Scientific Working Group on Digital Evidence

SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) 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 change

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall 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; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

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 the SWGDE cover page containing the disclaimer.
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 create date) of the document and mention if the document is in a draft status.

Intellectual Property:
Unauthorized use of the SWGDE logo or documents 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.

SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers

Table of Contents

1. Purpose

The purpose of this document is to provide guidance for acquiring 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*, and *Special Publication 800-146, Cloud Computing Synopsis and Recommendations* [1,2].

3. Limitations

The examiner should have a basic understanding of the collection of digital evidence. This document is not intended to be an exhaustive guide for individuals who do not have experience collecting 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 every situation. Personnel should select the appropriate course of action based on available resources and their knowledge and understanding of the circumstances. This document identifies the high-level considerations and steps for the collection of cloud based digital evidence.

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. 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 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.

In some instances, an entity may utilize the cloud in a way that is not tied to a specific device. For example, utilizing computing services by a hosting provider to run a server instance, or as a file hosting service accessible through a web client. In these cases, there may be no specific or necessary device utilized by the user in order to access these services.

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.

Users may choose to upload data in an encrypted state, encrypt data via the cloud service provider, or both. When feasible, acquire any credentials necessary to decrypt acquired data (e.g. keys, certificates, passwords) or obtain the data in an unencrypted format.

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

5. Legal Considerations

As with all digital evidence acquisitions, collectors must have the appropriate legal authority prior to conducting the acquisition. Working with legal counsel to understand your legal authorities before the need for legal process arises is important. Advance development of procedures or working copies of legal process is a valuable practice that can save time, especially in exigent situations.

Cloud acquisitions fall into three broad categories in regards to the legal authority used to acquire the data:

- The person or entity seeking the data owns or controls the data sought from the provider
- The person or entity seeking the data has the consent of the person or entity who owns or controls the data
- The person or entity seeking the data neither controls the data nor has the consent of the person or entity who owns or controls the data.

6. 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.

When an entity is not the subject of the investigation, data stored for the entity by cloud service providers should be obtained directly from the entity so long as it will not compromise the investigation [3]. Approaching an entity directly may expose the investigation to potential risk; investigators may seek a preservation request to the cloud service provider prior to contacting the entity in order to protect the investigation.

Collecting a copy of the cloud data that has been stored on or synced to a local device, while outside the scope of this document, may be conducted in parallel with an acquisition of the data from the cloud. A comparison of the two may provide insight valuable to the investigator. When consent or legal process allows the search of a device utilizing cloud services, additional consent or legal authorization is required to search or collect data stored in the cloud.

Available methods include:

6.1 Compulsory legal process to the service provider

Because of the complexity of cloud service provider environments, this is typically the preferred option where use of compulsory process is necessary, and either the entity is the subject of the investigation or going directly through the entity may compromise the investigation. Because the data may exist in a proprietary format, the provider may be able to provide the data in a common file format. Under these conditions, it is the preferred option due to the fact that the collector will be receiving the data directly from the provider. When utilizing this option, obtain compulsory legal process, such as a search warrant, from the appropriate legal authority and serve it on the service provider. The service provider will then compile the requested data and provide it back to the collector.

- As some service providers may notify the data owner of legal process, review the provider's user notification policy for legal process received. Additional legal process is usually available to preclude notice by the provider. See 18 U.S.C. § 2705(b)[1] or equivalent state code.

6.2 Native data export tools

Some providers supply tools that allow their customers to export their own data from the provider's services (e.g. Google Takeout, Office 365 Security and Compliance.) Use of these tools is a best practice when feasible, and the collector has consent, or appropriate credentials and legal authority to export the data.

- Providers who do not provide a data export tool may publish documentation on how a user may export data from their services, such as an Application Programming Interface (API); if available, collectors should review this documentation and consider using these methods to obtain the data. If the cloud service does not provide an export tool, the collector should document specific steps taken or tools utilized to acquire the data.

6.3 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 applications 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.

- 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]

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

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).

6.4 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.

6.5 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 process.
- 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][2]), 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.

[2] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Public Law 115-141, section 105 https://www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm

7. Steps to Take Prior to Acquisition

- Identify the particular data sought, relevant time periods, the involved cloud service providers, and the utilized services.
    - 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 Exchanger (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.
- If applicable, request the provider preserve the data sought. Some jurisdictions, including the United States (see 18 U.S.C. § 2703(f)[3]), 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 6 Methods of Acquisition** above.
    - If using an acquisition option requiring the involvement of the service provider:
        - Identify a legal point of contact for the provider.
            - The Search.org 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 process. If notification to the user would adversely impact the collector's investigation, consider available mechanisms to preclude notice to the user. Many jurisdictions, including the United States (see

[3] 18 U.S.C. § 2703(f) – REQUIREMENT TO PRESERVE EVIDENCE. https://www.law.cornell.edu/uscode/text/18/2703

18 U.S.C. § 2705(b)[4]), have statutory authorities for precluding user notice by a provider.

- Obtain the proper legal authority or consent for the selected acquisition option.

8. 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 also be used in lieu of, or in addition to, 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 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* for details on media acquisition [4].
- Determine if the relevant data can be acquired using the planned method of acquisition, as discussed in Section 6 (e.g., native data export tools, use of a client application, or a physical search and seizure).
- Obtain 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). If requesting data from a provider, the request should include the language to obtain the data as originally stored by the entity.
        - 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 6. If all methods fail, consider screen captures or photographs of the relevant data.

[4] 18 U.S. Code § 2705(b) – PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS. https://www.law.cornell.edu/uscode/text/18/2705

9. Steps to Take After Acquisition

- 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 store the acquired data, (i.e. transfer the acquired data to a suitable means of evidence storage).

10. References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *NIST Special Publication 800-145*, September 2011. [Online]. https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] M. Badger, T. Grance, R. Patt-Corner, and J. Voas, "Cloud Computing Synopsis and Recommendations," *NIST Special Publication 800-146*, May 2012. [Online]. 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," December 2017. [Online]. https://www.justice.gov/criminal-ccips/file/1017511/download

[4] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Computer Forensic Acquisitions,". [Online]. https://www.swgde.org/documents

SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers

History

Revision	Issue Date	Section	History
1.0 DRAFT	2019-06-06	All	Initial draft created and voted by SWGDE for release as a Draft for Public Comment.
1.0 DRAFT	2019-07-16	All	Formatting and technical edit performed for release as a Draft for Public Comment.