:	Facebook	X	WhatsApp	TikTok	Instagram	Discord
Posts/Comment Content, # of likes/shares	*As Expected*	*As Expected*	*NA*	*NA*	*Partial*	*As Expected*
Posts/Comment Creation Date	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
Attachment Filename	**As Expected*	**As Expected*	*As Expected*	*NA*	**As Expected*	*As Expected*
Attachment File Content	*As Expected*	*As Expected*	*As Expected*	*NA*	*As Expected*	*As Expected*
Files: Filename	**As Expected*	**As Expected*	**As Expected*	*NA*	**As Expected*	*As Expected*
File Content	*As Expected*	*As Expected*	*As Expected*	*NA*	*Not As Expected*	*As Expected*
Create Date	*As Expected*	*As Expected*	*As Expected*	*NA*	*Not As Expected*	*As Expected*
Hash	**As Expected*	**As Expected*	*As Expected*	*NA*	**As Expected*	*As Expected*

Table 6: Social Media and Messaging Services