iTL

Mobile Device Data Population for Tool Testing

COMPUTER FORENSIC TOOL TESTING
NIST
0100001101000110010101010001010100

Rick Ayers

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Agenda

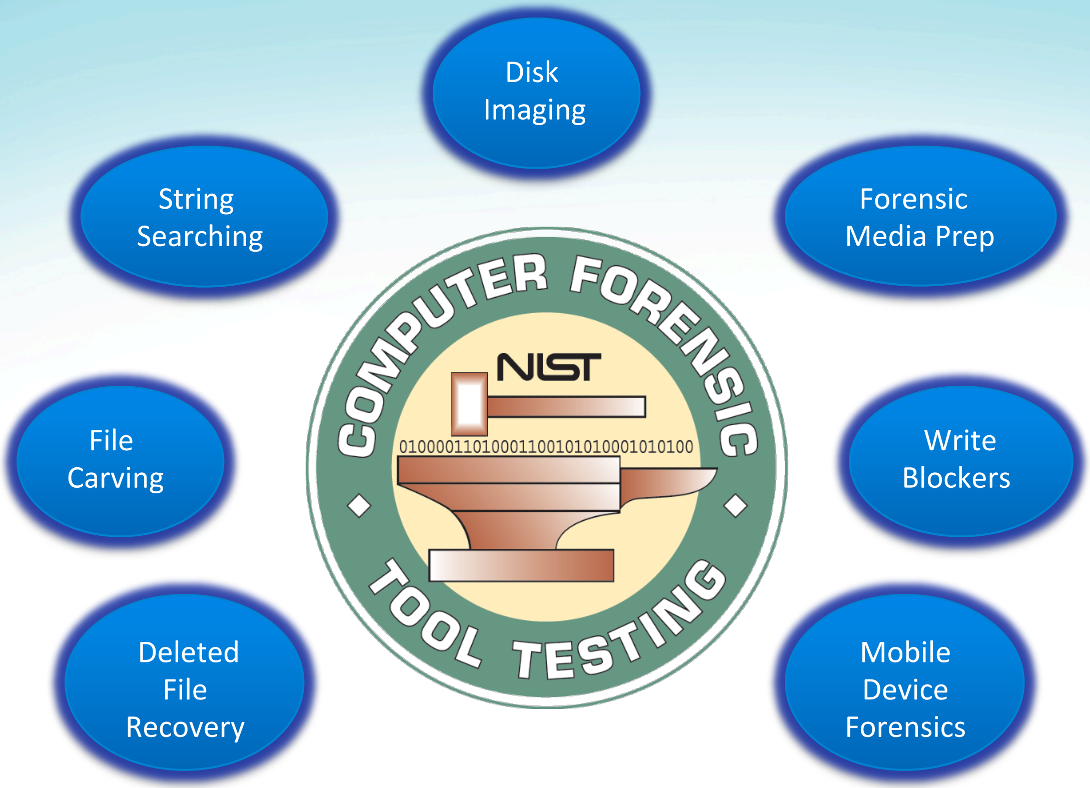
- Mobile Device Forensics Challenges
- Computer Forensic Tool Testing (CFTT) Program
- Setup and Test Procedures
- Mobile Device Data Population
  - Data Types
  - Population Techniques
  - Factors

Challenges

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

FEDERATED TESTING

COMPUTER FORENSICS TOOL CATALOG



TEST SPECIFICATIONS

TEST ASSERTIONS AND TEST PLANS

TEST REPORTS

SETUP DOCUMENTS

Setup and Test Procedures

- Objective: Documentation on data population of target media and test procedures providing third parties with information for an independent evaluation or replication of posted test results.
- Contents:
  - Data types
  - Test case execution procedures
  - Data population techniques

Mobile Device Data Population Factors

- Fresh / Unused mobile device
- PII on device with existing user data
- Connectivity: Cellular, WiFi, Bluetooth, PC synchronization

Mobile Device Data

- Subscriber / Equipment related data
  - Useful for uniquely identifying a cellular subscription and physical identification of a mobile device
    - IMEI, ESN/MEID, ICCID, MSISDN, SPN
- Address Book / Contacts
  - Contact name, associated number, metadata
  - Long, Regular, Special character, Blank, Non-Latin character entries
  - Contact metadata: email, address, URL, birthdates, pictures, ring-tones, notes

Mobile Device Data

- Personal Information Management (PIM) data
  - Datebook / Calendar, Memo (long, regular, special character entries)
- Call Logs
  - Incoming, outgoing, missed
  - Date / time and duration
- SMS / Chat / MMS Messages
  - Incoming, outgoing, drafts, deleted
  - Long, Regular, Special character, non-Latin character entries
  - Audio, graphic, video attachments

Mobile Device Data

- Stand-alone files
  - Audio: wav, aiff, mp3, flac, mp4
  - Graphic: jpg, gif, bmp, png, tiff
  - Video: 3gp, mov, flv, avi, wmv
- Email
  - Incoming, outgoing, drafts, deleted
  - Attachments: audio, graphic, video, txt, doc, pdf, etc.
- Native / Third-party applications
  - Vary based on manufacturer

Mobile Device Data

- Internet related data
  - Browsing history
  - Bookmarks
- Social media data
  - Profile data
  - Status updates
  - PMs
- GPS data
  - Longitude / Latitude coordinates
  - Geotagged pictures / video

Data Population Techniques

- Manual input
- E-mail client pairing
- PC synchronization
- Bluetooth

Mobile Device Population Techniques

- Manual input (time consuming)
  - SMS/MMS messages (incoming, outgoing, read, unread, active/deleted, drafts)
  - Call logs (incoming, outgoing, missed, date/time/duration, active/deleted)
  - Third-party application data
  - Social media data
  - GPS related data
- E-mail client pairing
  - Contacts, calendar entries, memos, stand-alone files (audio, graphic, video, docs)

Mobile Device Population Techniques

- PC Synchronization
  - Stand-alone files (audio, graphic, video, documents)
- Bluetooth pairing
  - Supported data objects e.g., Contacts, calendar entries, memos
  - Photos, video, audio files

Mobile Device Population Techniques

- Subscriber / Equipment Data
  - IMEI – battery cavity, *#06#
  - ICCID – printed on UICC
  - MSISDN – mobile device settings

Conclusions

- **Challenges of Mobile Forensics**
- **Overview of CFTT**
- **Setup and Test Procedures documentation**
  - **Goal:** provide techniques for populating mobile devices used for testing mobile forensic data extraction tools
- **Data Population Factors**
- **Common Mobile Device Data Elements**
- **Mobile Device Data Population Techniques**

Thank You!

Contact Information:

Rick Ayers

richard.ayers@nist.gov

www.cftt.nist.gov/mobile_devices.htm