Scientific Working Group on Digital Evidence

SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices

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 the Acquisition of Data from Novel Digital Devices

Table of Contents

1. Scope

This document outlines a framework for performing forensic acquisitions of novel digital devices. These techniques are intended for new or previously unencountered technologies with no established procedures or best practices specific to the examination of those particular devices. They can be applied to devices such as media streaming dongles, "PC-on-a-stick" systems, embedded systems, "Internet of Things" (IoT) connected devices, similar non-traditional or unfamiliar digital devices, or technologies yet to be developed.

2. Physical Examination

- Inspect the physical hardware (including onboard components) for manufacturer, product name, model numbers, or other identifiers to search online for additional information.
- Review online resources to identify additional information about the device, including operating system, available drivers or software development kits (SDKs), storage capabilities, and network interfaces to identify possible ways to connect to the device for acquisition. Developer documentation, patent and regulatory filings, and intellectual property litigation frequently provide useful information. Consider contacting the manufacturer for additional information.
- Identify communication ports on the device such as JTAG, SPI, UART, and Serial
- Identify power requirements
- Identify the storage on the device:
    - Identify removable storage (e.g. SD card, micro hard drive)
    - Determine if the device has onboard NAND or flash storage
        - Identify the type of storage chip architecture
        - Determine how the storage is mounted to the board and the best method for removal or in-situ extraction

3. Acquisition

Acquisition of novel devices may require a departure from traditionally accepted forensic techniques. This should not preclude the acquisition or analysis of these devices, but examiners must assess the impacts of the techniques used against the objectives of the examination, and minimize changes to relevant portions of the subject device. Examiners should test and validate novel techniques on duplicate devices, and identify and document changes or other impacts that occur due to use of the technique. When conducting the acquisition, examiners should minimize changes to the device contents, and document the acquisition well enough that artifacts created by the acquisition process can be readily distinguished from artifacts from the operation of the device prior to the acquisition. Prior to performing potentially destructive acquisition or analysis processes, examiners should consider consulting with other knowledgeable examiners to validate the proposed process is reasonable and minimizes adverse impacts.

Acquisition techniques involving interaction with the device place a level of trust in the device that may be inappropriate in situations where devices -- and their constituent hardware components and software -- may be compromised, malicious, or are of unknown provenance. Examiners should be aware devices may attempt to deceive examiners or conceal relevant data. Consider whether the specific circumstances surrounding an examination warrant the use of alternate or additional acquisitions or examination techniques to detect or circumvent deceptive device behavior.

3.1 Acquiring data from local storage

3.1.1 Removable local storage

If the storage on the device can be easily removed, consider following conventional acquisition techniques. For example, physical storage could be removed and connected to a write-blocker for forensic acquisition. Examiners should consider whether the contents of storage may be more readily accessed via the device, such as storage encrypted using hardware cryptographic modules, or data stored in uncommon formats or using unique filesystems.

3.1.2 Native Interface

If a device provides a native method for accessing data -- e.g. a user interface, an application programming interface (API), or a device that presents an internal storage volume over USB or a network interface -- examiners should consider using these methods to acquire target data. For networked devices, examiners should consider whether the device exposes any interfaces via the network, and the viability of using those interfaces to acquire device data. These methods often provide relatively simple, minimally intrusive methods of accessing relevant data.

3.1.3 Forensic Boot Disk

If the device can be booted from external media, such as an SD card or USB flash drive, an alternate operating system could be utilized to complete a forensic acquisition. A powered USB hub may be necessary if additional powered USB devices need to be connected in order to operate the device and perform the acquisition. Some devices may implement UEFI and changes may need to be made in order to boot properly (i.e., enabling legacy BIOS option).

3.1.4 Disassembly of the Device to Expose Obscured Connection Points

If exposed ports offer limited connection capability (e.g. DisplayPort only), disassembly of the device may be required to determine if other connection options are available. Disassembly may expose interfaces such as a microSD card, a serial header connection for a USB, or JTAG TAPs where direct connection to the board may allow forensic acquisition of the storage volume.

3.1.5 Destructive Techniques

If all other methods of connecting have been exhausted, removal of the flash storage could be performed to complete a direct forensic acquisition of the data. This technique is considered destructive because it may not be possible to successfully reattach the module to the board. It is also possible the board or module could be damaged during the removal process.

3.2 Acquiring data from external sources

If the device has a networking capability, consider whether it may store data in "the cloud" or another network accessible location, or whether its network traffic contains relevant data. Observing network traffic from the device during setup and operation may provide relevant data from the device, insight into external locations where this data may be stored, and identifiers a provider may need to retrieve stored content. Examiners should test techniques involving network communication with external sources on duplicate devices first.

Privacy policies and terms of service from the manufacturer or provider may describe the types of data stored by the provider or other third parties. If relevant data is stored with a third party, follow your jurisdiction's procedures to preserve and lawfully obtain it.

If a device has a companion mobile application or website, analyzing these and their associated artifacts may provide additional avenues for obtaining relevant data or pointers to it.

4. Analysis

After successful forensic acquisition of data, examiners can use conventional digital forensic analysis techniques and tools to investigate the data.

5. References

- SWGDE Best Practices for Examining Mobile Phones Using JTAG
- SWGDE Best Practices for Chip-Off
- SWGDE Best Practices for Computer Forensics
- SWGDE Focused Collection and Examination of Digital Evidence

SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices

History

Revision	Issue Date	Section	History
1.0 DRAFT	2016-09-15	All	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2016-10-08	All	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0	2017-01-12	None	Following period of Public Comment, no feedback was received and no edits were made. SWGDE voted to publish as an Approved document (Version 1.0).
1.0	2017-02-21	Formatting	Formatted and published as Approved Version 1.0.