CFTT – JTAG, Chip-Off
NIST 2019

COMPUTER FORENSIC TOOL TESTING

NIST

010000110100011001010100010100

CFTT at NIST

- CFTT – Computer Forensic Tool Testing Program provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.

Benefits of CFTT

- Tool validation results issued by the CFTT project at NIST provide information necessary for:
  - Users to make informed choices about acquiring and using computer forensic tools
  - Interested parties to understand the tools capabilities
  - Toolmakers to improve tools

Mobile Device – Evidence Sources

Contacts, Calendar, Memos

subscriber/ equipment

Call logs – incoming/o utgoing

Photo, Video, Audio

SMS/MMS

Email, IM, Web data

Social media data

GPS data

Mobile Device Forensics - Challenges

- Multiple interfaces
- Acquisition support for old and current models
- Quality control
- Closed mobile device operating systems
- Damaged devices

Mobile Device Forensics

- Recovering digital data using forensically sound conditions and accepted methods
- Numerous questions arise when encountering mobile devices during an investigation
  - What is the best method to preserve the data?
  - How should the device be handled?
  - How should data be extracted?

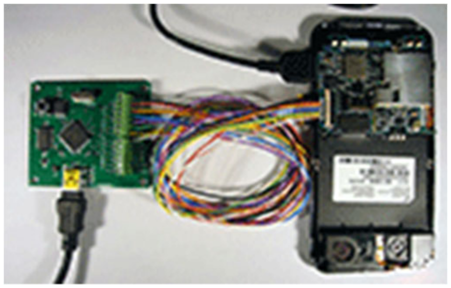
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

