Scientific Working Group on Digital Evidence

SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage

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 & Multimedia Evidence Video Acquisition from Cloud Storage

Table of Contents

1. Purpose

The purpose of this document is to provide guidance for acquiring remotely stored video, audio, and associated data.

These guidelines may also be used to assist organizations when developing standard operating procedures (SOPs) for the acquisition of video, audio, and associated data from the cloud.

2. Scope

This document provides guidance and best practices for acquiring video and audio evidence that is not locally stored and ensuring data integrity.

3. Limitations

The responding individual should have a basic understanding of video and audio evidence. This document is not intended to be an exhaustive guide for field personnel who do not have experience acquiring video and audio evidence.

Due to the vast number of emerging platforms and cloud storage 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 [**1**]. This document identifies the major considerations and steps that will be part of the acquisition process.

This document addresses criminal investigative techniques used by government organizations; these techniques may not apply or be available to non-criminal investigations and/or non-government organizations. It is not meant to replace legal guidance from a responsible legal professional.

4. Types of Cloud Storage

These devices are increasingly common and do not have onboard storage capacity, but instead convey recorded data to a remote storage site. The following list suggests some, but not all, of the situations where it might be necessary to acquire data from remote storage:

- 4.1 Web-enabled devices in a home or business setting that stream encoded video directly to internet-hosted (cloud) storage (e.g., Nest® cameras, Arlo™ cameras, nanny cams, doorbell cams). Live-stream, playback, and export functions are usually controlled by a device in the physical location or through the user's phone/computer, but no data is stored on the device itself.
- 4.2 Security systems in place at multiple sites (e.g., banks, chain stores, convenience stores), with storage offsite at a centralized location. There may be no ability to view, play, or export stored data at the location where it was recorded.
- 4.3 Video that has been logically exported from a digital video recorder (DVR) and transferred to the cloud for sharing via file sharing sites (e.g., Dropbox™, Google Drive, etc.)

5. Legal Considerations

Proper legal authority should be obtained before acquiring remotely stored video evidence. Refer to organization policy regarding specific legal requirements for acquisition (i.e., search warrants, consent, exigent circumstances).

6. Steps to Take Prior to Acquisition

6.1 Determine the physical location of the recording device. If the video is on site, refer to *SWGDE Best Practices for Data Acquisition from Digital Video Recorders* [**2**].

6.2 Obtain legal authority.

6.3 If system functions and attributes are not already known, it is advisable to review specifications on product/service provider web sites, conduct additional research about the system online, and/or contact technical support for full information. Document representatives' names and any reference numbers (if applicable) when speaking directly to service providers or technical support personnel.

6.4 Determine the date/time/camera of interest and how much data needs to be acquired.

7. Steps to Take for Acquisition

7.1 Notes should be kept during the acquisition process to document pertinent information regarding system information and retention method (see sample worksheet in [**2**] *Appendix A*). Due to the nature of acquisition from cloud storage, not all field information may be available. Photographs may also be used in lieu of, or in addition to, written notes.

7.2 Some systems may utilize edge storage (or data stored either at the camera itself or at a local hub) in addition to cloud storage. Most often, edge recordings are stored on loose media such as SD or CompactFlash memory card. Any edge storage 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 loose media acquisition [**3**].

7.3 Determine if the relevant data can be acquired via the current state of access (e.g., service provider must be contacted for acquisition).

- Logging in to the user account to download is preferred over using a link emailed from the system owner/operator. When possible, download video directly from the interface or by a hyperlink provided by the system owner/service provider.
- If video can be viewed but not downloaded, either by login or via an emailed link, screen capture the relevant video.

7.4 Regardless of the capability to conduct immediate acquisition, data should be obtained directly from the service provider if possible, as it may provide better quality recordings or additional metadata.

