Scientific Working Group on Digital Evidence

Best Practices for Chromebook Acquisition and Analysis

22-F-002-1.0

Disclaimer and Conditions 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 suggested best practices, practical guidance, technical positions, and educational information 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.

As a condition to the use of this document (and the information contained herein) in any judicial, administrative, legislative, or other adjudicatory proceeding in the United States or elsewhere, 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 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 sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, 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 and Conditions of 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 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

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.

Scientific Working Group on Digital Evidence

Best Practices for Chromebook Acquisition and Analysis

Table of Contents

1. Purpose

The purpose of this document is to describe best practices for the acquisition and analysis of Chromebooks. These processes are designed to maintain the integrity of digital evidence.

2. Scope

The intended audience for this document is personnel tasked with analyzing digital evidence involving Chromebooks. This document does not cover associated storage from cloud and warrant returns.

3. Limitations

This document is not intended to be a training manual or a specific operating procedure. This document is not all-inclusive and does not contain information relative to specific commercial products. If dealing with technology outside your area of expertise, consult with an appropriate specialist.

Devices and hardware change frequently, along with feature changes with the Chrome Operating System ("ChromeOS") updates. This document will discuss ChromeOS features and capabilities present at the time of the document's creation. A successful forensic image of a Chromebook will not follow conventional acquisition procedures used in other laptop-style forensic acquisition practices. Recovery images will be used in most cases to obtain a forensic image of the internal memory. Validated tools for the acquisition of Chromebooks are limited. Encrypted user data is stored in the internal memory; however, a large amount of data is stored in the cloud. Without an associated Google account and password for the device, most recoverable user data will be encrypted.

4. Definitions

- **LevelDB**
  Storage library created by Google for fast key-value storage that provides an ordered mapping from string keys to string values. See GitHub project: https://github.com/google/leveldb
- **Google Takeout**
  Utility for users to export the content of their Google Account. This includes not only Chromebook data but other sources including Android mobile phones, Chrome browser, and other Google products.
- **Google Workspace**
  An enterprise solution that includes multiple Google applications as well as security and management functions.

5. Acquisition

5.1 Methods

- **Developer Mode**
  Obtain a physical disk image of the device using functions or command-line driven methods while utilizing the Google Chromebook's developer mode.
- **DDM Logical Backup**
  Collection of a Chromebook using the Daniel Dickerman Method (DDM). This is a capture of a Chromebook's unencrypted data and is generally performed in sync with consent.
- **Cloud Environment**
  Acquisition of a user's Chromebook data may be obtained using a multitude of services offered by the Google environment, including Google Takeout, Google search warrant returns, or logs featured in Google enterprise and Google education services. Cloud acquisition sources are outside of the scope of this document.
- **Logical Collection of Files**
  Logical copy of files directly from the Chromebook to an external drive via command line or copy/paste. This is the least preferred method, but important when either the only source or a DDM Logical Backup is a partial acquisition.

5.2 Considerations

- Must know the associated Google account and password for all users for the logical backup.
- Switching a Chromebook to developer mode will wipe the device.
- Chromebook data utilization amount compared to the size of the target drive via the DDM may result in a partial acquisition
  - Example 1: A 64 GB Chromebook with 50 GB of space used will only have 14 GB available to write data to, resulting in only a partial image without any prompt
  - Example 2: If the targeted partition that is created to write the DDM logical backup is smaller than the amount of data to be written, it will result in a partial image without any prompt that the acquisition is partial.
- Storage available on a Chromebook will affect acquisition capabilities for DDM logical backups.
- Using the DDM, it is possible that certain devices do not have a Recovery Mode available.
- Not all Chromebook models have a recovery image available. The DDM methodology will not work for all devices.

- Not every type of external media will work in creating a recovery drive. At the time of this paper, there is no discernible drive that works consistently.
- Methodology may be applicable to Chromebooks and to Chromium OS which can run on virtual machines and on other hardware.