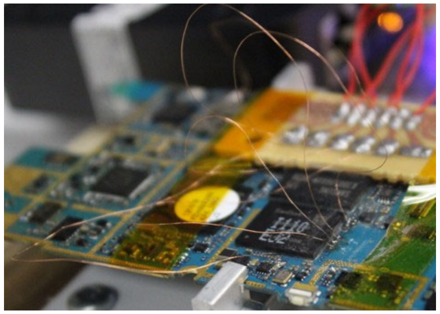
Data Extraction

- Level 1
  - Manual Extraction

- Level 2 – 3
  - Logical Extraction
  - Physical Extraction

- Level 4-5
  - JTAG
  - Chip-Off





JTAG

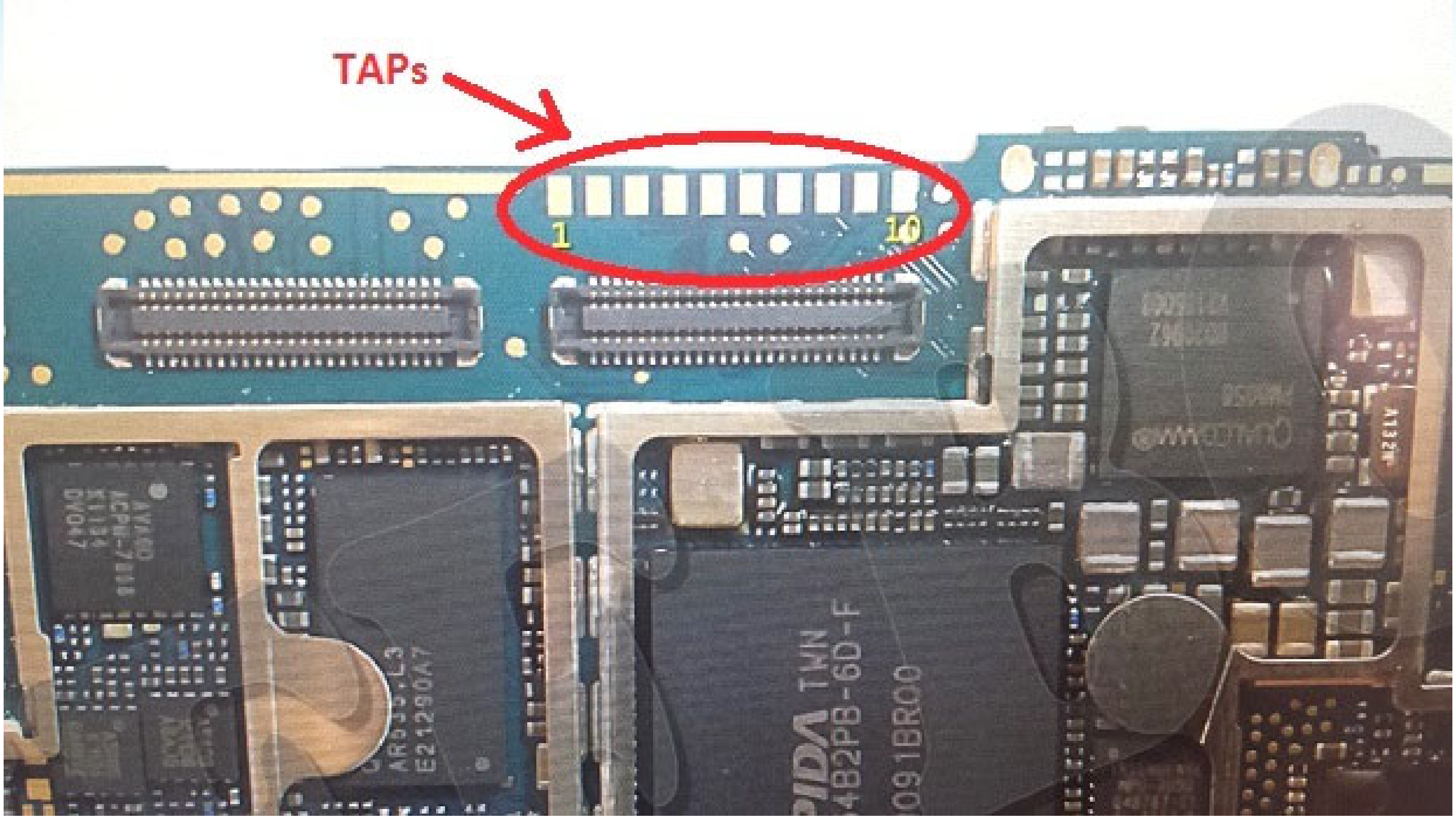
- **Joint Test Action Group**
  - Electronics industry association formed in 1985 for developing a **method of verifying designs and testing printed circuit boards** after manufacture.
  - In 1990 the Institute of Electrical and Electronics Engineers codified the results of the effort in **IEEE Standard 1149.1-1990**, entitled Standard Test Access Port and Boundary-Scan Architecture.

