JTAG Tool Testing

Jenise Reyes-Rodriguez
National Institue of Standards and Technology

Disclaimer

Certain company products may be mentioned or identified. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that these products are necessarily the best available for the purpose.

Outline

- JTAG Definition
- Why test JTAG tools?
- JTAG methods
- Preliminary Observations
- Plans for CFTT JTAG Tool Testing

What is JTAG?

- JTAG = Joint Test Action Group – method for testing circuits
- IEEE codified the JTAG efforts – IEEE Standard 1149.1
- Technique used to acquired data directly from a mobile device's Printed Circuit Board (PCB)

NIST

Why doing JTAG?

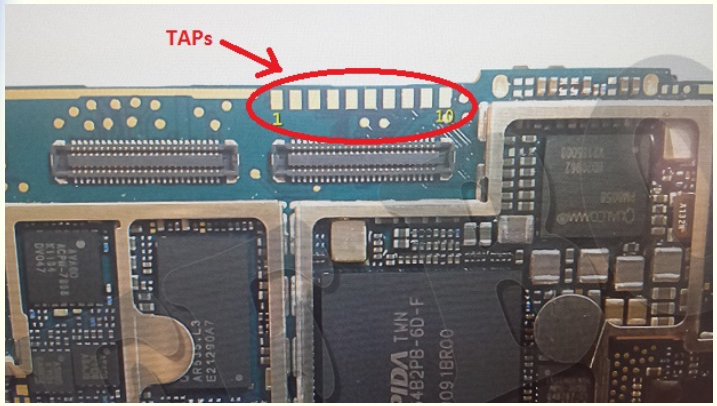
- Bypasses passwords/gesture swipes – python scripts
- Data dumps from Windows Phones
- Water damaged phones – mobile device repair

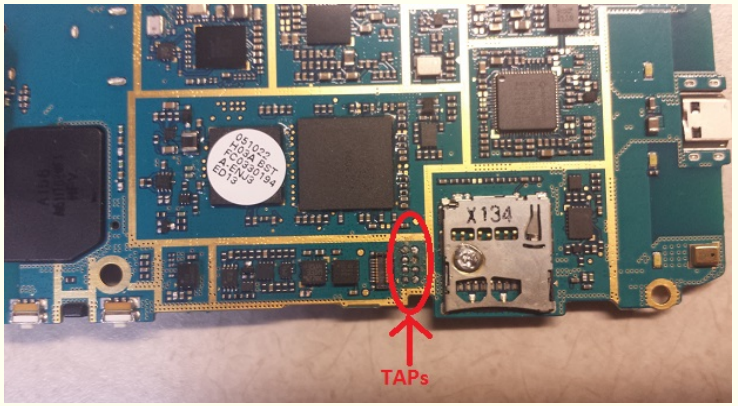
Importance of JTAG Tool Testing

- Goal of testing: Support the admissibility of JTAG acquired
- Goal for Preliminary Observations: share what we have learned so far

JTAG Requirements

- Memory, Power, TAPs & Processor
  - processor – makes a device JTAG-able
- TAPs = Test Access Ports
  - different: sizes, location, shapes & quantity





JTAG Cycle

TAPs ⟷ Processor ⟷ Memory

Are all mobile devices devices JTAG-able?

- **NO!**
  - mostly applies to Android + Windows
  - device may not have TAPs
  - device not supported by JTAG tool *
  - processor may be supported but:
    - TAPs configuration has not been discovered (iOS devices)
    - TAPs may be disabled
    - TAPs shut down by OS
    - fuse in processor may be bad

