Mobile Device Forensics – NIST 2019

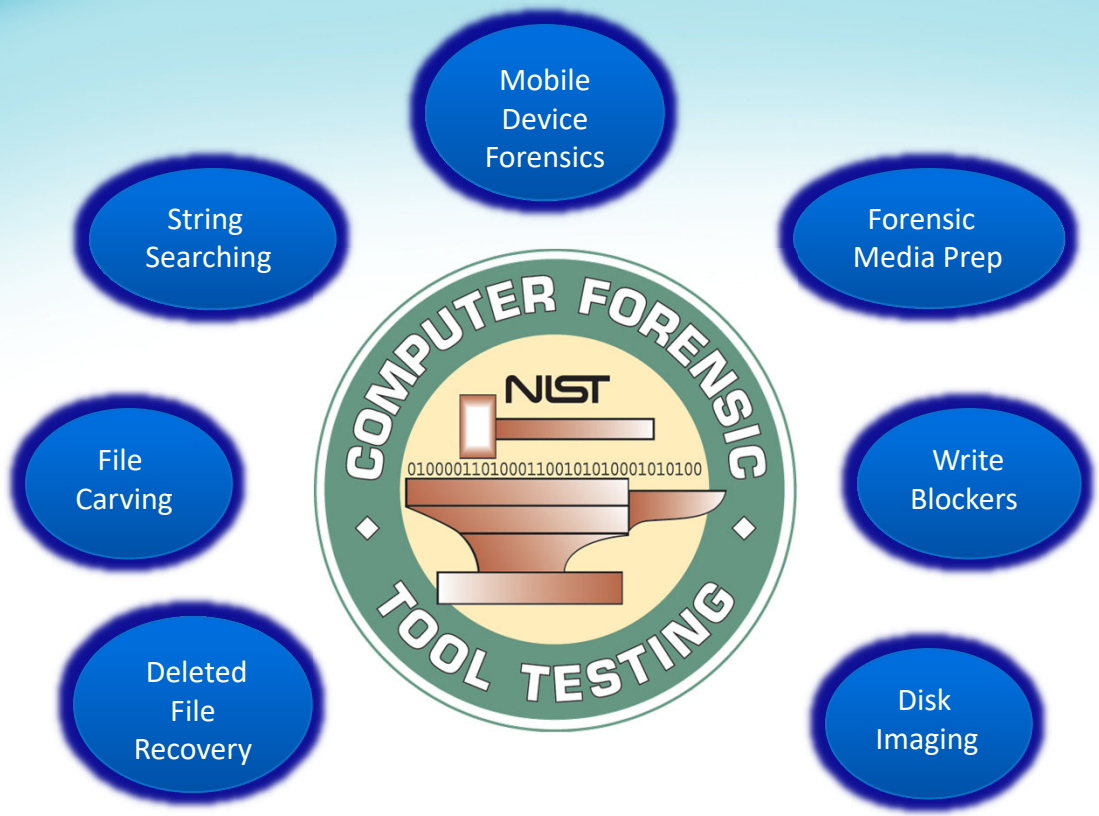
Rick Ayers

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



TEST SPECIFICATIONS

TEST ASSERTIONS AND TEST PLANS

SETUP DOCUMENTS

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?

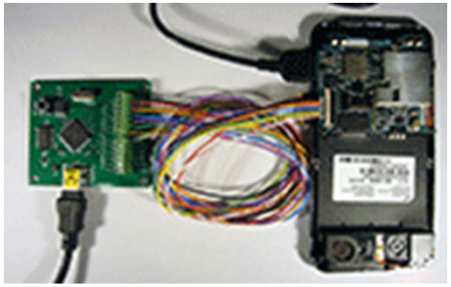
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

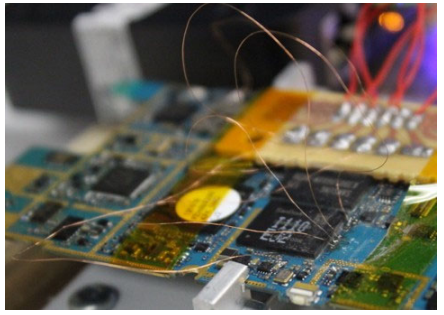
Data Extraction

- Level 1
  - Manual Extraction

- Level 2 – 3
  - Logical Extraction
  - Physical Extraction

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





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