Mobile Forensics and JTAG

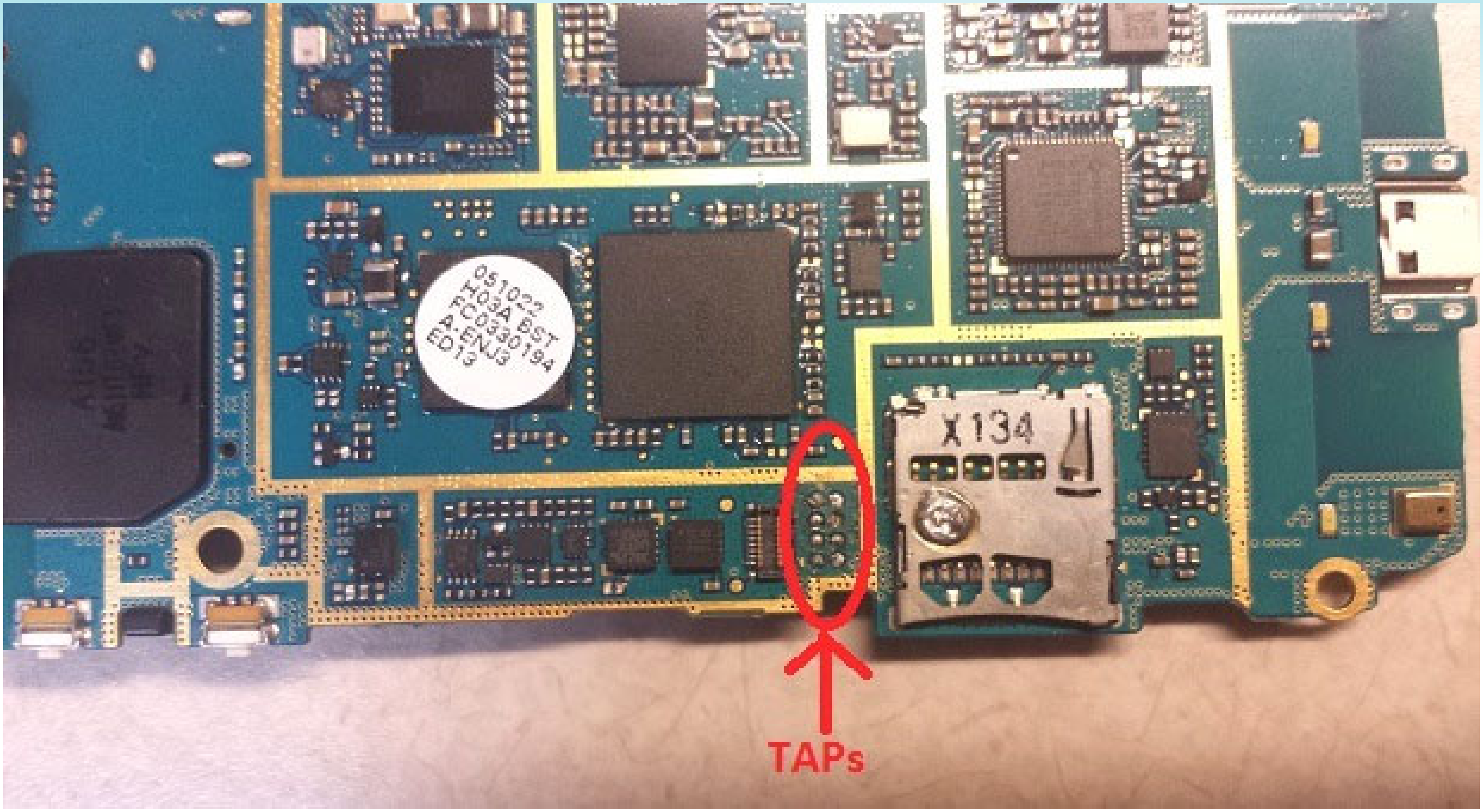
- Advantages
  - Byte-for-byte memory extraction
  - Non-destructive, unlike Chip-off
  - Doesn’t require specific data cables for each make/model
  - Recover PIN-codes, pass-phrases, gesture swipes
  - Bypass phones with locked/disabled USB data ports
  - Data recovery from damaged mobile devices
    - Liquid
    - Thermal
    - Structural

