NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Going deeper and deeper into Cell Phones

Jenise Reyes-Rodriguez
Software and Systems Division, ITL
NIST November 13, 2019

Welcome to NIST!

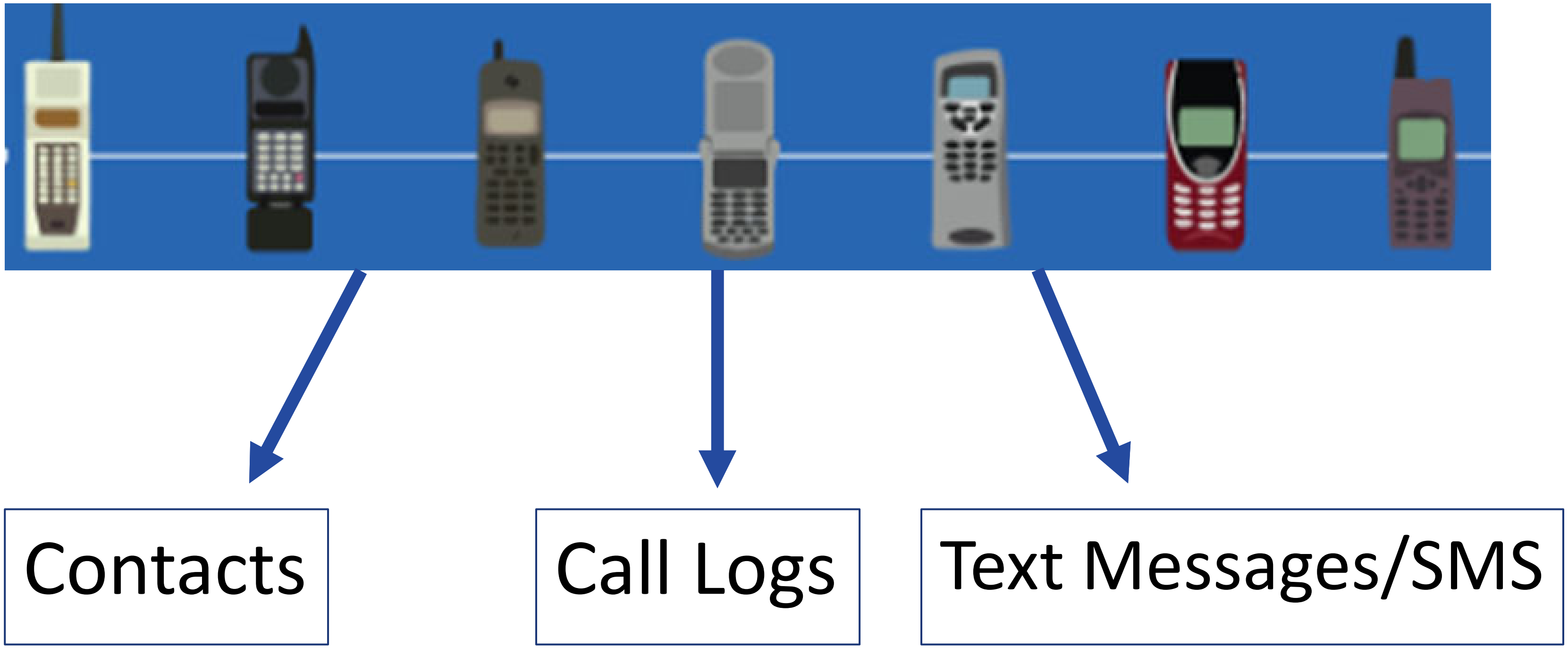
☺

Computer Forensic Tool Testing

- Provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.
- Established around year 2000
- Develop a **specification for analyzing mobile device memory/binary dumps** and to **support the admissibility of forensic data in court** by providing the law enforcement community testing information