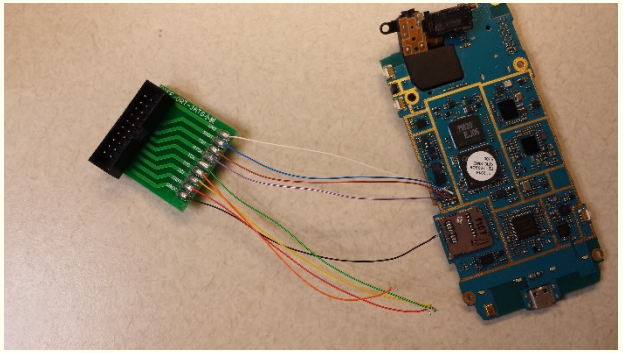
NIST

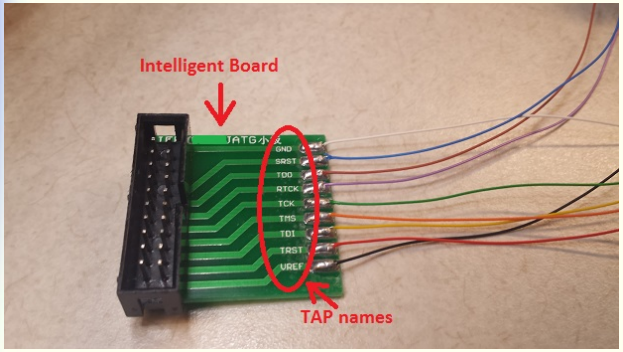
Device not supported? – still a chance

- Look for device's processor
- Is there another device using the same processor?
- Use that device's profile – known as sister phone's profile
- Probe each TAP to identify them
- Hopefully connection between phone and JTAG box is established

Methods to JTAG a mobile device

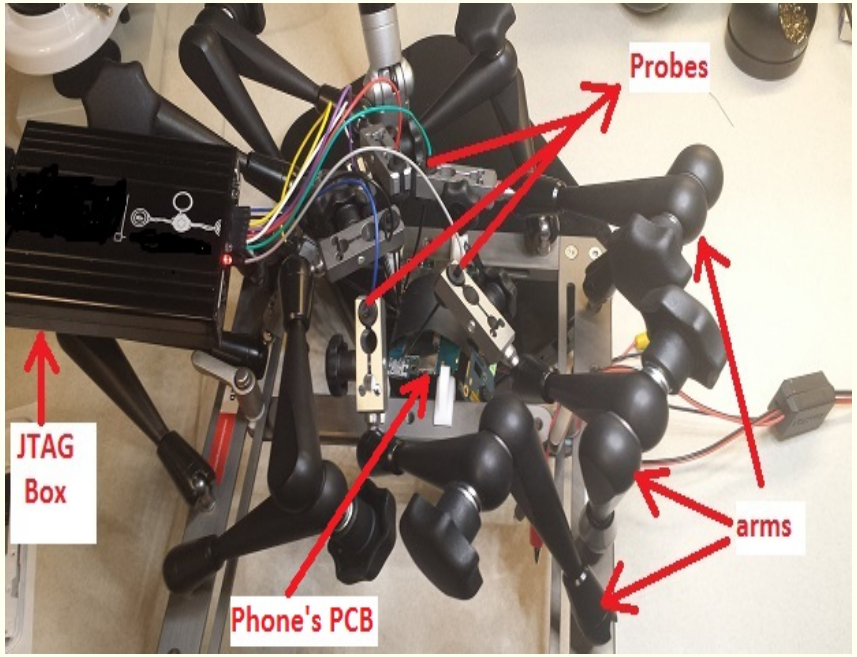
Soldering Method 1

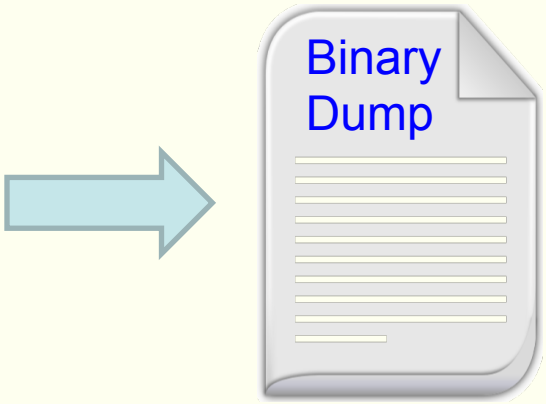




Binary
Dump

Solderless Method 2





Preliminary Observations

- Solderless method seems to be easier
- When JTAGing a phone, tool may crash few times before it can finish the acquisition a 100%.
- Acquisition speed may vary depending on the length of the wires
- Acquisition speed may also vary depending on the solder points

NIST

More Observations

- Solder vs Solderless method
  - speed
  - extracted data
  - binary compare – not hashes
- Analyze and compare data acquired
  - Binary dumps - import data file acquired into forensic tool capable of parsing binary dumps

NIST

Still Learning…

- To identify:
  - differences/similarities between both JTAG methods
  - differences between analysis tools
  - how to combine JTAG boxes and analysis tools

Contacts

James Lyle (project leader)
james.lyle@nist.gov

Rick Ayers
richard.ayers@nist.gov

Jenise Reyes-Rodriguez
jenise.reyes@nist.gov

www.cftt.nist.gov