JTAG Requirements

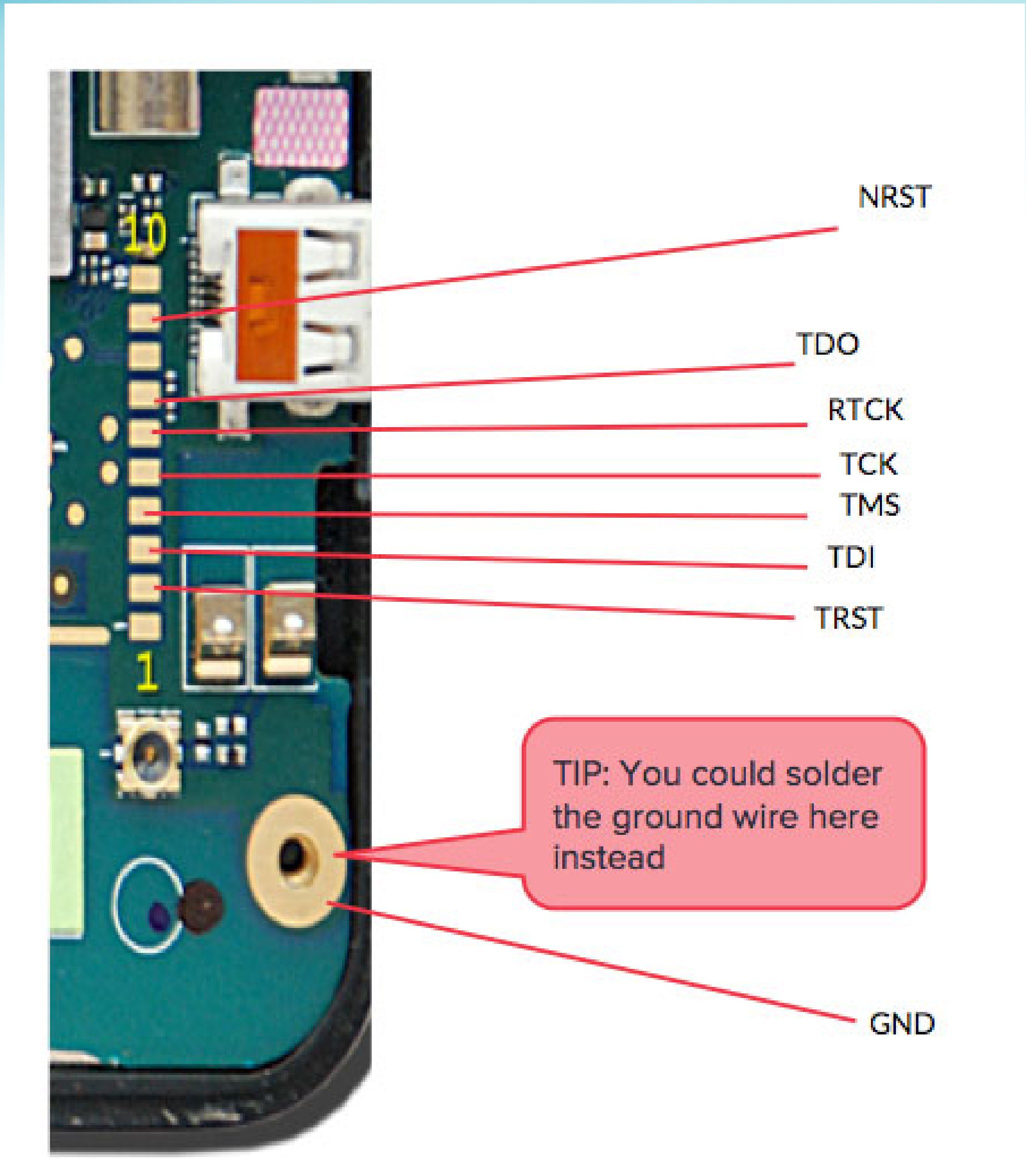
- Power, Memory, TAPs (Test Access Ports) and Processor



