January 2025

Cloud & Remotely Stored Data Extraction (CDX) Using Account Credentials: Specification, Test Assertions, and Test Cases

Version 1.1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Abstract

This specification defines requirements, test assertions, and test cases for basic methods of extracting digital artifacts using account credentials from storage in cloud-based services. This document defines cloud data extraction requirements. These requirements are used to derive test assertions, which are statements of conditions that are then checked after a test case is run. Each test assertion is covered by one or more test cases consisting of a test protocol and the expected test results. The test case protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results. Version 1.1 of the specification provides additional test assertions to address social media applications: Discord, Reddit, Telegram and Signal.

Comments and feedback are welcome. This document, and future revisions, are available for download at: https://www.cftt.nist.gov.

TABLE OF CONTENTS

1 Introduction

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. A capability is required to ensure that forensic tools consistently produce accurate, repeatable, and objective test results. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic tools by the development of functional specifications, test procedures, test criteria, and test sets. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools' capabilities. This approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing. This project is further described at https://www.cftt.nist.gov/.

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS) Science and Technology Directorate, and the National Institute of Standards and Technology.

2 Purpose

There are several methods to access and extract cloud artifacts, i.e., remotely stored in a cloud service, e.g., using data returned from a cloud-based service application and accessing the cloud account using credentials. This specification defines requirements, test assertions, and test cases for Cloud Data Extraction (CDX) Forensics Tools capable of performing the following three tasks only using account credentials:

1. Establishing connectivity to cloud-based services,
2. Acquiring tokens for authenticating to cloud-based services and
3. Extracting and reporting artifacts from cloud-based services.

The requirements are used to derive test assertions, which are statements of conditions that are then checked after a test case is run. Each test assertion is covered by one or more test cases consisting of a test protocol and the expected test results. The test case protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

3 Scope

The scope of this specification is limited to software tools capable of establishing connectivity and extracting digital artifacts from supported cloud-based services. This specification is general and capable of being adapted to other future cloud services.

4 Definitions

This glossary defines terms used within this document.

Cloud-based service – A service where application data are stored by a service provider on one or more remote servers rather than a users' local machine.

Token – Authentication data similar to a password that is stored on a user's device and allows access to a cloud service.

5 Cloud Data Model

This tool testing specification is based on the model of cloud data in Figure 5-1. This is a simplified generalization of the NIST definition of cloud services (Mell & Grance, 2011).

Cloud Data Model

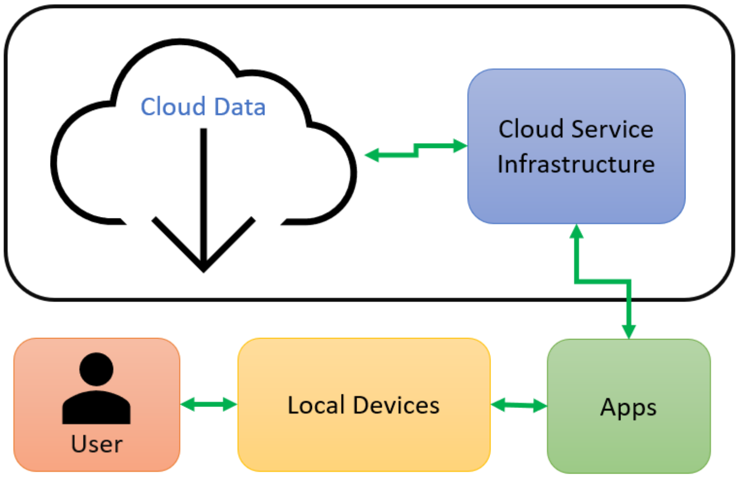

Figure 5–1 Model of Cloud Service Interactions

The user interacts with data stored on a remote server through software applications installed on local devices communicating with the cloud service. The model still applies to a forensic investigation in that the user is replaced by the forensic analysist; the local device is replaced by the analysist's device; and the cloud data extraction tool replaces the app.

The Cloud Data Extraction (CDX) tool being tested supports one or more cloud services. Each cloud service provides a repository to store a variety of data that can be extracted as artifacts. The data are stored by the cloud service as it interacts with the user through apps supported by the cloud service. Extracted artifacts collected can be limited based upon a user defined date range.

One difficulty with testing CDX tools is that there are more applications and associated artifacts than is practical to test a CDX tool for the capability to extract each artifact. The method for dealing with this complexity is to have a list of categories for the cloud services and artifacts and select representative applications for each category. Another troublesome issue is authenticating an account when two-factor authentication (2FA) is required. Authentication may fail due to 2FA although the correct user credentials have been applied.

