Scientific Working Group on Digital Evidence

Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers

23-F-004-1.1

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)

c) Address
d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers

Table of Contents

1. Purpose

The purpose of this document is to provide guidance for acquiring, preserving, and analyzing digital evidence from a cloud service provider.

2. Scope

For the purpose of this document, "cloud" refers to computing or storage capability provided by an entity other than the owner of the data and "cloud service provider" refers to the entity providing these computing or storage capabilities. The U.S. National Institute of Standards of Technology (NIST) provides an expansive definition and discussion of cloud computing generally in Special Publication 800-145, "The NIST Definition of Cloud Computing" [1], and Special Publication 800-146, "Cloud Computing Synopsis and Recommendations" [2].

3. Limitations

The examiner should have a basic understanding of the acquisition, preservation, and analysis of digital evidence. This document is not intended to be an exhaustive guide for individuals who do not have experience collecting, preserving, or analyzing digital evidence.

Due to the vast number of emerging platforms and cloud service providers, it is not possible to establish a precise set of procedures to cover all possible methods for acquisition, preservation, or analysis of evidence from every cloud service provider that may be encountered. Personnel should select the appropriate course of action based on available resources and their knowledge and understanding of the circumstances.

Guidance in this document is not meant to replace legal guidance from a responsible legal professional, nor is it meant to cover every conceivable situation.

4. Definitions

The following definitions apply to this document. For additional definitions, please refer to the SWGDE Glossary.

- **Lawful Custodian**: owner, person, or enterprise with legal authority over the data.
- **Cloud Service Provider (Provider)**: a provider of an electronic communication service or remote computing service that stores data on behalf of another.
- **Enterprises**: companies, academic institutions, non-profit organizations, government agencies, and similar entities that use service providers to store electronic communications and other data.
- **Collectors**: those responsible for collecting data.

5. Data in the Cloud

Devices utilizing cloud storage are ubiquitous. Cloud storage is often used to augment storage capacity, sync information between devices, or offer remote computing services. Some devices, such as a digital video recorder (DVR), may store settings and proprietary codecs locally, while

the data itself may be streamed to or from cloud storage rather than being stored locally on the device. These specific device configurations may be needed for viewing, export, or extraction of data from the cloud.

Computing devices may synchronize or backup user data and settings to cloud providers by default, requiring little user interaction. Some devices default to an automatic synchronization with cloud services. Other devices may not be synchronized with the cloud provider directly, but instead utilize a separate system or device as a proxy for cloud data storage. The examiner should be aware that data may exist in multiple places. Cloud storage may also encompass data that is not stored or synchronized to a device.

There may be differences in the state of encryption between a local device and the data synchronized with the cloud. Data on the local device may be encrypted or difficult to decode; however, requesting data from the cloud provider could provide the data in an unencrypted or readable form, or vice versa.

A user can encrypt data before it is uploaded to a cloud service provider, leverage encryption tools offered by the cloud service provider, or both. The examiner should consider obtaining any credentials (e.g., keys, certificates, passwords, tokens, MFA devices) that may be necessary to access or decrypt acquired data.

A cloud storage provider may be able to provide additional information associated with an account, such as subscriber information, historical devices, device activity, and user records. Historical data stored in the cloud may be more extensive than that found on a local device.

6. Legal Considerations

As with all digital evidence acquisitions, those responsible for collecting the digital evidence ("Collectors") must have the appropriate legal authority prior to conducting the acquisition. Working with legal counsel to understand the legal landscape before the need for or process arises is important. Advance development of procedures or legal process templates is a valuable practice that can save time, especially in exigent situations.

Cloud acquisitions fall into three broad categories regarding the legal authority needed to acquire the data:

- Person or entity is seeking their own data
- Consent
- Via legal authority such as a search warrant or subpoena.

The collector must ensure they fully understand the scope of their collection authority and ensure the processes they use prevent over-collection or exceeding their search authority.

7. Preservation

When there is a risk of destruction or loss of evidence, or if the risk of such loss or destruction is unknown, investigators should seek to preserve cloud data through the use of preservation requests to the provider pursuant to 18 U.S.C. § 2703(f), or appropriate litigation hold requests to the provider or enterprise records custodian.

