JTAG Data Extraction & Analysis

NIST

Jenise Reyes-Rodriguez

AAFS - February 17th, 2017

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

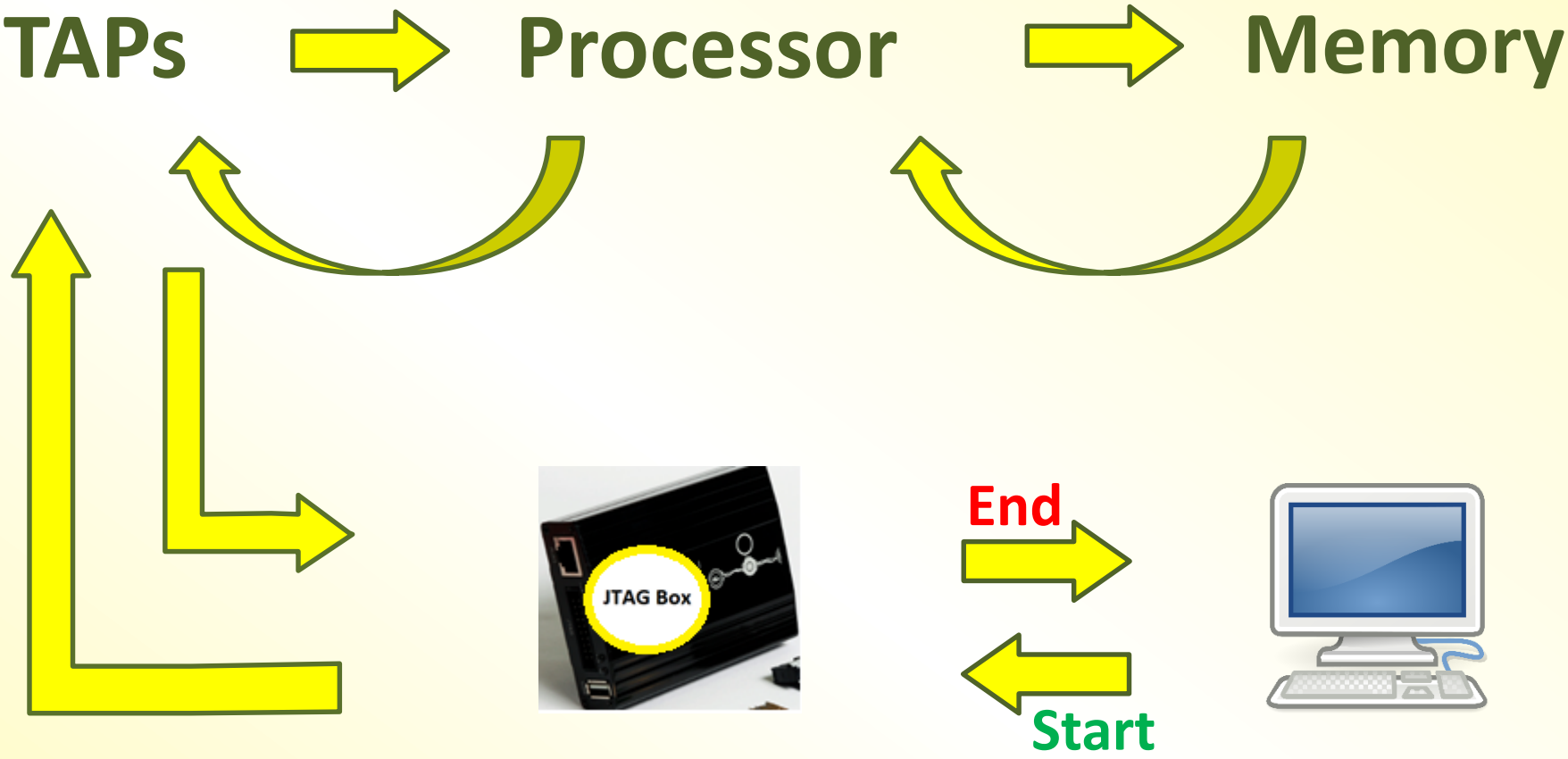
- **Joint Test Action Group (JTAG)**

  Process Overview

- Motivation
- Approach
- Test Observations
- Next Steps

JTAG Process Overview

- Requirements: Memory, Power, TAPs & Processor
- JTAG Cycle



Outline

- JTAG Process Overview
- **Motivation**
- Approach
- Test Observations
- Next Steps

Our Motivation

- Develop a specification for testing JTAG tools, including a strategy for analyzing JTAG data dumps.

- To support the admissibility of JTAG acquires in court by providing the law enforcement community testing information.