Evolution of Cell phones

Some time ago…



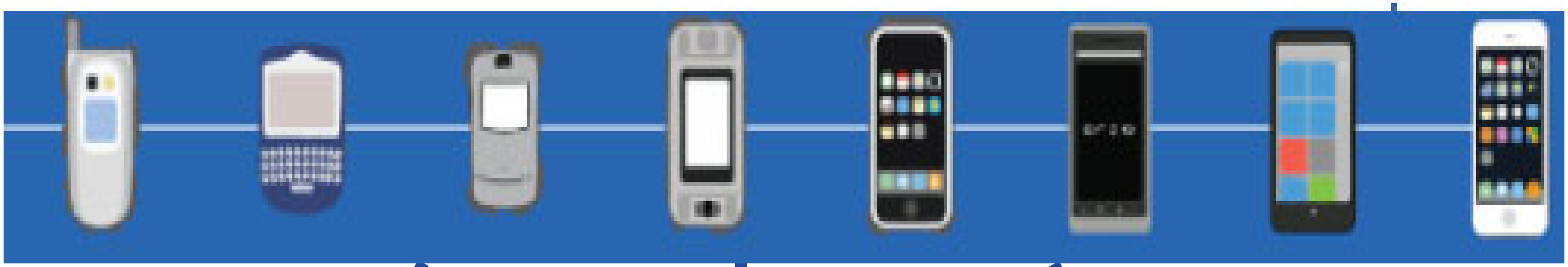
Contacts

Call Logs

Text Messages/SMS

More current cell phones

Up to this day…



Contacts

Call Logs

Text Messages/SMS

Calendar entries

Apps

Notes/Memos

GPS

MMS

Emails

Media files
(audio, pictures, video)