8. Methods of Acquisition

Once legal authority has been established, the methods below outline various available acquisition methods. Specific steps to take prior, during, and after acquisition are outlined in detail in subsequent sections.

In some situations, a copy of the cloud data may be synced and stored to a local storage device. Collecting a local copy of the data, while outside the scope of this document, may be conducted in parallel with the acquisition of the cloud data. A comparison of the two collections may provide insight valuable to the examiner. When consent or legal process allows the search of a local device that utilizes cloud services, additional consent or legal authorization is required to search or collect data stored with a cloud service provider.

8.1 Compulsory legal process to the cloud service provider

Because of the complexity of cloud service provider environments, legal process is typically the preferred option where use of compulsory process is necessary.

When the lawful custodian utilizes a cloud storage provider, such as a business (enterprise) using Microsoft 365, and the enterprise is not the subject of the investigation, the collector should consider obtaining the evidence directly from the enterprise; so long as doing so will not compromise the investigation. As approaching the enterprise custodian directly may expose the investigation to potential risk, the collector should consider sending a preservation request to the cloud service provider prior to contacting the enterprise or lawful custodian in order to protect the evidence.

When either the lawful custodian or enterprise is the subject of the investigation, or when approaching the enterprise may compromise the investigation, seeking data from the provider is the preferred method. In this case, legal process is served to the provider who will then compile the requested data and provide it to the Collector. Because the data may exist in a proprietary format, the cloud service provider may be able to provide the data in a common file format or provide a tool to access the data.

Some cloud service providers notify the lawful custodian of the received legal process. Collectors should review the cloud service provider's user notification or privacy policy for their actions when they receive legal process. Additional legal processes are usually available to preclude notice by the provider. See 18 U.S.C. § 2705(b)[1] or equivalent state code.

[1] 18 U.S. Code § 2705(b) – PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS
https://www.law.cornell.edu/uscode/text/18/2705

8.2 Production by the lawful custodian

Some cloud service providers supply tools that allow the lawful custodian to export their own data from the cloud service provider's platform. Use of these tools is a best practice when available and the Collector has consent, or when the Collector has appropriate credentials and legal authority to export the data. It should be noted that some data returned by the cloud service provider's native data export tools may not be as complete as compared to if the data had been received directly from the cloud service provider through legal process.

Cloud service providers who do not provide a data export tool may publish documentation on how a user may export data from their platforms, such as an Application Programming Interface (API). Collectors should review such documentation and consider using these methods to obtain the data.

8.3 Use of a client application, API, or other interface

Some cloud service providers allow access to data stored with them and associated metadata via client application interfaces or APIs. It is possible that access to the data through these APIs may be gained from a device utilizing the cloud services. However, as noted before, when consent or legal process allows the search of a device utilizing cloud services, a separate consent or legal process will be required to search or collect data stored in the cloud. The following are some additional considerations:

- Providers may also allow access to stored data via application-specific protocols (e.g., stored email content may be available via an Internet Mail Access Protocol [IMAP] interface or stored files via a Common Internet File System [CIFS] interface). While these access methods may not allow for the collection of all data available, they are a viable option in the absence of more exhaustive options.
- Be aware that cloud-sharing links can be time sensitive or restricted (e.g., days available, password required, view only).
- Certain digital forensic tools allow for the collection of cloud data using harvested credentials from mobile device acquisitions. It is important to verify proper legal authority is obtained as the cloud data may require additional legal process.
- If multifactor authentication is enabled for an account, certain digital forensic tools used to export the data may not bypass the authentication mechanism, and access to a separate account or a physical device may be required for a successful export.
- In the case of Internet of Things (IoT) devices or mobile device applications, tokens may be utilized to authenticate as the endpoint with the cloud service provider in order to facilitate the export of data. The use of access tokens to gather user cloud data is a complex legal issue. Access tokens provide authenticated access to user data and courts may view the use of such tokens to export cloud contents as equivalent to acquiring the contents themselves. The law in this area is still developing, and the courts have not yet addressed all of the potential issues. Local rules may vary on the legality of this

technique, even with a search warrant. Collectors should consult with legal counsel prior to using this method outside of consent.