5.3 Acquisition Process

- There are two recommended acquisition methods.1) a physical acquisition of the device in Developer mode; and 2) DDM logical backup of Chromebook by profile.
- A device discovered to be in developer mode can be acquired via standard Linux commands without the need for a password.
- However, it is critical to note that placing a Chromebook into developer mode will wipe the user partition resulting in no user Chromebook data. Acquiring a DDM logical backup of a ChromeOS device requires the username and password for the device.
- It is recommended to follow the steps defined in the DDM. What follows are important notes and caveats when utilizing this method.
    - When entering usernames, do not use any "."s in the username. For example, if the username is swgde.documents@gmail.com type swgdedocuments@gmail.com instead. Note: this dot still exists while representing the domain (i.e., gmail.com).
    - Recovery Partitions can run out of space as enough free space is required to create the image. The user will be launched to the recovery screen, although the partial image should still be usable.
    - Verify the password in the username field as password typing is blind in recovery mode. Also, the keyboard may be set to a different language configuration.
    - If an incorrect password is entered, you will NOT receive feedback that a wrong password was entered. One can test the validity of the password by logging into the Chromebook with the username/password combination. Be sure to document this process. It is recommended to only test a single known password once.
    - Use of username and password may require access to multifactor authentication. Google refers to this process as 2-factor verification.
    - Chromebooks may be paired for unlocking with an Android device via a feature called "Smart Unlock". This works by pairing the Android device with the Chromebook and, once paired and authenticated, unlocking the connected Android device unlocks the Chromebook.
    - In managed environments, administrators may be able to provide usernames and passwords.

- Do not reset the username and password in an attempt to acquire the Chromebook with an unknown password. Chromebook acquisition requires the last known password for decryption of the container.
- Use custom recovery version 87 and below, as recoveries 88 and newer currently do not work in this usage.

- Other data pertaining to a Chromebook may be available from the following sources: Google warrant return, Google Takeout, and/or Google Workspace.

6. Analysis

Chromebook DDM logical backup images contain artifacts that are not available via cloud collection (warrant return, Google Workspace, or Google Takeout) at the time of this writing. This includes shell history, offline storage, and some Chromebook browser artifacts such as Chrome autofill, Chrome web visits, Chrome cache records, Chrome cookies, Chrome current session, Chrome downloads, Chrome keyword search terms, Chrome favorite icons, Chrome last tabs, Chrome last session, Chrome shortcuts, and Chrome logins.

Chromebook parsing is supported by several tools including open source utilities CLEAPP and Hindsight as well as commercial tools.

- CLEAPP by Alexis Brignoni and Mark McKinnon
- Hindsight by Ryan Benson

Chromebooks contain multiple Level DB database files. There are multiple viewers that can be used to analyze LevelDBdatabases including

- Leveldb-py by Mark Mckinnon
- CCL Chrome IndexedDB by Alex Caithness, CCL
- Parse Leveldb by Kathryn Hedley
- Leveldb Dashboard by Scalyr

Regardless of tool support, it is recommended to conduct manual analysis for a more thorough understanding. Chromebooks often utilize “extensions”. Chrome extensions are small applications that behave as traditional desktop applications but run entirely in the Chrome browser. It is important to review installed extensions and their associate permissions in order to determine if the extension data needs further analysis.

6.1 Key artifacts

- Avatar
- Browser Cache
- Browser History

- Browser History: Current Sessions
- Browser History: Current Tabs
- Browser History: Last Sessions
- Browser History: Last Tabs
- Downloads
- Extensions
- Extensions: manifest.json
- Extensions: Sync App Settings
- Offline Storage
- Shell History

Key artifact locations can vary depending on acquisition type and ChromeOS version. For key known locations see Chromebook Data Locations document.

7. Reference Sites and Publications

- Daniel Dickerman Acquisition Method
  https://dfir.pubpub.org/pub/inkjsqrh/release/2

- Google LevelDB
  https://github.com/google/leveldb

- CLEAPP by Alexis Brignoni and Mark McKinnon
  https://github.com/markmckinnon/cLeapp

- Hindsight by Ryan Benson
  https://github.com/obsidianforensics/hindsight

- CLEAPP it! - Chrome OS Logs Events and Protobuf Parser
  https://abrignoni.blogspot.com/2021/05/cleapp-it-chromeos-logs-events-and.html

- Mark Mckinnon
  https://github.com/markmckinnon/Leveldb-py

- CCL by Alex Caithness
  https://github.com/cclgroupltd/ccl_chrome_indexeddb

- parse_leveldb by Kathryn Hedley
  https://github.com/khyrenz/parse_leveldb

- Scalyr
  https://app.scalyr.com/leveldbdashboard

- Chromebook Data Locations
  https://www.magnetforensics.com/blog/chromebook-data-locations

History

Revision	Issue Date	History
1.0	6/9/2022	Initial draft created
1.0	7/15/2022	Voted to release as a Draft for Public Comment
1.0	9/22/2022	No comments received and no changes made. Voted to release as final publication.