Scientific Working Group on Digital Evidence

Best Practices for Chip-Off Processes

SWGDE 15-F-002-2.0

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.

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:

DRAFT

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.

DRAFT

Scientific Working Group on Digital Evidence

Best Practices for Chip-Off Processes

Table of Contents

1. Purpose 2
2. Scope 2
3. Limitations 2
4. Disclaimer 2
5. Training 3
6. Details of chip-off processes 3
   - 6.1 Preparation and Disassembly 3
   - 6.2 Chip Removal 3
   - 6.3 Reading data from the chip 4
7. Additional Resources 5
8. History 5

DRAFT

1. Purpose

This document describes best practices for acquiring data from a device by removing the flash memory chip from the printed circuit board (PCB) and reading the data directly from the chip. This document supplements and expands upon the material in 18-F-003-2.0 SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition. While the chip-off method of data extraction is commonly used on mobile devices, this technique can also be used to acquire data from other devices with flash memory attached to a PCB.

2. Scope

This document focuses on a physical data acquisition method using a possibly destructive process in a lab environment. The document targets individuals with intermediate to advanced digital forensic skills who may conduct chip-off extraction techniques.

3. Limitations

This document was prepared with the resources available at the time of publication. As with all information technology, digital forensics is a constantly evolving environment with frequent implementation of new features and innovations.

It does not cover reverse engineering or advanced data analysis techniques required to decode or analyze the data obtained from a chip-off extraction. This is not intended to serve as a training document.

This document is not intended for use as a step-by-step guide for conducting a thorough forensic investigation, nor should it be construed as legal advice.

4. Disclaimer

Not every device is a candidate for this process. Generally, traditional forensic methods of data acquisition should be attempted first, but this order may vary depending upon the make and model of the device, case facts, and available tools. The chip-off process should be considered destructive, as the flash memory chip may be irreversibly removed from the PCB. Examiners should confirm that the proposed examination is within the scope of their authority and consistent with applicable agency policies before proceeding.

Good candidates for this process may include, but are not limited to:

- damaged devices;
- password-locked devices with no bypass support;
- devices that are not encrypted;
- devices for which debugging mode is not enabled;
- examinations where non-invasive physical acquisitions are not supported or logical data extraction is not sufficient.

5. Training

The chip-off process requires special knowledge and training; see SWGDE Core Competencies for Embedded Device Forensics (in draft). An examiner should be trained and knowledgeable in the following topics:

- digital forensic procedures and evidence handling;
- basic electronics concepts, theory, and troubleshooting;
- disassembling devices;
- research and identification of flash memory and memory controller chips;
- differences in chip packages;
- familiarity with rework stations and processes;
- procedures for removing chips;
- reballing or preparing chips to be read;
- soldering and desoldering techniques;
- procedures for reading chips with a flash programmer/reader.

6. Details of chip-off processes

6.1 Preparation and Disassembly

6.1.1 Preparation

An examiner should identify flash memory and critical components suspected of containing relevant data. Before beginning the chip-off process, verify that all necessary tools and equipment are available, and ensure that both hardware and software solutions are compatible with the specific chip being removed. Examiners should wear appropriate personal protective equipment (PPE) when performing chip-off processes.

6.1.2 Disassembly

Before beginning disassembly, ensure that appropriate tools and equipment are available for the specific device and procedure. Heat, mechanical, or chemical methods, or a combination of techniques, may be necessary to remove heat or RF shields covering the flash memory chip.

6.2 Chip Removal

If the device has been exposed to liquid or excessive humidity, dry the PCB before removing the chip. Ensure the drying method is safe for the specific device and its components, minimizes the risk of further physical damage, and protects the integrity of the data. Following drying, chip removal should be performed as soon as practical to minimize the potential for corrosion.

Refer to *SWGDE 14-F-002-2.0 Best Practices for Handling Damaged Digital Storage Devices* for more information.

6.2.1 Removal by Heat

An examiner should use appropriate equipment (e.g., a hot-air rework station, soldering iron, or infrared rework station) based on the type of chip and its attachment method. Heating softens or melts the solder or adhesive, allowing the chip to be removed from the printed circuit board (PCB).

The examiner should use the lowest temperature necessary to effectively soften or melt the solder or adhesive and remove the chip while minimizing the potential for thermal damage. When available, the chip manufacturer's specifications should be consulted for applicable temperature limits and handling requirements.

6.2.2 Removal by Mechanical Means

Mechanical removal of the chip may be necessary instead of heat removal due to the possibility that phase-change flash memory chips may lose data when exposed to temperatures exceeding the manufacturer's guidelines. Examples of mechanical removal include:

- Cutting the PCB and grinding to remove layers of the PCB to expose the chip contacts.
- Using a computer numerical control (CNC) machine or milling equipment to remove layers of the PCB and expose the chip contacts.

Appropriate tools (e.g., tweezers, suction tools, or a scalpel) should be used to safely remove the chip from the PCB.

6.2.3 Removal by Chemical Means

In situations where thermal or mechanical removal is not appropriate, such as when a chip must remain in place on the PCB, chemical methods may be used to expose the chip or its contacts. Chemical methods may also be used for chip decapsulation when appropriate.

Examiners should use appropriate personal protective equipment (PPE), follow applicable safety procedures, and use only the type and amount of chemical necessary for the procedure.

Following the procedure, the chip should be appropriately cleaned and thoroughly dried before further processing.

6.3 Reading data from the chip

- Follow the manufacturer's instructions for connecting the chip to the appropriate reader or adapter and supplying power when required.
- Use appropriate hardware and software to acquire the data from the chip.
- Confirm that the amount of data acquired is consistent with the expected capacity and configuration of the chip. Any discrepancies should be documented and evaluated by the examiner.
- Calculate and document the hash value for the acquired output file.

7. Additional Resources

Scientific Working Group on Digital Evidence, *Best Practices for Mobile Device Evidence Collection & Preservation, Handling and Acquisition*. SWGDE 18-F-003-2.0. *SWGDE*, 2025, https://www.swgde.org/documents/published-complete-listing/18-f-003-2/.

Scientific Working Group on Digital Evidence, *Core Competencies for Embedded Device Forensics*. SWGDE 19-F-001-1.0. *SWGDE*, 2020, https://www.swgde.org/documents/published-complete-listing/19-f-001-swgde-core-competencies-for-embedded-device-forensics/.

Scientific Working Group on Digital Evidence, *Best Practices for Computer Forensic Acquisitions*. SWGDE 17-F-002-2.1. *SWGDE*, 2023, https://www.swgde.org/17-f-002

Scientific Working Group on Digital Evidence, *Best Practices for Handling Damaged Digital Storage Devices*. SWGDE 14-F-002-2.0. *SWGDE*, 2025, https://www.swgde.org/documents/published-complete-listing/14-f-002-best-practices-for-handling-damaged-digital-storage-devices/

8. History

Revision	Issue Date	History
1.0 DRAFT	9/17/2015	Initial draft created. Voted by SWGDE for release as a Draft for Public Comment.
1.0 DRAFT	9/29/2015	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	1/14/2016	Minor edits made throughout. Voted by SWGDE for release as an Approved Document.
1.0	2/8/2016	Formatting and technical edit performed for release as an Approved Document.
2.0 DRAFT	5/12/2026	All sections were updated based on a 5-year refresh
2.0 DRAFT	8/31/2026	Technical content was updated in sections 4-7 and editorial changes made throughout the document.
2.0 DRAFT	10/7/2026	SWGDE voted to approve as Draft for Public Comment. Formatted for release as a Draft for Public Comment