8.4 Physical search and seizure of the service provider's hardware providing the cloud computing services

In this option, investigators with the appropriate compulsory search authority can physically search the devices providing the cloud computing services on the provider's premises. Because of the technical complexity of many cloud computing provider environments and the risk of overly broad searches or causing unintended down-time or impairment to provider operations, this is typically an option of last resort, except in situations where a provider is untrustworthy or requires technical assistance from investigators to conduct the search. For some providers, the geographic dispersion of stored data may render this option unfeasible.

8.5 Other search authorities

Certain Collectors may have additional search authorities available depending on their specific jurisdiction and applicable statutes. Collectors should consult their legal counsel to evaluate whether other search authorities may be available.

- Emergency disclosure requests: Some jurisdictions, including the United States, have separate statutory provisions authorizing cloud service providers to disclose content to law enforcement or other authorities in emergency situations, absent other legal processes.
- International search authorities: For data stored by cloud service providers outside a Collector's country, special legal provisions may apply. Foreign data may be available via treaties, including mutual legal assistance treaties and multilateral instruments, like the Council of Europe Convention on Cybercrime ("Budapest Convention"), or letters rogatory. In some jurisdictions, including the United States (see the Clarifying Lawful Overseas Use of Data Act [CLOUD Act]), statutes extend the reach of domestic legal process to foreign-stored data of providers operating within that country. Some foreign law enforcement agencies may also be willing to directly facilitate immediate release from a provider in their jurisdiction in an emergency.

9. Steps to Take Prior to Acquisition

- Identify the particular data sought, relevant time periods, the involved cloud service providers, and the utilized services.
- Collectors should consider the possibility that a third party has manipulated the data sought, for example, through unauthorized access to a cloud service.
- Collectors should assess and document controls that were in place on the cloud service to detect or prevent this type of activity.

- Collectors should collect information regarding the creation, modification, and interaction with the data sought and the service containing that data to establish the provenance of the collected data.
- Collectors should consider whether independent sources of information may exist for a particular event and should consider collecting all of these to verify consistency between these sources or identify anomalies.
- Recheck legal authority and ensure legal scope is not exceeded
- Billing records and account information may identify the specific provider and services.
- Domain Name System (DNS) and WHOIS records may provide insight into the cloud service provider operating a particular property or service. For example, DNS Mail Exchange (MX) records specify the servers handling email for a particular domain. These records allow investigators to identify the email service provider for a particular domain.
- Most providers publish privacy policies on their website detailing the services they provide, the types of information they collect, and circumstances under which they collect that information.
- U.S. law enforcement agencies may contact the U.S. Department of Justice's "Computer Crimes and Intellectual Property Section (CCIPS)" for assistance [3].
- If applicable, request the provider preserve the data sought. Some jurisdictions, including the United States (see 18 U.S.C. § 2703(f)), have statutory authorities requiring service providers to preserve data at the request of law enforcement pending further legal process.
- Identify an appropriate acquisition option; see Section 7 Methods of Acquisition above.
- If using an acquisition option requiring the involvement of the service provider:
- Identify legal point of contact for the provider.
- The Search.org Internet Service Provider (ISP) List (https://www.search.org/resources/isp-list/) is a law enforcement community effort and contains information on many commonly encountered providers.
- Most privacy policies contain contact information for a privacy contact or Data Protection Officer.
- Consider the provider's policies regarding user notification of legal processes. If notification to the user would adversely impact the Collector's investigation, consider available mechanisms to preclude notice to the user (e.g., Notice of Non-Disclosure). Many jurisdictions, including the United States (see 18 U.S.C. § 2705(b)), have statutory authorities for precluding user notice by a provider.
- Obtain the proper legal authority or consent for the selected acquisition option.