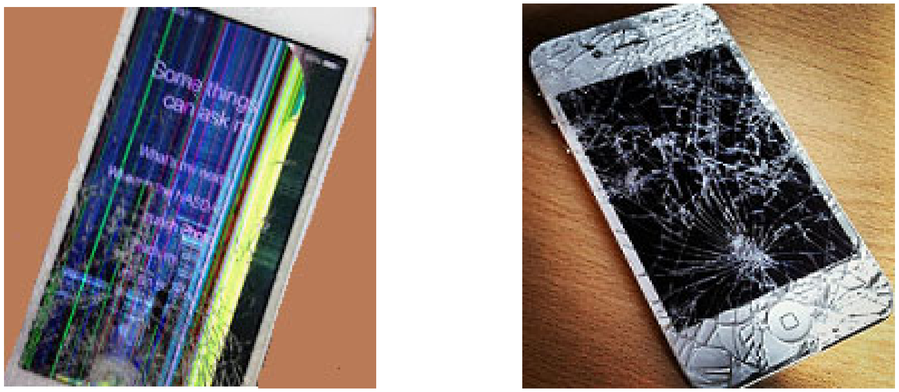
Browser history

Deleted data

Damaged devices

Damaged Devices

structural



liquid

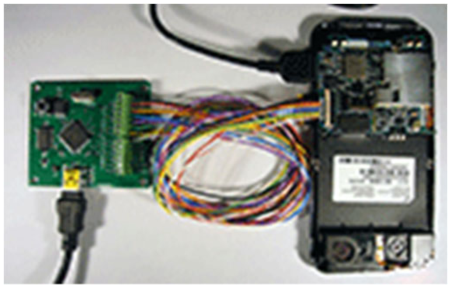
heat

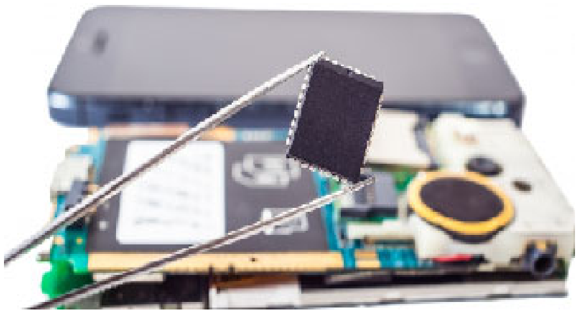
Data Extraction

- Level 1
  - Manual Extraction

- Level 2 – 3
  - Logical Extraction
  - Physical Extraction

- Level 4-5
  - **JTAG**
  - **Chip-Off**





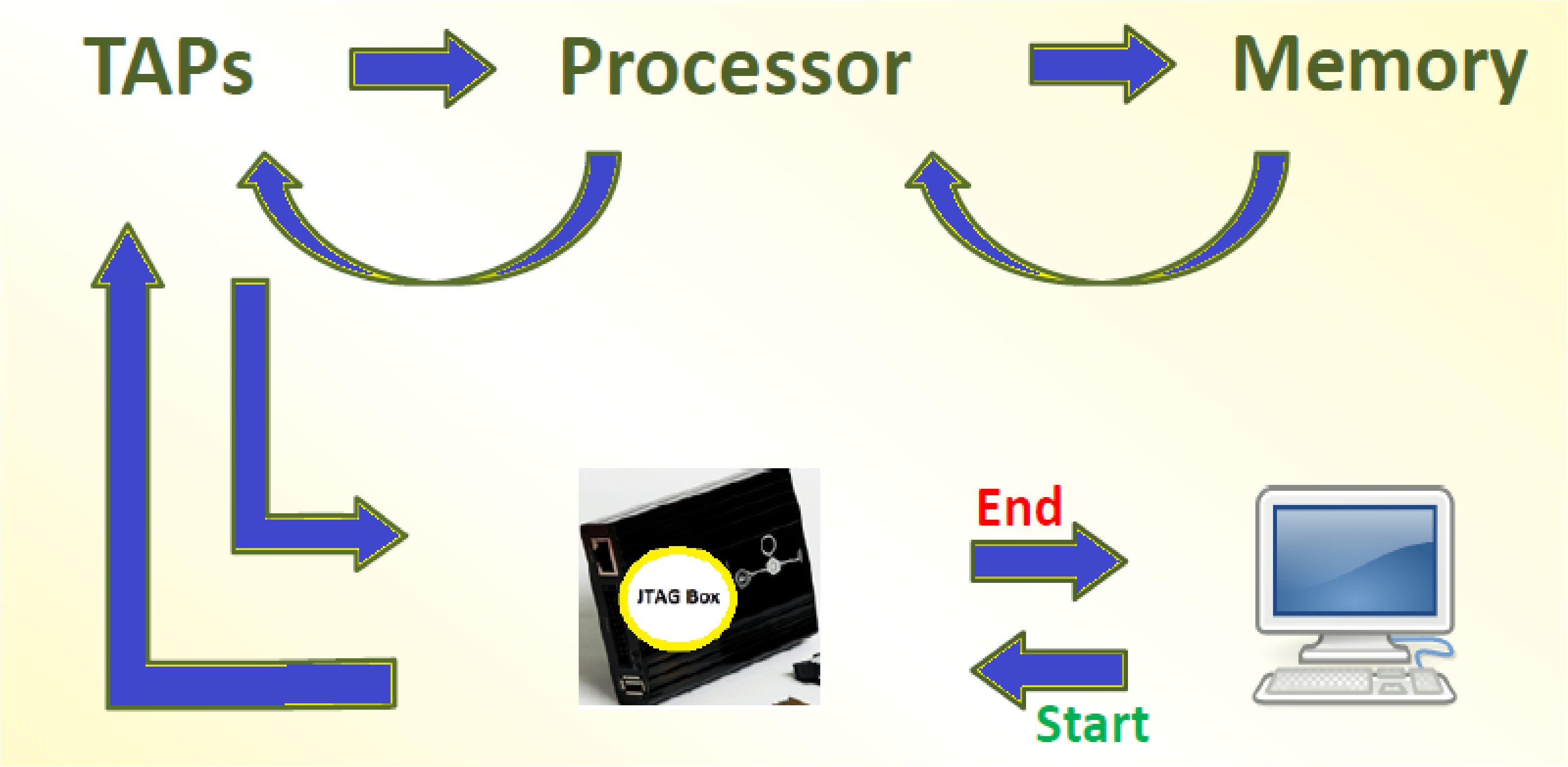
JTAG

- 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.

