JTAG and Chip-Off Data Analysis and Testing

NIST

Jenise Reyes-Rodriguez

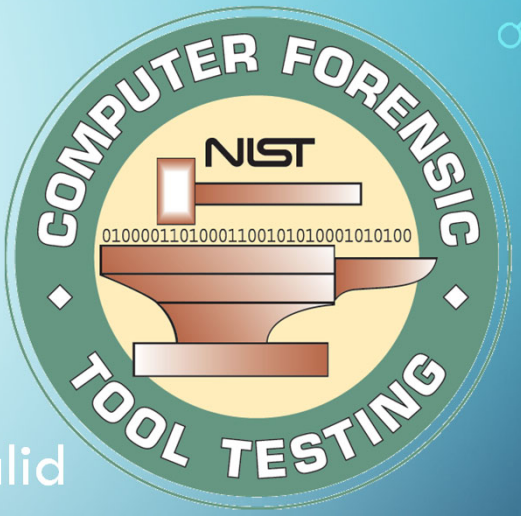
AAFS – February 20th, 2020

Anaheim, California

DISCLAIMER

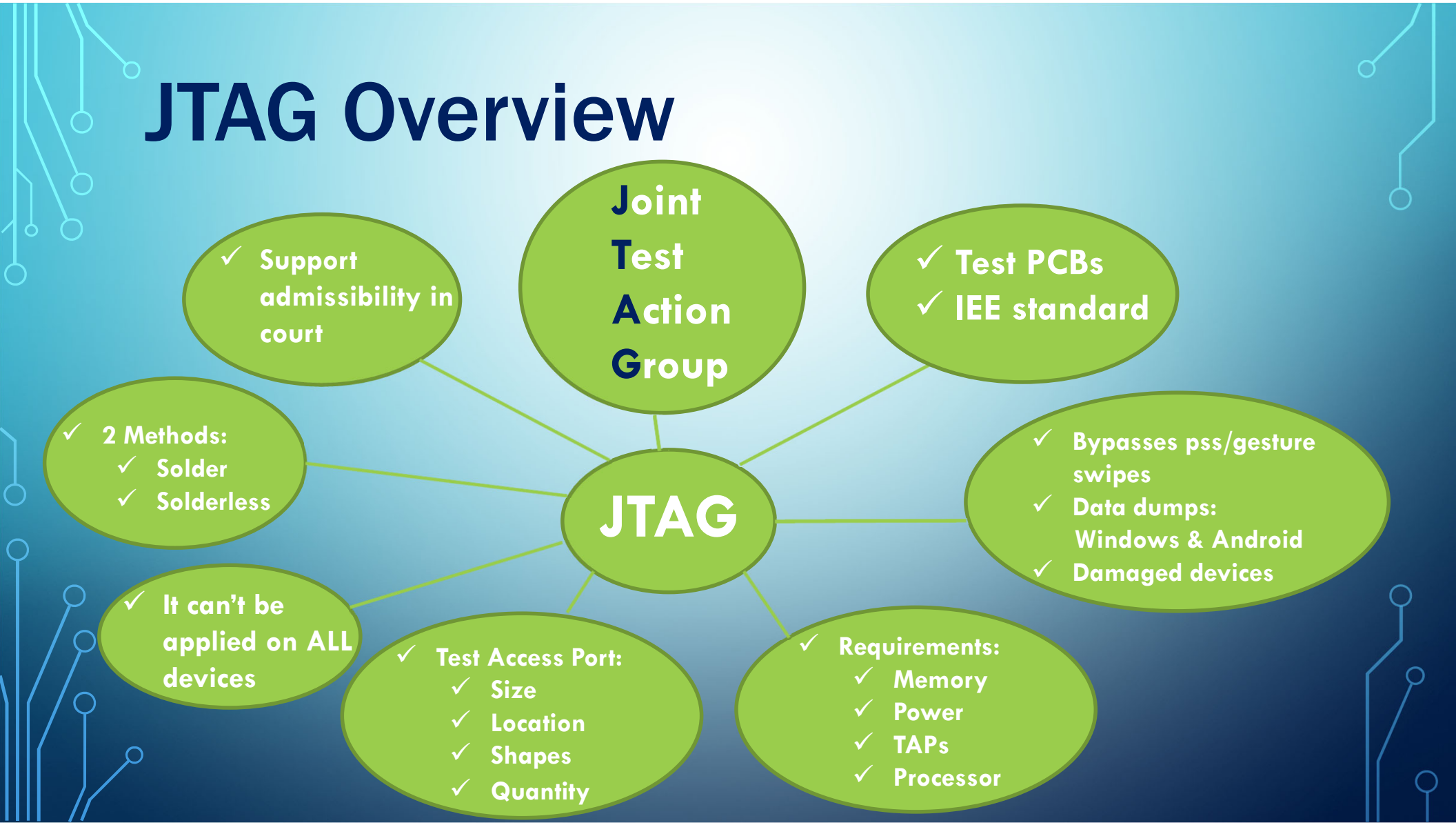
Certain company products may be mentioned or identified. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that these products are necessarily the best available for the purpose.