Outline

- JTAG Process Overview
- Motivation
- **Approach**
- Test Observations
- Next Steps

Our Approach

Step 1

Soldering Method

Solderless Method
(ISP, eMMC chips)

Step 2

- Parsed binary dumps with Analysis tools
- Analysis Tools = Forensic Tools

Step 3

- Deeper Binary Dumps Analysis

Outline

- JTAG Process Overview
- Motivation
- Approach
- **Test Observations**
- Next Steps

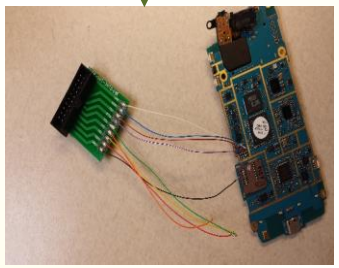
Test Observations

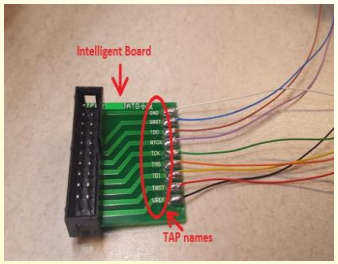
Step 1

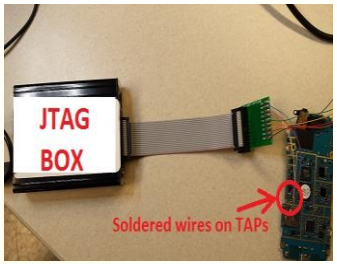
Soldering Method

Binary Dump

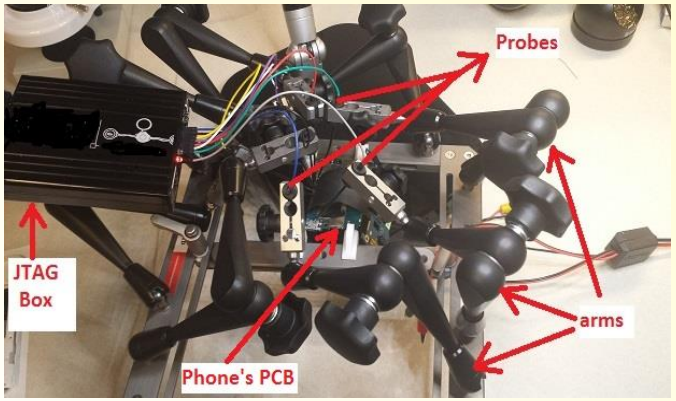
Solderless Method
(ISP, eMMC chips)







