Scientific Working Group on Digital Evidence

Best Practices for Examining Digital Devices Using JTAG Processes

15-F-001-2.0

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 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 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

DRAFT

secretary@swgde.org. The following information is required as 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 overrepresent 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 Examining Digital Devices Using JTAG Processes

Table of Contents

1. Purpose 4
2. Scope 4
3. Limitations 4
4. Disclaimer 4
5. Training 5
6. Details of the JTAG Process 5
   - 6.1 Preparation 5
   - 6.2 Disassembly 6
   - 6.3 TAPs Identification 6
   - 6.4 Connectivity 6
   - 6.5 Configuration 6
   - 6.6 Extraction 6
   - 6.7 Preservation 6
   - 6.8 Hashing 6
7. Conclusion 6
8. References 7

DRAFT

1. Purpose

The purpose of this document is to describe best practices for acquiring data contained within a digital device using a Joint Test Action Group (JTAG) boundary scan technique as defined in IEEE 1149.1-2013, *IEEE Standard for Test Access Port and Boundary-Scan Architecture* [1]. This document supplements and further expands upon the material in *SWGDE 23-F-003-1.0 Best Practices for Internet of Things (IoT) Seizure and Analysis* [2], *SWGDE 18-F-003-2.0 Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition* [3], and *SWGDE 16-F-003-1.0 Best Practices for the Acquisition of Data from Novel Digital Devices* [4], which should be referenced before reading this document.

2. Scope

This document focuses on a physical acquisition method of digital devices, utilizing a non-destructive process in a lab environment. It does not cover reverse engineering and advanced data analysis techniques required to decode/analyze the data obtained from a JTAG 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. This document is targeted at intermediate to advanced examiners seeking familiarization with JTAG 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.

4. Disclaimer

SWGDE 18-F-003-2.0 Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition should be read prior to beginning and followed during the JTAG process [3]. Not every digital 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 case facts, available tools, and the make and model of the device.

Good candidates for this process 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; and
- examinations where non-invasive physical acquisitions are not supported and/or logical data extraction is not sufficient.

5. Training

Special knowledge and training are required before undertaking the JTAG process. Proper JTAG training should, at a minimum, cover the following topics:

- overview of boundary scanning and the JTAG process;
- repairing and disassembling digital devices;
- soldering and desoldering techniques;
- identification of Test Access Ports (TAPs) through probing;
- electrical theory (e.g., direct current), multimeter, and alternate power supply usage;
- digital forensic procedures and evidence handling.

6. Details of the JTAG Process

The JTAG process communicates through TAPs or USB to probe specific memory using a boundary scan method to push data from the digital device memory to the forensic computer.

The JTAG process can also be used with different digital devices (e.g., GPS units, routers, game systems). The operating systems vary greatly depending on different devices; however, the JTAG process is similar regardless of the device and operating system.

6.1 Preparation, Identification, and Documentation

Before beginning the JTAG process, the examiner should identify and document the device, PCB, and components relevant to the examination. Documentation should include photographs of the device and PCB before modification or connection to test access points.

The examiner must document all identified JTAG TAPs, their functions, identification methods, equipment and connections used, and any device or PCB modifications.

Research available technical information to determine JTAG support and the appropriate connectivity method.

Sources of technical information may include:

- manufacturer documentation
- component datasheets and technical reference manuals
- schematics and PCB layouts
- regulatory filings
- JTAG equipment and software documentation
- other reliable technical resources

Verify the technical information corresponds to the device and PCB revision being examined. Document the information used to identify the JTAG interface and connectivity method.

DRAFT

6.2 Disassembly

If disassembly of the device is necessary, appropriate precautions should be taken to minimize the risk of damage and, when practicable, allow the device to be returned to its original condition following completion of the JTAG data extraction.

6.3 TAPs Identification

When TAPs are utilized, identify the location and provide access to the required JTAG TAPs. The five (5) required TAPs (plus Ground) are:

- TDO (Test Data Out) shows the data shifted out of the device.
- TDI (Test Data In) shows the data shifted into the device's test or programming logic.
- TMS (Test Mode Select) samples at the rising edge of TCK to determine the next state.
- TCK (Test Clock) synchronizes the internal state machine operations.
- TRST (Test Reset) resets the TAP controller's state machine to a known state.

Other TAPs used for JTAG may include:

- GND (Ground) may be a pad or known ground source on the device.
- RTCK (Return Test Clock) listens for the return signal to achieve adaptive clocking.
- SRST (System Reset) power cycles the device.
- VREF (Voltage Reference) indicates signal levels.
- VCC (Voltage Collector) supplies power.

6.4 Connectivity

Connect the device to the JTAG extraction equipment using either:

- jig
- direct wire connection
- USB

6.5 Configuration

Configure the JTAG software settings as appropriate for the device, acquisition method, and examination requirements.

6.6 Extraction

Extract the data from the digital device.

6.7 Preservation

Enable file-level write protection on the extracted data file(s).

6.8 Hashing

Calculate a hash of the write-protected data file(s) and make a working copy for analysis.

DRAFT

7. Conclusion

This document provides best practices for the forensic acquisition of data using Joint Test Action Group (JTAG) techniques, from preparation through verification. It should be used in conjunction with *SWGDE 20-F-005-1.0 Best Practices for Mobile Device Forensic Analysis* and other applicable SWGDE guidance [5].

DRAFT

8. References

[1] Institute of Electrical and Electronics Engineers (IEEE), *IEEE Standard for Test Access Port and Boundary-Scan Architecture*, IEEE 1149.1-2013, https://standards.ieee.org/ieee/1149.1/4484/.

[2] Scientific Working Group on Digital Evidence. *Best Practices for Internet of Things (IoT) Seizure and Analysis*. SWGDE 23-F-003-1.0. *SWGDE*, 2024, https://www.swgde.org/documents/published-complete-listing/23-f-003-best-practices-for-internet-of-things-seizure-and-analysis/.

[3] 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/.

[4] Scientific Working Group on Digital Evidence. *Best Practices for the Acquisition of Data from Novel Digital Devices*. SWGDE 16-F-003-1.0. *SWGDE*, 2017, https://www.swgde.org/documents/published-complete-listing/16-f-003-swgde-best-practices-for-the-acquisition-of-data-from-novel-digital-devices/.

[5] Scientific Working Group on Digital Evidence. *Best Practices for Mobile Device Forensic Analysis*. SWGDE 20-F-005-1.0. *SWGDE*, 2020, https://www.swgde.org/documents/published-complete-listing/20-f-005-swgde-best-practices-for-mobile-device-forensic-analysis/.

DRAFT

History

Revision	Issue Date	History
1.0 DRAFT	06/04/2015	Original draft created and voted for release as a Draft for Public Comment.
1.0 DRAFT	06/20/2015	Formatting and technical edit completed for release as a Draft for Public Comment.
1.0 DRAFT	09/17/2015	SWGDE voted to release as an Approved Document.
1.0	09/29/2015	Formatting and technical edit performed for release as an Approved Document.
2.0 DRAFT	05/12/2026	Technical content and editorial changes.
2.0 DRAFT	09/01/2026	Technical content updated in sections 5-6.5, 6.7, 6.8, and editorial changes.
2.0 DRAFT	09/10/2026	SWGDE voted to release as a Draft for Public Comment.
2.0 DRAFT	10/08/2026	Document formatted for release for Public Comment.

DRAFT