May 2023

Test Results for Cloud Data Extraction Tool:
Magnet Forensics Axiom v6.11.0.34807

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 Magnet Axiom v6.11.0.34807 for extracting supported cloud-based application data.

Test results from other tools can be found on DHS's computer forensics webpage at https://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: Axiom

Software Version: v6.11.0.34807

Supplier: Magnet Forensics

WWW: magnetforensics.com

1 Results Summary

Magnet Axiom v6.11.0.34807 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 inconsistent file names, file sizes and/or hashes compared to the original file uploaded by a user.

***Email service data*:**

.Heic and .bmp file attachments are not displayed for Gmail and Outlook.

Productivity data:

Prefix and suffix for contacts in Japanese and Arabic languages are not reported.

Social Media and Messaging data (Facebook):

- Direct Messages (DM) do not report heic, txt, doc and pdf files.
- Videos are reported twice as .jpg and .mp4 files.
- Facebook heart emoticon that was used to “heart” a post was extracted as picture.
- Preview of document files is not available.
- Note, as per above graphic and video files uploaded to Facebook will be returned as jpg and mp4 files.

Social Media and Messaging data (Twitter):

- All DMs provide a link that wasn't on the original DMs. The link redirects to the Twitter sign-in page.
- Participant Names are not included in DMs.
- Note, as per above graphic and videos files uploaded to Twitter will be returned as jpg and mp4 files.

Social Media and Messaging data (Instagram):

- Potential Facebook Picture Create and Last accessed dates incorrect as: 1/1/0001 12:00:00am.
- Note, as per above graphic and videos files uploaded to Instagram 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

Magnet Axiom v6.11.0.34807 was installed on Windows 10 Pro version 10.0.19042.1586.

2.2 Cloud-based Application Data

Magnet Axiom v6.11.0.34807 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 - Artifacts
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 Outlook Contacts	**Google Calendar** ***Account Profile:*** *Username, Password, Token* ***Calendar Data:*** *Calendar Name, Event Description, Location of Event* *Start Date, End Date, Event Recurrence Date Range* **Outlook Contacts** ***Account Profile:*** *Email, Password, Token* ***Contact Data:*** *Name, Contact Photo, Phone Number, Email, Address, City, St, Zip* *Contact Website, Groups, Creation Date*

Service	Artifact Group - Artifacts
Social Media: Facebook Twitter WhatsApp Instagram TikTok	**Facebook** ***Account Profile:*** *Username, Email, Password, Token,* *User Info: Phone, DOB, Education, Family members, etc.* ***Contacts:*** *Name, Facebook ID, Interaction Status (Friend, Family)* *Workplace, 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* **Twitter** ***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* *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* **WhatsApp** ***Account Profile:*** *Username, Password, Token* ***Contacts:*** *Name, Email, Phone Number*

Service	Artifact Group - Artifacts
	Messages: *Participants (To, From), Created on Date, Attachment Filename, File Content* ***Call Logs:*** *Participants (To, From), Creation Date, Duration, Status (Received, Missed), Location (Longitude, Latitude)* **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), Created on Date, Last Activity Date, Attachment Filename, Attachment File Content* ***Posts:*** *Author, Body of Post, Participants, Creation Date, Last Modified Date, Reactions (Likes, Comments), # of Likes, Attachment Filename, Attachment File Content*

Table 1: Cloud-based Application 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 Magnet Axiom v6.11.0.34807.

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 Axiom v6.11.0.34807. 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*	*As Expected*
Valid Credentials	*As Expected*	*As Expected*	*As Expected*
Account Profile: Username	*As Expected*	*NA*	*As Expected*
Email	*As Expected*	*NA*	*NA*
Password, Token	*As Expected*	*As Expected*	*As Expected*
User Information, Profile Pic	*NA*	*NA*	*NA*
Files: Filename	*As Expected*	*As Expected*	*As Expected*
File Content	*As Expected*	*As Expected*	*As Expected*
File Size	*As Expected*	*As Expected*	*As Expected*
Creation Date	*As Expected*	*As Expected*	*As Expected*
Last Viewed Date	*As Expected*	*As Expected*	*As Expected*
Hash	*As Expected*	*As Expected*	*As Expected*

Table 2: Storage Services

Email Services

Test Cases:	Gmail	Outlook
Connectivity: Invalid Credentials	*As Expected*	*As Expected*
Valid Credentials	*As Expected*	*As Expected*
Account Profile: Username	*NA*	*NA*
Email	*NA*	*NA*
Password, Token	*As Expected*	*As Expected*
User Information, Profile Pic	*NA*	*NA*
Contacts: Name	*As Expected*	*As Expected*
Email Address	*As Expected*	*As Expected*
Date-Time Contacted/# of Times Contacted	*As Expected*	*As Expected*
Email Data: Direction (incoming, outgoing)	*As Expected*	*As Expected*
Status (read, unread)	*As Expected*	*As Expected*
Creation Date	*As Expected*	*As Expected*
Sender, Receiver Email Address	*As Expected*	*As Expected*
Subject	*As Expected*	*As Expected*
Email Body	*As Expected*	*As Expected*
Attachment Filename	*As Expected*	*As Expected*
Attachment File Content	*Partial*	*Partial*
Folder: Drafts, Inbox, Sent	*As Expected*	*As Expected*
Email Header	*As Expected*	*As Expected*
Hash	*As Expected*	*As Expected*

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

Productivity (Contacts)

Test Cases:	Outlook Contacts
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*
Contacts: Name	*Partial*
Contact Photo	*NA*
Phone Number	*As Expected*
Email	*As Expected*
Address, City, St, Zip	*As Expected*
Contact Website	*NA*
Groups	*As Expected*
Creation Date	*As Expected*

Table 5: Productivity Contact Services

Social Media Services

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

Test Cases:	Facebook	Twitter	WhatsApp	Instagram
Posts/Comment Creation Date	*As Expected*	*As Expected*	*NA*	*As Expected*
Attachment Filename	**As Expected*	*NA*	*NA*	**As Expected*
Attachment File Content	*As Expected*	*NA*	*NA*	*As Expected*
Files: Filename	**As Expected*	**As Expected*	**As Expected*	**As Expected*
File Content	*As Expected*	*As Expected*	*As Expected*	*NA*
Create Date	*NA*	*As Expected*	*As Expected*	*Not As Expected*
Hash	**As Expected*	**As Expected*	*As Expected*	**As Expected*

Table 6: Social Media Services