10. Steps to Take During Acquisition

- Notes should be kept during the acquisition process to document pertinent information regarding system information, methods used, or how the data is received. Photographs and screen captures may supplement written notes to document data with evidentiary value.
- When a Collector is acquiring the data, note that some systems may utilize local storage in addition to cloud storage. With proper (potentially separate) legal authority, any local data should be acquired in addition to the steps outlined in this document. Refer to *SWGDE Best Practices for Computer Forensic Acquisitions* [4] for details on media acquisition.
- Determine the appropriate method of acquisition based on the data and available options, as discussed in Section 8 (e.g., native data export tools, use of a client application, or a physical search and seizure).
- Acquire the data using the selected method of acquisition.
- If a request is made to a provider, it likely will require legal process (e.g., discovery request, subpoena, search warrant, written consent) The request should include the language to obtain the data as originally stored by the Data Owner.
- Be aware the examiner may be given data in a proprietary format, and may need to view, process, decrypt, or convert the data through the services of that particular cloud service provider. Consider also requesting data from the cloud service provider in a readable, non-proprietary format.
- If issues arise obtaining the data via planned methods, attempt alternate methods presented in Section 8. If all methods fail, consider screen captures or photographs of the relevant data.

11. Steps to Take After Acquisition

- If receiving data from a provider pursuant to a legal demand, the collector must verify the respondent has produced all the data requested, and only the data requested. If the collector determines the respondent has produced data outside the scope of the legal demand, they must cease analysis and consult with appropriate legal counsel.
- Compute and record hash values for the acquired data. If a provider has digitally signed their production or provided hash values, verify the signature or hash values.
- Verify the acquisition has acquired (or the provider has produced) all of the expected data and the Collector can preview the data.
- Document the acquisition according to the collecting organization's procedures. Retain all notes, including screenshots, photographs, and logs generated during acquisition.

- If the data was provided on physical media (e.g., optical disc, hard drive) document the item as received.
- Follow organizational evidence procedures to preserve and store the acquired data, (i.e., transfer the acquired data to a suitable means of evidence storage).

12. Analysis

Acquired cloud data can contain everything from simple metadata to entire computing systems; it is beyond the scope of this document to address all appropriate analysis techniques or methods. Considerations include the following:

Due to the collection nature of data stored in cloud storage, metadata including date/time stamps may not be accurately reflective of the original evidence. For instance, the creation date timestamp may be reflective of the date/time the data was downloaded from the collection tool or moved to the storage media. It may not be the date/time when the item (such as a picture or document) was created. Modified timestamps may also be indicative of actions by the system such as data syncing to the cloud storage and not of end user activity. Timestamps in the cloud can be stored in times other than local or Coordinated Universal Time (UTC) such as the Cloud Service Provider's local time. Examiners should utilize their forensic knowledge to identify any discrepancies, and if needed, conduct further artifact analysis. Examiners should evaluate the possibility of malicious activity on the involved cloud service account and take appropriate steps if that is suspected. Examiner documentation should explain any discrepancies.

13. References

[1] Mell, Peter, and Tim Grance. "The NIST Definition of Cloud Computing." *NIST Special Publication 800-145. National Institute of Standards and Technology*, Sept. 2011, https://csrc.nist.gov/publications/detail/sp/800-145/final.

[2] Badger, Mike, et al. "Cloud Computing Synopsis and Recommendations." *NIST Special Publication 800-146. National Institute of Standards and Technology*, May 2012, https://csrc.nist.gov/publications/detail/sp/800-146/final.

[3] U.S. Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division. "Seeking Enterprise Customer Data Held by Cloud Service Providers." *U.S. Department of Justice,* Dec. 2017, https://www.justice.gov/criminal-ccips/file/1017511/download.

[4] Scientific Working Group on Digital Evidence. *Best Practices for Computer Forensic Acquisitions*. SWGDE 17-F-002-2.0, SWGDE, 2023, https://www.swgde.org/17-f-002/.

14. History

Revision	Issue Date	History
1.0 DRAFT	6/15/2023	Initial draft created by adding additional information to the previous document SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers, then adding substantive additional content thus changing the title of the document.
1.0 DRAFT	5/15/2024	Minor update to Section 12 based on Public Comment.
1.0 DRAFT	6/13/2024	SWGDE voted to approve as a Draft for Public Comment. Formatted for release as a Draft for Public Comment.
1.0	12/3/2024	SWGDE voted to approve as Final Approved Document. Formatted for release as a Final Approved Document.
1.1	1/13/2025	Based on public comment, in section 7.0, corrected typo from 18 U.S.C. § 2303(f) to U.S.C. § 2703(f).