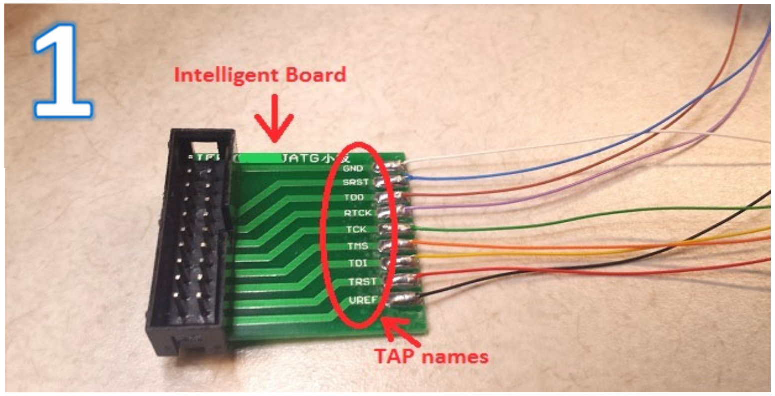
JTAG Requirements

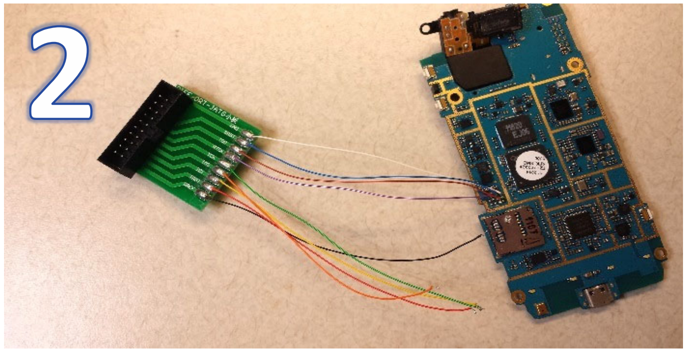
- Power
- Memory
- TAPs (**T**est **A**ccess **P**orts)
- Processor