7.5 Take the following actions to prevent deletion, and assist in acquisition, of data from the service provider.

- Request the information not be deleted. This is usually accomplished with a preservation request to the service provider. For a sample preservation request, see **Appendix A** [**4**].
  - Locate the proper contact for the service provider's custodian of records or registered agent. Many service providers furnish guidelines and provide information on request to assist law enforcement in obtaining cloud stored data.
  - Some service providers have an online portal for submission of preservation requests; in these cases, a separate preservation letter may not be necessary.
  - Service providers may notify account holders of received records requests. If the disclosure of any request could impact an ongoing investigation, consider issuing a non-disclosure order to the service provider.
  - Preservation requests may be honored by providers for a limited period of time. Efforts should be made for proper legal service within that timeframe.
- Request available data from the service provider. In most cases, it will be necessary to submit legal process (e.g., subpoena, search warrant) to obtain this data. (See [**4**], *Appendices*, for sample language for search warrants under 18 USC § 2703.) The legal process should include the following information:
  - date/time
  - location
  - account number
  - camera number
  - clip identifier
  - contact information for requestor
  - language requesting any and all data files, including proprietary data and universal file formats
  - specific language requesting any and all metadata files, including timestamps
  - language requesting any provider documentation of the acquisition process to include hash or checksum values, which can help to ensure integrity
  - any other information that may assist the service provider in retrieving the complete and correct data
- Legal process may be completed by other investigatory personnel with the resultant data transmitted to the technician.

8. Upon Receipt of Video

8.1 Verify that acquired data contains the relevant video and plays back correctly.

8.2 Consider capturing screenshot(s) of any download portal and/or saving emails to document the way data was received.

8.3 Download media immediately and transfer to a more permanent means of storage. Be aware that cloud-sharing links can be time sensitive/restricted (e.g., days available, password required, view only).

8.4 If data was transmitted via physical media (e.g., optical disc, hard drive) document and/or photograph the item as received.

8.5 Refer to *SWGDE Best Practices for Maintaining the Integrity of Imagery* for additional information on factors affecting the integrity and storage of digital media files [**5**].

9. References

[1] Virginia Department of Forensic Science, "Digital & Multimedia Evidence Section Procedures Manual," DFS Document 242-D100, Revision 8, 12 December 2016. [Online]. http://www.dfs.virginia.gov/wp-content/uploads/2017/01/242-D100-DME-Procedures-Manual.pdf

[2] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Data Acquisition from Digital Video Recorders". [Online]. https://www.swgde.org/documents/draftsForPublicComment

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

[4] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 3rd ed.: Office of Legal Education Executive Office for United States Attorneys, 2009. [Online]. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[5] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Maintaining the Integrity of Imagery,". [Online]. https://www.swgde.org/documents

Appendix A

Appendix A: Sample of Preservation Request

[Service Provider]
[Address]

Re: Request for Preservation of Records

Dear Service Provider:

Pursuant to Title 18, United States Code Section 2703(f), this letter is a formal request for the preservation of all stored communications, records, and other evidence in your possession regarding the following account pending further legal process: [account information] (hereinafter, "the Account").

I request that you not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the Account, or otherwise alert any user of the Account as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.

I request that you preserve, for a period of 90 days, the information described below currently in your possession in a form that includes the complete record. This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request. This request applies to the following items, whether in electronic or other form, including information stored on backup media, if available:

1. The contents of any communication or file stored by or for the Account and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.
2. All records and other information relating to the Account and any associated accounts including the following:
    a. subscriber names, user names, screen names, or other identities;
    b. mailing addresses, residential addresses, business addresses, email addresses, and other contact information;
    c. length of service (including start date) and types of service utilized;
    d. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
    e. all stored video, audio, and/or metadata;
    f. correspondence and other records of contact by any person or entity about the Account, such as "Help Desk" notes; and
    g. any other records or evidence relating to the Account.

If you have questions regarding this request, please call me at [phone number].

Sincerely,
[NAME]
[GOVERNMENT ENTITY]

Scientific Working Group on Digital Evidence

SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage

History

Revision	Issue Date	Section	History
1.0 DRAFT	2017-09-04	All	Initial draft created and voted by Video Committee to move forward for a SWGDE vote to release as a Draft for Public Comment.
1.0 DRAFT	10/06/2017	--	Voted by SWGDE for release as a Draft for Public Comment.
1.0 DRAFT	10/17/2017	--	Formatted and posted as a Draft for Public Comment.