Outline

• Trends & challenges in mobile forensics

• Developments in digital evidence that will change mobile forensics

• Responses & suggestions for moving forward

• Questions & comments
A Plentora of Devices

- The New York Times
- Sony e-book reader
- Flipshare device
- Sylvania laptop

View & organize videos
Email videos
Publish clips online
Make movie mixes with music
Capture photos from videos
Dozens of Tools
Demand for Services Is Up
Storage Capacity is Increasing
Increased Security

- More data stored as plain text
- Increases in computing power and memory
- Easier to implement good security
Traditional Access Methods Becoming More Difficult

- **Bootloaders**
  - Manufacturers implementing security in boot ROM

- **JTAG Ports**
  - Manufacturers not connecting JTAG pins to accessible test pads

- **Chip Removal**
  - Increased use of custom/proprietary IC processor and memory chips
Significant Developments in Digital Evidence

- Investigative Based Model
  - Non-forensic
  - Non-examiner
  - Timely/rapid
  - On-scene
  - Live capture
  - Preview/triage
  - Low cost/COTS
  - Further the investigation

- Laboratory Based Model
  - Forensic
  - Highly skilled
  - Methodical
  - Comprehensive
  - Static
  - Robust QA Program
  - High cost
  - Fair, impartial & scientific
Significant Developments in Digital Evidence

- The Perfect Storm
  - DNA becomes new standard
  - West Virginia State Police Crime Lab
  - Houston Crime Lab
  - Baltimore County Circuit Court Judge rules against latent prints
  - FBI Madrid Train Bombing
  - The Innocence Project
Significant Developments in Digital Evidence

- 13 Recommendations, including:
  - NIFS
  - Remove control from law enforcement
  - Mandatory accreditation
  - Mandatory certification
    - Licensing??
  - Mandatory QA
  - National Code of Ethics
A Path Forward...

- Minimum Quality Assurance Standards
- Leveraging off of Non-Examiners
- Aggressive use of preview
- More robust tools
- Increased sharing of resources
- Increased standardization for mobile devices
- Increased participation
Minimum Quality Assurance Standards?

- Write protection OR copy
- Chain of custody
- Known tools
- Peer review
- Contemporaneous notes
- Written report
- ???
Leverage off of Non-examiners

- Investigators/CPIK: 50%
- Non-Cell Phone Certified Examiners: 30%
- Cell Phone Certified Examiners: 15%
- HQ Experts: 5%
Example: CPIK

• Making available two easy to use cell phone tools to special agents and investigators for previewing at least a portion of data.

• Cell Phone Investigative Kiosks are being set up at FBI Field Offices and Regional Computer Forensic
Aggressive Use of Previews

- New Zealand Police Model
  - 80 percent reduction in submitted matters
  - 100 percent of resources on 20 percent of cases
More Robust Tools

- Results are always different for different Manufacturers
- Each product does well in some areas and not so well in other areas
- Don’t focus on low hanging fruit

<table>
<thead>
<tr>
<th>Product</th>
<th>Contacts</th>
<th>Call Logs</th>
<th>Calendar</th>
<th>Message</th>
<th>Photos</th>
<th>Audio</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Yes</td>
<td>Partial</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>B</td>
<td>Yes</td>
<td>Partial</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>C</td>
<td>Yes</td>
<td>Partial</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>D</td>
<td>Partial</td>
<td>Partial</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Example: Increased Sharing of Resources

Scientific Working Group on Digital Evidence (SWGDE)
Scientific Working Group on Imaging Technology (SWGIT)
American Academy of Forensic Sciences
High Tech Crime Investigators Association (HTCIA)
International Association of Computer Investigative Specialists (IACIS)
International Association of Chiefs of Police, Sub-committees on Public Private Liaison and Cyber Crime-Digital Evidence
Others...
Example: Increased Sharing of Resources

- [www.cftt.nist.gov/mobile_devices.htm](http://www.cftt.nist.gov/mobile_devices.htm)

CFTT Overview

- CFTT – Computer Forensics Tool Testing Program provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.
- Directed by a steering committee composed of representatives of the law enforcement community.
- The steering committee selects tool categories for investigation and testing by CFTT staff. A vendor may request testing of a tool, however the steering committee makes the decision about which tools to test.
- CFTT is a joint project of: NIJ, OLES, FBI, DoD, Secret Service and other agencies.
Increased Standardization of Devices

- Open Mobile Terminal Platform (OMTP)
  - September 2007 announced Micro USB is future common connector
  - BONDI Initiative addressing the Mobile Platform Fragmentation Problem
Increased Participation

- Get involved in the policy side not just the technical side.
  - Take a position on the NAS Report and its recommendations.
  - Take a position on PI licenses for forensic examiners.
  - Write letters, e-mails, and articles.
  - E.g. Forensic Magazine; International Journal of Digital Evidence, etc.
Thank You...
Questions & Comments