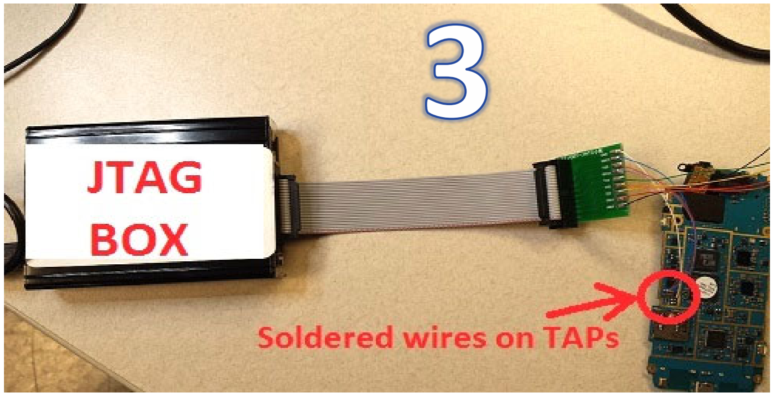
JTAG Cycle



JTAG Method 1 – Solder



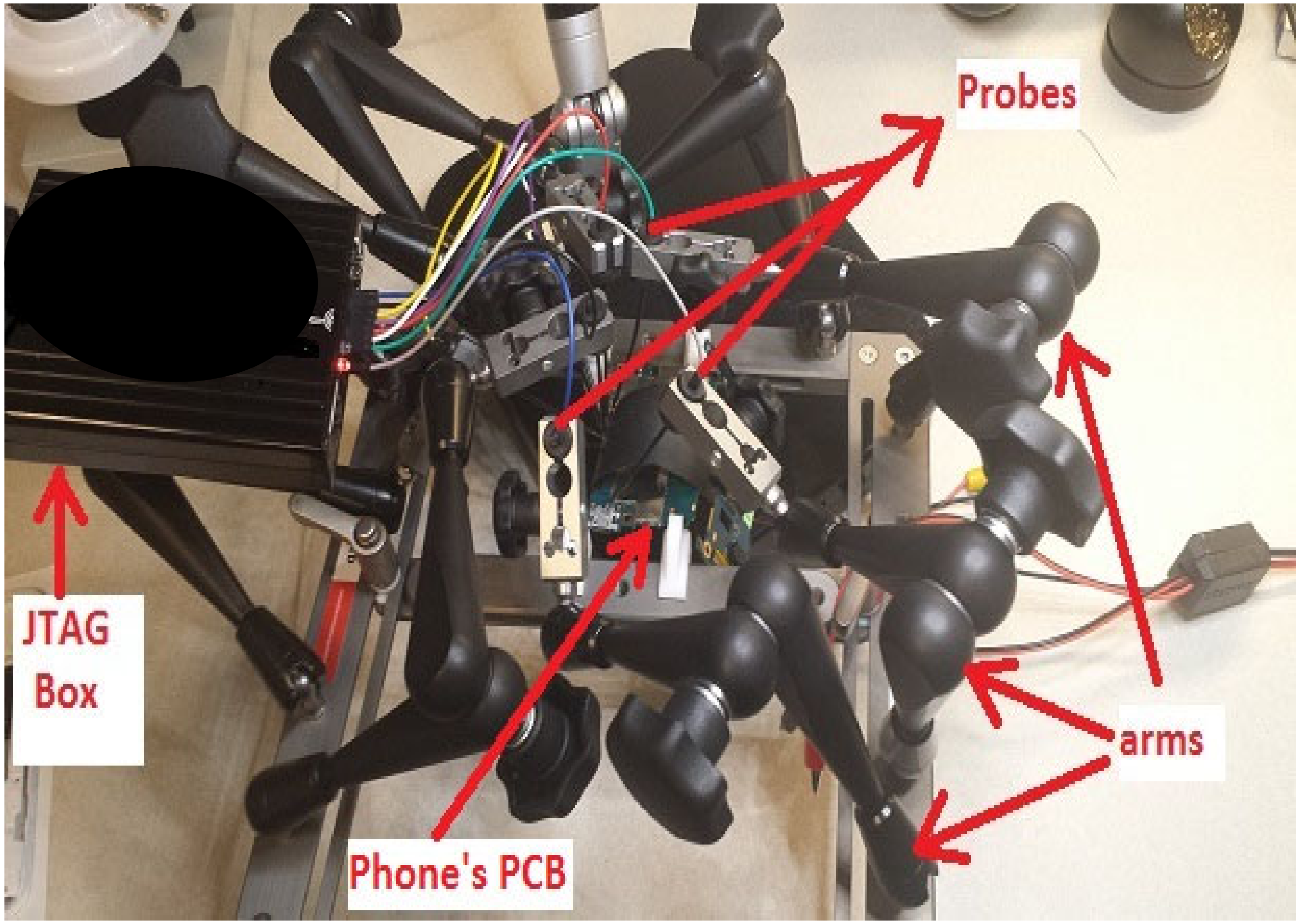


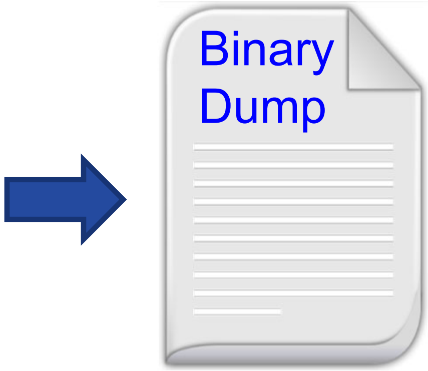


4

Binary Dump

JTAG Method 2 – Solderless


[redacted]