Appendix A presents a list of the services with their supported applications and artifacts for initial tool testing.

6 Requirements

This section lists the CDX Tool requirements. There are two types of requirements. These are: requirements for core features and requirements for optional features. The core features must be met by all CDX tools. The requirements for optional features only apply if the CDX tool supports the feature.

6.1 Core Features

The following requirements shall be met by all tools:

CDX-CR-01. The tool shall provide the user with the ability to enter credentials allowing access to supported cloud-based services.
CDX-CR-02. The tool shall inform the user of incorrectly entered credentials.
CDX-CR-03. The tool shall provide the user with supported cloud services for data extraction.
CDX-CR-04. The tool shall report all extracted artifacts from a cloud-based service.
CDX-CR-05. The tool shall render all presented text correctly.

6.2 Optional Features

CDX-CO-01. The tool shall provide the ability to save/collect tokens used for authentication of supported cloud-based services.

7 Test Assertions

This section describes the assertions, used during testing, based on the type of requirement. The following section, 7.1, describes the assertions based on the core requirements described in the section above. The next section, 7.2, describes the assertions based on the optional requirement also described in the section above. Lastly, section 7.3, describes the criteria used in each of the assertions.

7.1 Core Assertions

The table below describes the assertions related to the core requirements described in section 6 above.

Assertion	Req
CDX-CA-01. The tool informs the user that valid credentials entered have been successfully accepted.	CR-01
CDX-CA-02. The tool informs the user that invalid credentials entered have not been accepted.	CR-02
CDX-CA-03. The tool provides the user with a list of supported cloud services it supports.	CR-03
CDX-CA-04. The tool presents acquired data accurately and completely.	CR-04
CDX-CA-05. The tool renders English text correctly.	CR-05
CDX-CA-06. The tool renders non-English text correctly.	CR-05

7.2 Optional Test Assertions

The table below describes the assertions related to the optional requirements described in section 6.

Test Assertions for Optional Features	Req
CDX-CO-01. The tool presents the user with the ability to select specific tokens for supported cloud-based services.	CO-01
CDX-CO-02. The tool provides the user with the ability to complete authentication to a supported cloud-based service using an acquired token.	CO-01

7.3 Conformance Indicators for Test Assertions

The following list describes the conformance criteria for each test assertion:

- CDX-CA-01. The tool informs the user that valid credentials entered have been successfully accepted. The tool allows the user to begin examining artifacts without an error message.

- CDX-CA-02. The tool informs the user that invalid credentials entered have not been accepted. The tool gives the user an error message when invalid credentials are entered.

- CDX-CA-03. The tool provides the user with a list of supported cloud services. The tool produces a list of supported services. The user may have to request the list.

- CDX-CA-04. The tool presents acquired data accurately and completely. The tool reports all requested artifacts.

- CDX-CA-05. The tool renders English text correctly. If the reported artifact or metadata is in English text, the text is rendered correctly.

- CDX-CA-06. The tool renders non-English text correctly. If the artifact or metadata is in non-English text, the text is rendered correctly. The following language features should be covered: Latin-based text with accents, umlauts, and other markings; non-Latin-based text; Asian Kanji; Japanese Kana; and languages rendered right-to-left. The following are recommended for non-English text:

Text	Language	English Translation	Feature Covered
cañón	Spanish	Canyon	Accent and tilde
Schönheit	German	Beauty	Umlaut
Россия	Russian	Russia	Non-Latin
Сибирь	Russian	Siberia	Non-Latin
中国	Chinese	China	Asian Kanji
東京	Chinese or Japanese	Tokyo	Asian Kanji
スバル	Japanese Katakana	Subaru (car brand)	Katakana
みつびし	Japanese Hiragana	Mitsubishi (Car brand)	Hiragana
فلافل	Arabic	Falafel	Right-to-Left
كسكس	Arabic	Couscous	Right-to-Left

- CDX-CO-01. The tool presents the user with the ability to select specific tokens for supported cloud-based services. The tool provides an access token on request.
- CDX-CO-02. The tool provides the user with the ability to complete authentication to a supported cloud-based service using an acquired token. The access token allows the user to begin examining artifacts without an error message.