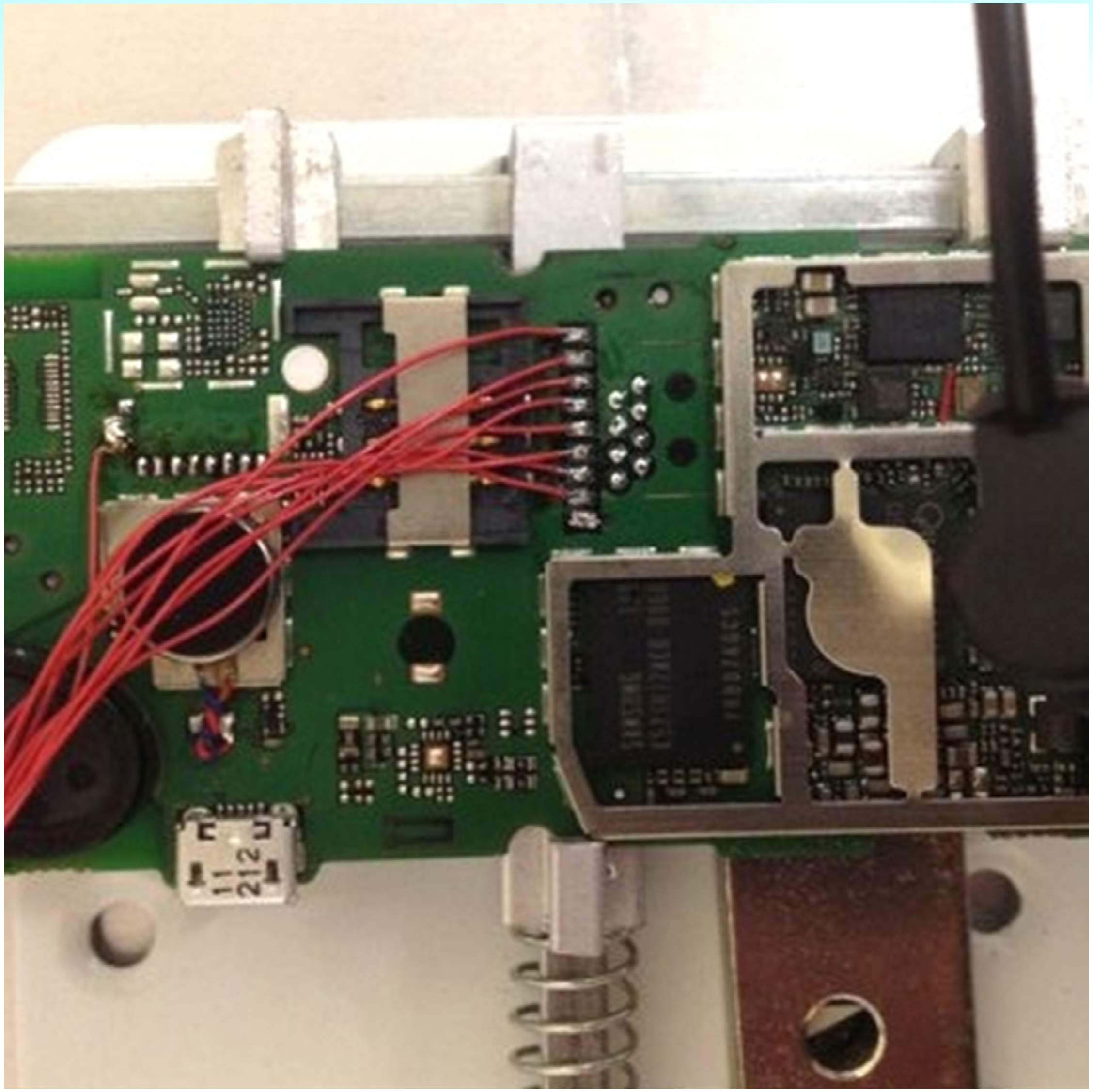
JTAG TAPs



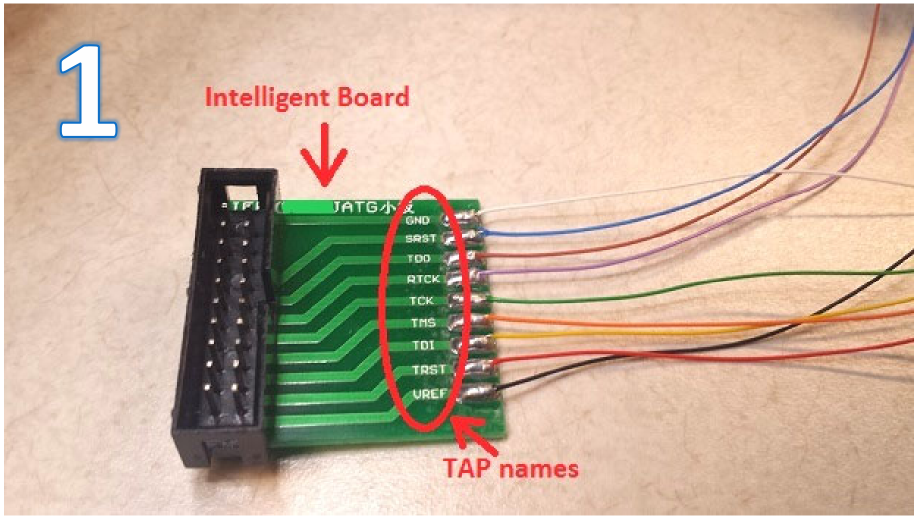
TAPs ID