CFTT at NIST

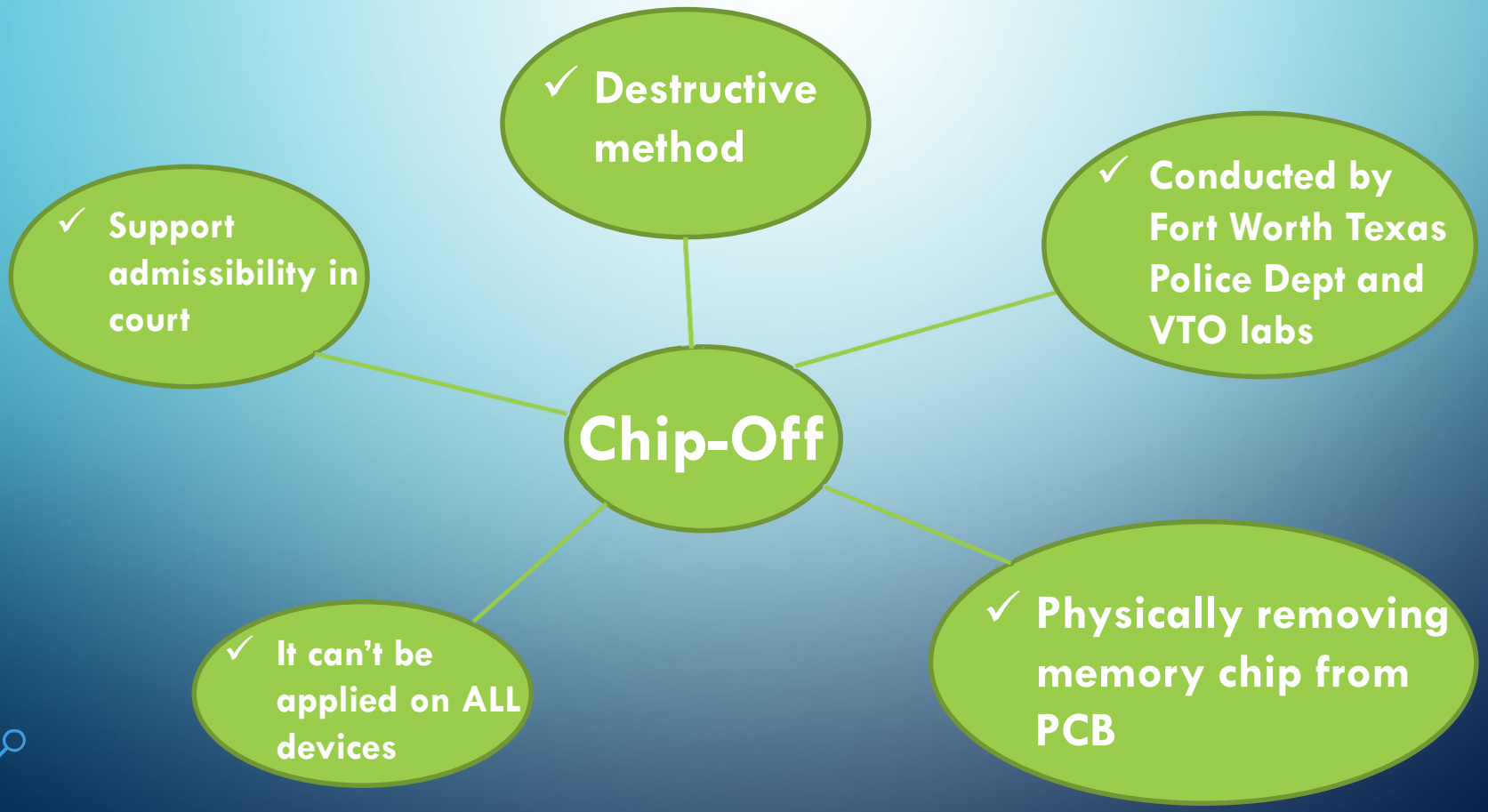


- Provides method of assurance that tools used in computer-related crime investigations produce valid results.
- Benefits:
  - Users make informed choices about acquiring/using computer forensic tools
  - Interested parties – understand the tools capabilities
  - Toolmakers – improve their tools