8 Cloud Data Extraction Test Cases

For each cloud service category there is a test case and test data set that cover a particular cloud service. Test data is created dynamically on-the-fly following the methods described in the CFTT *Cloud Test Data Creation* document (preparation in progress). Service categories and applications included in test cases are:

- Storage: Google Drive, iCloud, and One Drive
- Email: Gmail, and Outlook
- Location: Google Maps
- Productivity: Google Calendar, Google Contacts, iCloud Contacts
- Social Media and Messaging: Facebook, Twitter, WhatsApp, Instagram, TikTok, Discord, Reddit, Telegram, Signal

8.1 CDX-01-ST Storage Services

For each storage service supported by the tool do the following:

1. Attempt to connect with invalid credentials; CA-02
2. Attempt to connect with valid credentials; CA-01, CA-03
3. Extract selected artifacts; CA-04, CA-05, CA-06

Optional Steps:

4. Attempt to acquire authenticating token and establish connection to cloud service; AO-01, AO-02
5. Extract selected artifacts; CA-04, CA-05, CA-06

Potential Test Cases:

- CDX-01-ST-GD; Google Drive
- CDX-01-ST-IC; iCloud
- CDX-01-ST-OD; One Drive

8.2 CDX-02-EM Email Services

For each storage service supported by the tool do the following:

1. Attempt to connect with invalid credentials; CA-02
2. Attempt to connect with valid credentials; CA-01, CA-03
3. Extract selected artifacts; CA-04, CA-05, CA-06

Optional Steps:

4. Attempt to acquire authenticating token and establish connection to cloud service; AO-01, AO-02
5. Extract selected artifacts; CA-04, CA-05, CA-06

Potential Test Cases:

- CDX-02-EM-GM; Gmail
- CDX-02-ST-OL; Outlook

8.3 CDX-03-LO Location Services

For each storage service supported by the tool do the following:

1. Attempt to connect with invalid credentials; CA-02
2. Attempt to connect with valid credentials; CA-01, CA-03
3. Extract selected artifacts; CA-04, CA-05, CA-06

Optional Steps:

4. Attempt to acquire authenticating token and establish connection to cloud service; AO-01, AO-02
5. Extract selected artifacts; CA-04, CA-05, CA-06

Potential Test Cases:

- CDX-03-LO-GL; Google Maps

8.4 CDX-04-PR Productivity Services

For each storage service supported by the tool do the following:

1. Attempt to connect with invalid credentials; CA-02
2. Attempt to connect with valid credentials; CA-01, CA-03
3. Extract selected artifacts; CA-04, CA-05, CA-06

Optional Steps:

4. Attempt to acquire authenticating token and establish connection to cloud service; AO-01, AO-02
5. Extract selected artifacts; CA-04, CA-05, CA-06

Potential Test Cases:

- CDX-04-PR-GCA; Google Calendar
- CDX-04-PR-GCO; Google Contacts
- CDX-04-PR-ICC; iCloud Contacts

8.5 CDX-05-SM Social-Media and Messaging Services

For each storage service supported by the tool do the following:

1. Attempt to connect with invalid credentials; CA-02
2. Attempt to connect with valid credentials; CA-01, CA-03
3. Extract selected artifacts; CA-04, CA-05, CA-06

Optional Steps:

4. Attempt to acquire authenticating token and establish connection to cloud service; AO-01, AO-02
5. Extract selected artifacts; CA-04, CA-05, CA-06

Potential Test Cases:

- CDX-05-SM-FB Facebook
- CDX-05-SM-TW Twitter
- CDX-05-SM-WA WhatsApp

- CDX-05-SM-IG Instagram
- CDX-05-SM-TT TikTok
- CDX-05-SM-DC Discord
- CDX-05-SM-RD Reddit
- CDX-05-SM-TG Telegram
- CDX-05-SM-SG Signal

9 References

Mell, P., & Grance, T. (2011, September). *The NIST Definition of Cloud Computing -- SP 800-145.* Retrieved July 2022, from https://doi.org/10.6028/NIST.SP.800-145

10 Appendix A

This appendix lists the artifacts (e.g., files, email, routes, social media posts, etc.) that the tool being tested attempts to extract for each cloud service that is supported and used in testing. Each cloud service has a unique set of supported applications that create extractable artifacts. Some cloud services may have unique artifacts that are unrelated to specific applications. The following service categories and applications are to be tested:

- Storage: Google Drive, iCloud, and One Drive
- Email: Gmail, and Outlook
- Location: Google Maps
- Productivity: Google Calendar, Google Contacts, iCloud Contacts
- Social Media and Messaging: Facebook, Twitter, WhatsApp, Instagram, TikTok, Discord, Reddit, Telegram, Signal

10.1 Services and Artifacts tested

The CDX tool selected for testing may provide support for fewer services and applications than the ones described in the following sections. The *Service* column in the tables below (sections 10.1.1 – 10.1.5) is the type of cloud service, the *Artifact Group Column* is a collection of related artifacts, and the *Artifact Column* is the artifact that the CDX tool needs to demonstrate that it can correctly extract. There should be a table created for each of the supported categories listing the artifacts by service. The following sections, 10.1.1 – 10.1.5 show what the tables may look like.