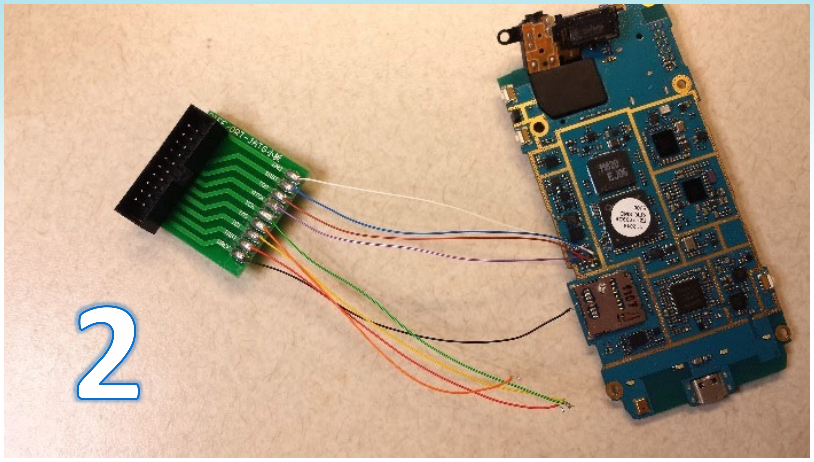

10
1
NRST
TDO
RTCK
TCK
TMS
TDI
TRST
TIP: You could solder the ground wire here instead
GND