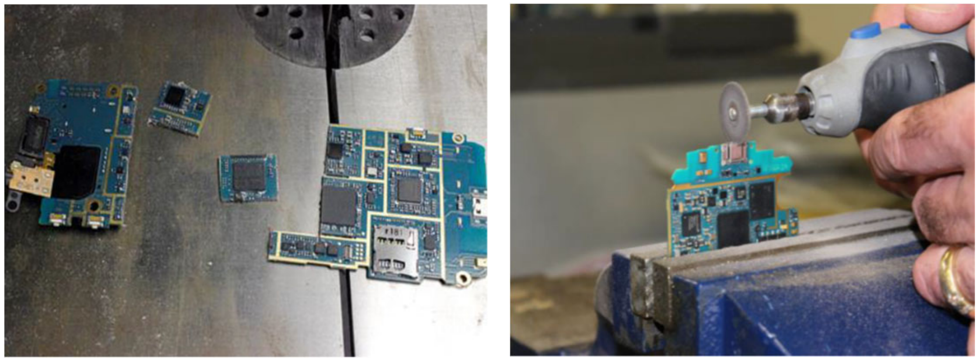


Chip-Off

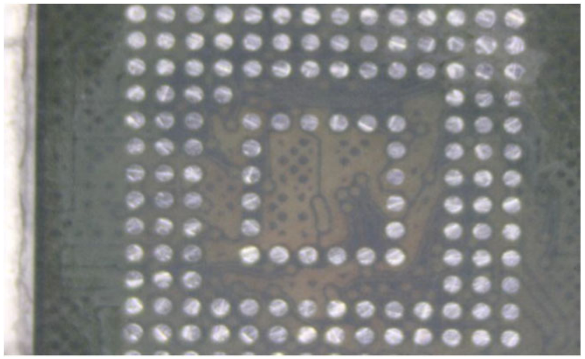
- Advanced digital data extraction and analysis technique which involves **physically removing flash memory chip**(s) from a subject device and then **acquiring the raw data** using specialized equipment
- **Conducted by Fort Worth, Texas Police Dept.**

Chip-Off Process - Material Removal

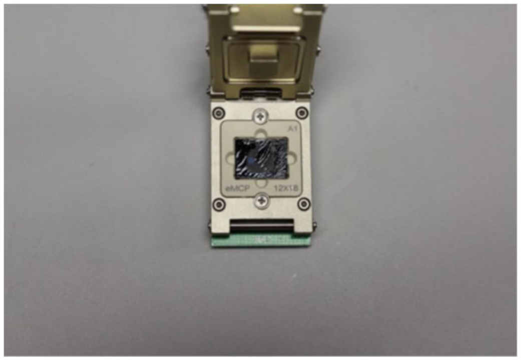
1 cutting/removing



2 cleaning/grinding



3 reading chip



4

Binary Dump

JTAG & Chip-Off in forensic investigations

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

*It depends

NOTE: applies only to Android and Windows devices

Data Analysis - Analysis Tools

- Import binary files
- Review data parsed by analysis tools and compare with the known data set

Analysis Tool Types

General Purpose

- disk imaging
- string search
- **import and parse JTAG binary dump**

Mobile devices

- phones
- Tablets
- **import and parse JTAG binary dump**

Difference among the tools?

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

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.
- 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.

Contact Information

Jenise Reyes-Rodriguez

jenise.reyes@nist.gov

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

James Lyle

James.lyle@nist.gov

Rick Ayers

Richard.ayers@nist.gov