Binary Dump

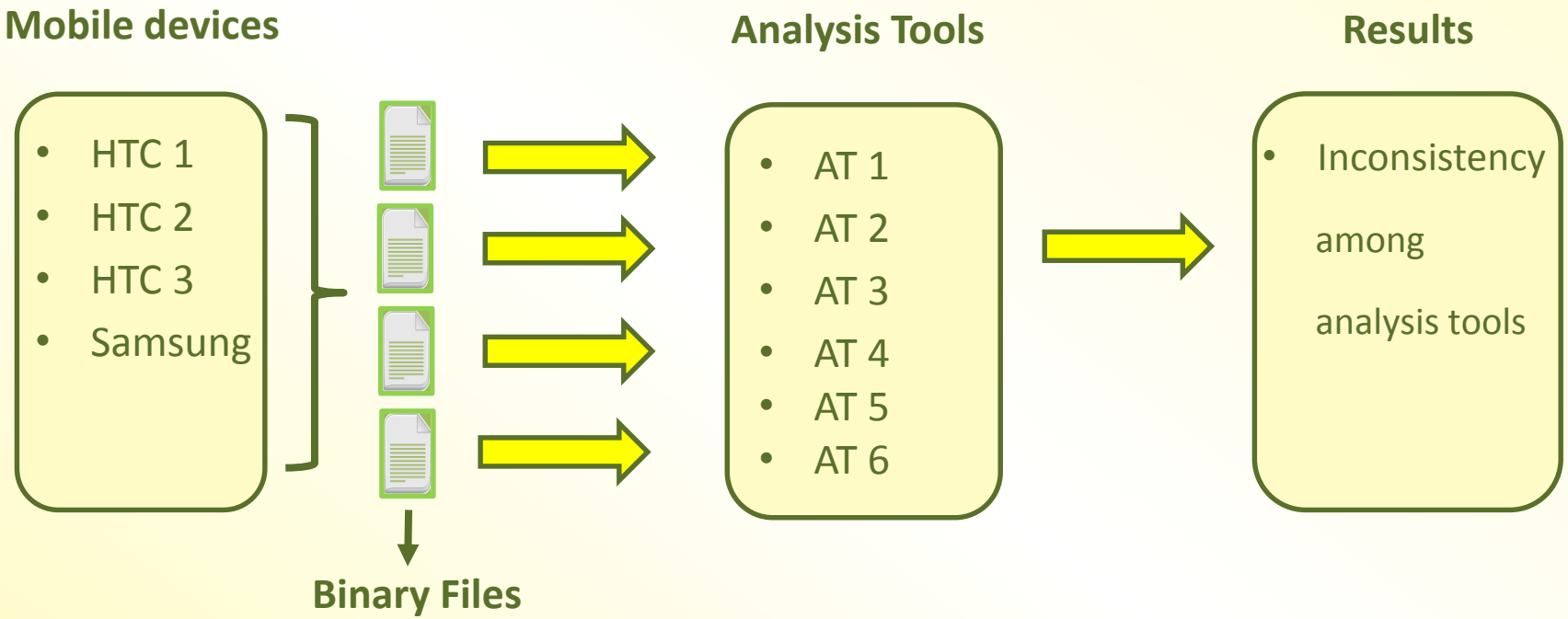


Binary Dump

Test Observations

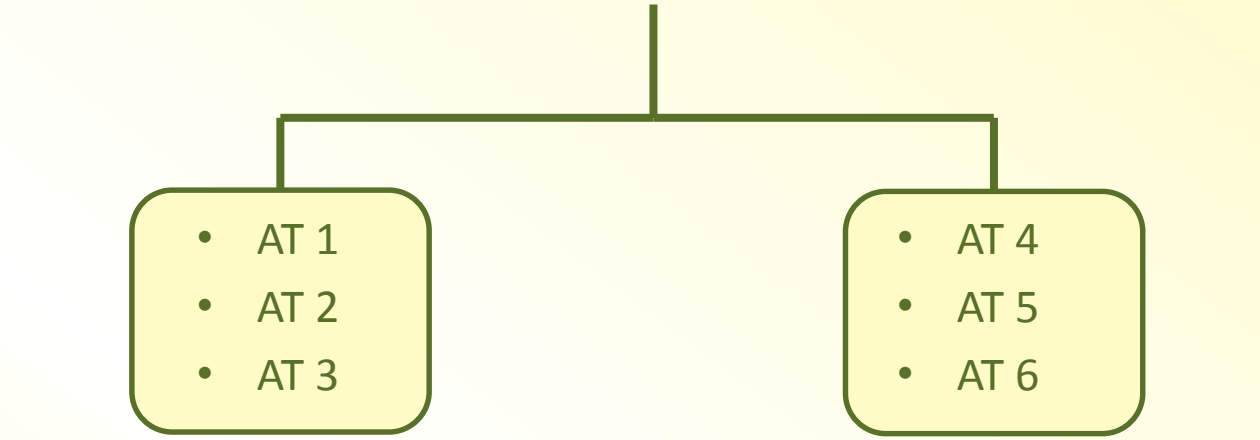
Step 2

- Parsed binary dumps with Analysis tools
- Analysis Tools (AT) = Forensic Tools



Test Observations

Analysis Tools (AT) Differences



Mobile Device forensic tools

⊙ Bette job identifying mobile objects (e.g. call logs….)

Computer Forensic Tools

⊙ Better job key word searching (e.g., IMEI)

Test Observations

Step 3

- Deeper Binary Dumps Analysis
  - Acquisitions (same device & JTAG Box)
  - Different JTAG boxes, same device

So far we have used:
- 2 binary files JTAG box A
- 1 binary file JTAG box B

Are JTAG Tools consistent?

Python Code

Observations

- Acquisitions are very similar
- User data consistent throughout Analysis tools
- Some data blocks differ, maybe system files moving around? **WE WILL INVESTIGATE FURTHER.**

Outline

- JTAG Process Overview
- Motivation
- Approach
- Test Observations
- **Next Steps**

Next Steps

Next Step

- Deeper Binary Dumps Analysis – block hashing
  - Acquisitions using same device & JTAG Box
  - Different JTAG boxes, same device

- Use mobile devices that are supported across most JTAG boxes (we have a total of 5)
- Use 1 device across the boxes:
  - compare the binary files
- Back–to-back acquisitions:
  - same device & JTAG box -> 

- Use analysis tools to compare binary files
- Eventually add **Chip-OFF** to this research

Announcement

July 24-28 @NIST, Gaithersburg, MD

Technical Tracks

- Crime Scene
- Death Investigation
- Human Factors
- Legal Factors
- Quality Assurance
- Laboratory Management
- Criminalistics
- Digital Evidence

go.usa.gov/x9yEK

Or search for “NIST 2017 forensic error management”

Contacts

Jenise Reyes-Rodriguez

jenise.reyes@nist.gov

*** www.cftt.nist.gov ***

James Lyle (CFTT project lead)

james.lyle@nist.gov

Rick Ayers (Mobile Device project lead)

richard.ayers@nist.gov