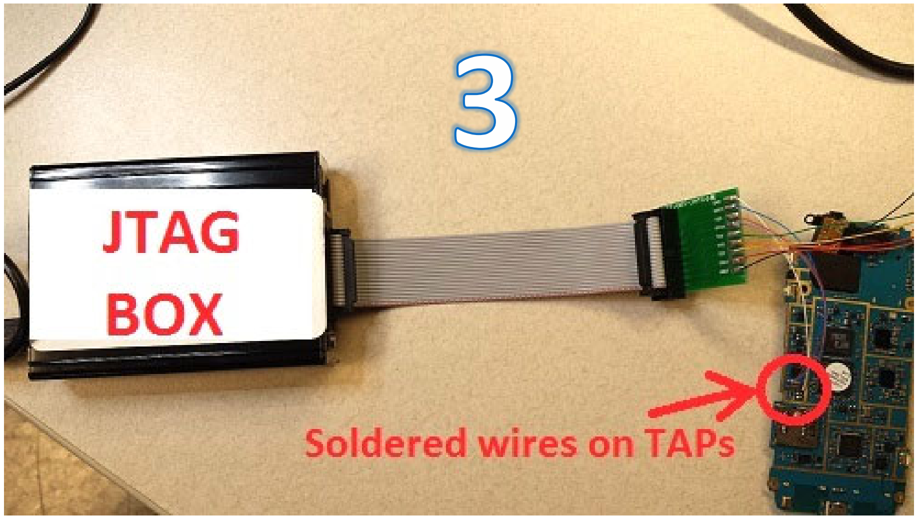
Soldering Method



Soldering Method





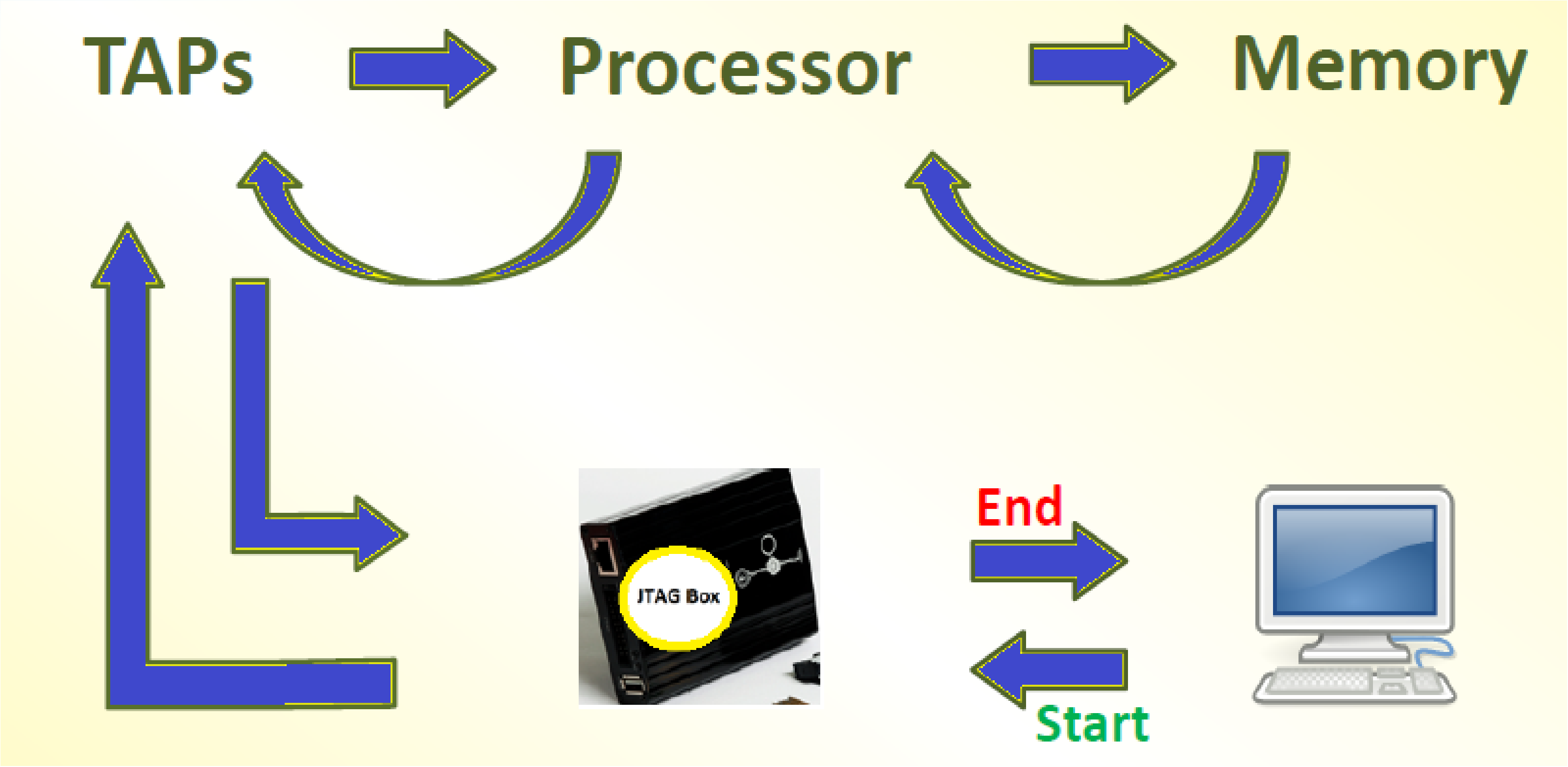


4 Binary Dump

JTAG Process

- Disassemble supported mobile device
- Prepare TAPs
- Connect to JTAG hardware interface
- Power the PCB
- Establish connectivity between the JTAG software and the PCB
- Begin memory extraction => binary image
- Import binary into analysis tool
- Examine memory contents

