SWGDE Best Practices for Chip-Off

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.

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 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

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 Chip-Off

Table of Contents

1. Purpose

This document describes best practices for acquiring data contained within a device by removing the flash memory chip from the printed circuit board (PCB) and directly reading the data from the chip. This document supplements and expands upon the material in *SWGDE Best Practices for Mobile Phone Forensics* [1]. 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 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.

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

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

5. Training

The chip-off process requires special knowledge and training. Proper training should, at a minimum, cover the following topics:

- digital forensic procedures and evidence handling;
- basic electronics concepts, theory, and troubleshooting;
- repairing and disassembling devices;
- 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.

6. Details of the chip-off process

6.1 Preparation and Disassembly

6.1.1 Preparation

Research the device. Identify the flash memory chips suspected of containing relevant data. Determine the model number, memory part numbers, processor part numbers, and chip package types (e.g., BGA, TSOP).

6.1.2 Disassembly

Ensure the appropriate tools are available for safely removing the chip and reading the chip after removal (e.g., appropriate chip reader adapter for the particular chip type). Best practices dictate the use of a validated chip reader for extracting data from the chip.

Take care during disassembly to ensure the PCB and components are not damaged. Heat may be required to remove the heat or radio frequency (RF) shields covering the flash memory chips.

6.2 Chip Removal

If the device has been exposed to liquid or extreme humid environments, consider drying the PCB prior to removing the chip to remove the moisture.

Utilize appropriate hardware (e.g., hot air gun, soldering iron, or hot air or infrared rework stations) to remove the specific type of chip. The heated removal of a chip melts the solder or adhesive to allow the chip to be lifted from the PCB.

Use the lowest temperature required to effectively melt the solder for removal of the chip from the board. If known, refer to the chip manufacturer's specifications for the particular chip being removed to understand the maximum temperature.

Phase-change flash memory chips may lose data if they are exposed to temperatures exceeding the manufacturer's guidelines. A mechanical removal of the chip, instead of heated removal, may be necessary in these circumstances. Examples of mechanical removal include:

- Cutting the PCB and grinding to remove layers of the PCB to expose the chip contacts.
- Utilizing a computer numeric control (CNC) or milling lathe to remove layers of the PCB to expose the chip contacts.

Use appropriate tools (e.g., tweezers, suction, scalpel) to remove the de-soldered chip from the PCB.

Chips need to be cleaned and prepared to the specifications of the reader with which they will be read.

6.3 Reading data from the chip

- Obtain the programmer or reader needed to read the chip.
- Identify the correct adapter for the chip.
- Follow manufacturer's instructions for attaching the chip and powering on the programmer.
- Run the programmer application to read from the memory registers of the chip.
- Save the output file to a designated location and write-protect it.
- Verify the integrity of the output file. The output file size should roughly match the capacity of the chip that was read.
- Hash the output file.

The output file extracted during the chip-off process can now be imported as a binary file into other forensic software for analysis.

7. Conclusion

In detailing the chip-off process, this document presents a set of best practices for this method of data extraction, from preparation through acquisition.

8. References

[1] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Mobile Phone Forensics". [Online]. https://www.swgde.org/documents/Current%20Documents

SWGDE Best Practices for Chip-Off

History

Revision	Issue Date	Section	History
1.0	09/17/2015	All	Initial draft created. Voted by SWGDE for release as a Draft for Public Comment.
1.0	09/29/2015	All	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0	01/14/2016	All	Minor edits made throughout. Voted by SWGDE for release as an Approved Document.
1.0	02/08/2016	All	Formatting and technical edit performed for release as an Approved Document.