JTAG Overview



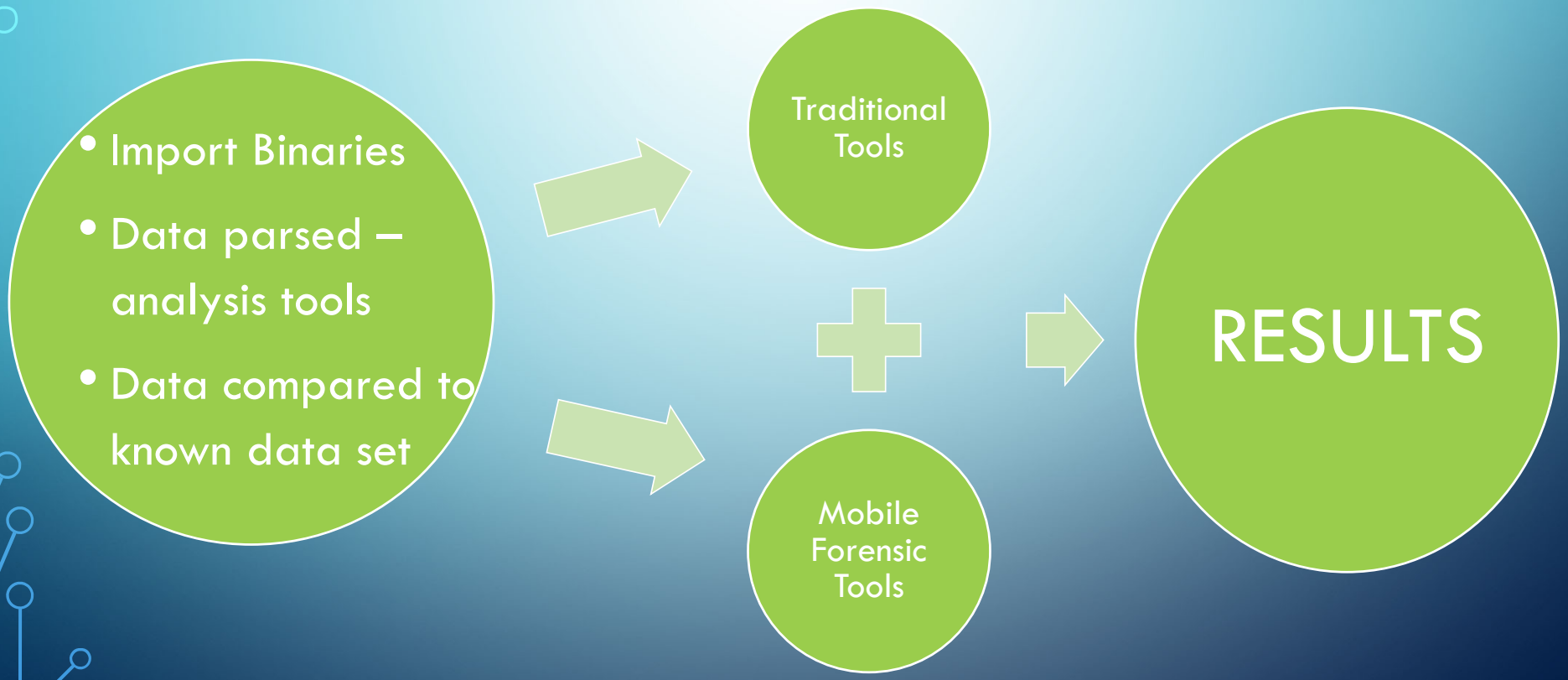
Chip-Off Overview



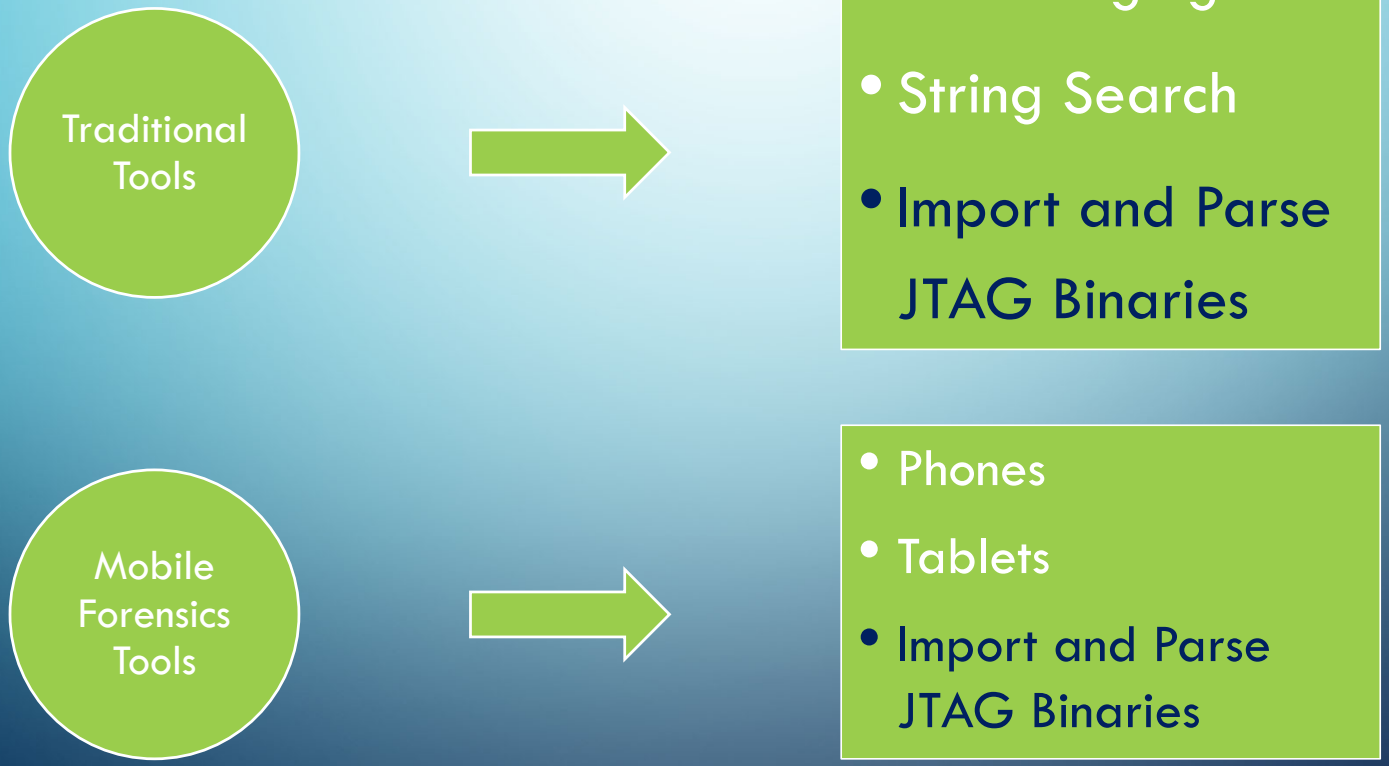
JTAG and Chip-Off side by side

Some Advantages	JTAG	Chip-Off
*Byte-for-byte memory extraction	Yes	Yes
Destructive process	No	Yes
Require specific data cables for each make/model	No	No
Recover PIN-codes, pass-phrases, gesture swipes	Yes	Yes
Bypass phones with locked/disabled USB data ports	Yes	Yes
Data recovery from damaged mobile devices (liquid, thermal, structural)	Yes	Yes

Data Analysis Flow



Analysis Tools



Data Analysis

- 9 tools used
- 10 devices

Results – Analysis Tools

- Differences between analysis tools types?

Differences	Traditional Tools	Mobile Forensics Tools
Presentation of Data	Presents the data in file explorer view format	Presents and categorizes the data better

* User data doesn't change *

Results – JTAG Technique

- Analysis tools anomalies for JTAG:
  - Social Media data:
    - Facebook, Pinterest, SnapChat were partially or not reported – mostly Facebook/most tools
  - Stand-alone files
    - graphic, video, audio not reported for some devices – an analysis tool

Results – JTAG Technique Cont.

- Analysis tools anomalies for JTAG:
  - GPS:
    - Coordinates or address not reported for some devices – some tools

Results – Chip-Off Technique

- Analysis tools anomalies for Chip-Off:
  - Social Media data:
    - Facebook, Pinterest, SnapChat were partially or not reported – mostly Facebook/most tools
  - Stand-alone files
    - graphic, video, audio not reported for some devices – most tools

Results – Chip-Off Technique Cont.

- Analysis tools anomalies for Chip-Off:
  - GPS:
    - coordinates or address not reported for some devices – most tools

Conclusions

- JTAG vs Chip-Off
  - both techniques were consistent across the board
- Analysis Tools Types
  - data presentation varies

Contacts

Jenise Reyes-Rodriguez

Jenise.reyes@nist.gov

Richard Ayers

Richard.ayers@nist.gov

Barbara Guttman

Barbara.guttman@nist.gov