JTAG Cycle



TAPs

Processor

Memory

End

Start

JTAG Research Phase 1

Device population

- JTAG SW/HW

- Binary Analysis
- 8 Tools
  - 4 mobile
  - 4 traditional

JTAG Testing Phase 2

Device population

- **JTAG** SW/HW

+

- **Chip-Off** SW/HW
  - Help from Fort Worth Texas, VTO Labs

- Binary Analysis
- 8 Tools
  - 4 Mobile
  - 4 Traditional

Research Impacts

- Identify capabilities/limitations
- Differences/similarities across a variety of digital forensic tools capable of parsing a mobile device JTAG binary file
- Informs the forensic community and LE of tools capabilities and limitations
- Provides vendors and tool makers with the opportunity to address any anomalous behavior found

JTAG, Chip-Off Research

- Our research and testing provides the forensic community with an understanding of the capabilities and limitations of a variety of digital forensic tools that provide support for the analysis of Joint Task Action Group (JTAG) and Chip-Off binaries from mobile devices operating over the Android operating system.
- The Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) has performed testing across classic digital forensic tools as well as tools tailored specifically for the data extraction and analysis from mobile devices.

JTAG, Chip-Off Research

- JTAG and Chip-off data extraction provide forensic examiners with the ability to often recover additional data in comparison to a logical or file system data extraction. JTAG is a non-destructive method that returns a byte-for-byte memory dump of accessible data from supported mobile devices.
- Chip-off is a destructive technique that entails removing the flash memory chip from the printed circuit board (PCB). Removing the flash memory entails cutting the PCB and grinding the PCB allowing the chip contacts to be exposed. Once the chip has been prepared the memory registers of the chip are read utilizing the correct adapter and by running a programmer application.

JTAG, Chip-Off Research

- The JTAG and Chip-off research and testing conducted within the CFTT lab includes JTAG and Chip-off binaries from a variety of mobile devices. Each mobile device was populated with a defined dataset including active and deleted data across numerous types of data elements. In addition to binaries collected using either the JTAG or Chip-off data extraction technique, data for supported devices were extracted using both JTAG and Chip-off. Analysis across multiple devices and techniques provides insight into advantages over one technique versus another. Additionally, performing both data extractions on supported devices illustrates any differences between JTAG and Chip-off extractions for a unique mobile device.

JTAG, Chip-Off Research

- The goal of our research and testing within the CFTT program is aimed to inform the forensic community with an understanding of the capabilities and limitations of various digital forensic tools that support analysis of JTAG and Chip-off binary files. These results provide insight into any pros and cons across a combination of supported techniques and tools.

JTAG, Chip-Off Research

- FINDINGS –
- Our research included 8 different Android devices ranging from Android 2.3 Gingerbread to Android 5.1 Lollipop.
- Of the 8 devices 4 of the devices had both JTAG and Chip-Off data extractions performed and the remaining 4 were Chip-Off.
- Overall the user data analyzed from JTAG and Chip-Off acquires has shown to be mostly consistent.
- There This differences were some minor differences but this was based on issues with a particular tool's ability to parse and report the data.

JTAG, Chip-Off Research

- Overall the tools ability to report the user data populated onto each device was as expected. Some problem areas include specific versions of social media applications e.g., facebook, linkedin, twitter, Instagram, pinterest, snapchat, whatsapp, etc.
- Software tailored to extract data from a mobile device typically normalized data artificats more so than traditional forensic extraction software. Data normalization makes it much easier to quickly identify data artifacts that may be of interest. While the data imported and parsed with a traditional software tool is present, it is much more difficult to find specific data artifacts. The user has to sort through individual folders and files.