10.1.1 Storage Services

Service (Storage)	Artifact Group	Artifact
Google Drive	Account Profile	
		Profile picture
		Username
		Password
		Token

Service (Storage)	Artifact Group	Artifact
	Files	
		Filename
		File content
		Size
		Creation Date
		Last viewed Date
		Hash
iCloud	Account Profile	
		Username
		Password
		Token
	Files	
		Filename
		File content
		File Type
		File Size
		Time of Last Update
One Drive	Account Profile	
		Username
		Password
		Token
	Files	
		Filename
		File content
		Size
		Creation Date
		Last Viewed Date
		Hash

10.1.2 Email Services

Service (Email)	Artifact Group	Artifact
Gmail	Account Profile	
		Name
		Username
		Password
		Token
	Contacts	
		Full Name
		Email Address
		Last Time Contacted Date
		# of Times Contacted Date
		Last viewed Date

Service (Email)	Artifact Group	Artifact
	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
Outlook	Account Profile	
		Email Address
		Password
		Token
	Contacts	
		Name
	Email Data	
		Sender, Receiver email addresses
		Subject
		Creation Date
		Submitted Date
		Delivered Date
		Email Body
		Text
		Attachment Filename
		Attachment File content
		Email header

336

337 10.1.3 Location Services

Service (Location)	Artifact Group	Artifact
Google Maps	Account Profile	
		Name
		Username
		Password
		Token
		Profile Picture
	Location Data	

Service (Location)	Artifact Group	Artifact
		Kml Filename
		Kml File content
		Creation Date
		Longitude, Latitude coordinates

10.1.4 Productivity Services

Service (Productivity)	Artifact Group	Artifact
Google Calendar	Account Profile	
		Username
		Password
		Token
	Calendar Data	
		Calendar Name
		Event Description
		Location of Event
		Start Date
		End Date
		Event Recurrence Date Range
Google Contacts	Account Profile	
		Email
		Password
		Token
	Contact Data	
		Name
		Contact Photo
		Phone Number
		Email
		Address, City, St, Zip
		Contact website
		Groups
		Creation Date
iCloud Contacts	Account Profile	
		Email
		Password
		Token
	Contact Data	
		Name
		Contact Photo
		Phone Number
		Email
		Address, City, St, Zip
		Contact info: notes, company
		Facebook username

342 10.1.5 Social Media Service

Service (Social Media)	Artifact Group	Artifact
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
		Creation Date
		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	

Service (Social Media)	Artifact Group	Artifact
		Filename
		File content
		File types: 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	

Service (Social Media)	**Artifact Group**	**Artifact**
		Username
		Password
		Token
	Contacts	
		Name
		Email
		Phone Number
	Messages	
		Participants (To, From)
		Creation 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)
		Creation Date
		Last Activity Date
		Attachment Filename
		Attachment File content
	Posts	
		Author
		Body of Post
		Participants
		Creation Date

Service (Social Media)	**Artifact Group**	**Artifact**
		Last Modified Date
		Reactions (Likes, Comments)
		# of Likes
		Attachment Filename
		Attachment File content
TikTok	Account Information	
		Username
		Profile Picture
		Bio
		# of Followers
		# of Following
	Inbox	
		Likes
		Comments
		Mentions
		Followers
	Messages	
		Participants (To, From)
		Creation Date
		Last Activity Date
		Attachment Filename
		Attachment File content
	Files	
		Filename
		File Content
		File Attachment
		Creation Date
	Posts	
		Author
		Body of Post
		Participants
		Creation Date
		Last Modified Date
		Reactions (Likes, Comments)
		# of Likes
		Attachment Filename
		Attachment File content
Discord	Account Information	
		Username
		Profile Picture
		Bio
	Messages	
		Participants (To, From)
		Creation Date

Service (Social Media)	Artifact Group	Artifact
		Attachment Filename
		Attachment File content
	Files	
		Filename
		File Content
		File Attachment
	Call Logs	
		Participants (To, From)
		Creation Date
		Duration
		Status (Received, Missed)
Reddit	Account Information	
		Username
		Profile Picture
		Bio
	Messages	
		Participants (To, From)
		Creation Date
		Message Content
	Posts	
		Author
		Body of Post
		Participants
		Creation Date
		Last Modified Date
		Reactions (Likes, Comments)
		# of Likes
		Attachment Filename
		Attachment File content