Scientific Working Group on Digital Evidence

SWGDE Best Practices for Examining Mobile Phones Using JTAG

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 Examining Mobile Phones Using JTAG

Table of Contents

1. Purpose

The purpose of this document is to describe best practices for acquiring data contained within a mobile 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*. This document supplements and further expands upon the material in *SWGDE Best Practices for Mobile Phone Forensics,* which should be referenced prior to reading this document.

2. Scope

This document focuses on a physical acquisition method (Level 3)[1] of mobile 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. Finally, this document does not address the analysis of the data after a successful JTAG extraction is complete.

3. Limitations

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

4. Disclaimer

SWGDE Best Practices for Mobile Phone Forensics should be read prior to beginning, and followed during, the JTAG process. Not every mobile 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 for which debugging mode is not enabled;
- examinations where non-invasive physical acquisitions are not supported and/or logical extraction of data is not sufficient.

[1] *SWGDE Best Practices for Mobile Phone Forensics*, Section 5.3 *Data Acquisition*, describes the Mobile Forensics Pyramid and the different levels of extraction.

5. Training

Special knowledge and training are required prior 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 mobile devices;
- soldering and de-soldering techniques;
- identification of 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 Test Access Ports (TAPs) or USB to probe specific memory using a boundary scan method to push data from the mobile device memory to the forensic computer.

1. *Preparation:* Determine the model number, memory part numbers, and processor part numbers of the device; research JTAG support and connectivity method.

2. *Disassembly:* If disassembly of the mobile device is necessary, caution and care should be taken to ensure it can be returned to a working state when the JTAG data extraction is complete.

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

    Other TAPs used for JTAG may include:

    a. GND (Ground) may be a pad or known ground source on the device.
    b. RTCK (Return Test Clock) listens for the return signal to achieve adaptive clocking.
    c. SRST (System Reset) power cycles the device.

d. VREF (Voltage Reference) indicates signal levels.

e. VCC (Voltage collector) supplies power.

4. *Connectivity:* Connect the device to the JTAG extraction equipment using either:
   a. jig,
   b. direct wire connection, or
   c. USB.
5. *Configuration:* Configure the settings of the JTAG software.
6. *Extraction:* Extract the data from the mobile device.
7. *Preservation:* Enable file level write protection on the extracted data file(s).
8. *Hashing:* Calculate a hash of the write protected data file(s) and make a working copy for analysis.

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

7. Conclusion

In detailing the JTAG process, this document presents a set of best practices associated with this particular method of data extraction, from preparation through verification. Again, this document should be reviewed concurrently with *SWGDE Best Practices for Mobile Phone Forensics*.

8. References

[1] *IEEE Standard for Test Access Port and Boundary-Scan Architecture*, IEEE 1149.1-2013.

[2] 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 Examining Mobile Phones Using JTAG

History

Revision	Issue Date	Section	History
1.0	06/04/2015	All	Original draft created and voted for release as a Draft for Public Comment.
1.0	06/20/2015	All	Formatting and technical edit completed for release as a Draft for Public Comment.
1.0	09/17/2015	All	SWGDE voted to release as an Approved Document.
1.0	09/29/2015	All	Formatting and technical edit performed for release as an Approved Document.