Comprehensive Digital Forensic Solutions

www.paraben.com
Mobile Device Forensic & Security Concerns
Presenter

Amber Schroader  
Chief Executive Officer  
amber@paraben.com

Paraben Corporation  
PO Box 970483  
Orem, UT 84097  
Phone: 801.796.0944  
Fax: 801.796.0610
Are we addicted?
The Best Approach

360° of Digital Forensics

- Support
- Testimony
- Training
- First Responder
- Seizure
- Acquisition

Analysis
Cases
Devices Everywhere

- PDA Devices
- Mobile Phones
- Hybrids
- Ultimate Hybrid
  - Android
  - iPhone
  - Pre
- GPS
- Vehicles
## What is mobile forensics?

<table>
<thead>
<tr>
<th>Computer Forensics</th>
<th>Mobile/Hybrid/PDA Forensics</th>
<th>Ultimate Hybrid Forensics (iPhone, Android, Palm Pre)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Storage device requiring file system</td>
<td>1. Embedded systems</td>
<td>1. Storage device requiring file system*, that depends on chip</td>
</tr>
<tr>
<td>2. Device is “static”</td>
<td>2. Device is “active”</td>
<td>2. Device is “very active” with multiple types of wireless</td>
</tr>
<tr>
<td>3. Larger storage capacity</td>
<td>3. Smaller on board storage capacity</td>
<td>3. Larger storage capacity</td>
</tr>
</tbody>
</table>

---

*File System is a full system that can allow a multi-gig storage device.

---

**What will be out next category?**

---

2009 Copyright Paraben
The First Responder

360° Digital Forensics

- Support
- Testimony
- Training
- First Responder
- Seizure
- Acquisition

Analysis
First Responder Cards

**General Cellular Phone Power/Accessories Reference**

Points of Evidence

- **Additional Multimedia Card/Storage**
- **SIM Card** (Typically located behind battery, DO NOT remove battery)
- **Handset**
- Maintain Power Plug in Mobile Charger

Typical Recovery Data:
- Phonebook, Call Logs, SMS (Text Messages), MMS, Graphics/Pictures, Date book, etc.
- General Pointers - Handle ALL evidence with appropriate equipment (gloves, bags, etc.) Maintain Device in original state.

**Basic Cellular Device Seizure Procedures**

*What is a cellular device:* A mobile communication device including TDMA, CDMA, and GSM that operate at a variety of frequencies.

**ON/OFF RULE**

- **ON**
  - DO NOT turn it off
  - Place in Faraday Bag with battery supply *
- **OFF**
  - Leave device OFF
  - Gather any associated cables, accessories or documentation for device
  - Return to Forensic Lab for evaluation by trained professional

Be sure to maintain your own personal safety at all times and make sure appropriate legal documents have been obtained.

*A Faraday Bag (Paraben's Strong-Hold Bag) will block the wireless signals that are being pushed to the device that can potentially change or harm your evidence.*

www.paraben.com
First Responder Cards

General PDA/Hybrid Power/Accessories Reference

Maintain Power
PDA devices are older style handhelds that require power to be able to maintain their data.

Hybrid devices are a mix of a mobile phone and a PDA device, some of these devices require power to maintain data and they all need to be treated as a live wireless device.

Basic PDA/Hybrid Device Seizure Procedures

Hybrid and PDA devices can be seized with the basic rules of maintaining power, and the best practice would be to block the potential wireless signal to the device.

ON/ OFF RULE

ON
DO NOT turn it off
Maintain power on device
NO POWER
NO DATA

OFF
If device is off or in sleep mode, leave device alone

SLEEP MODE
Gather any associated cables, accessories or documentation for device
Place Device in Faraday Device

Return to Forensic Lab for evaluation by trained professional

Be sure to maintain your own personal safety at all times and make sure appropriate legal documents have been obtained.

A Faraday Bag (Paraben’s Strong-Hold Bag) should be used with wireless devices like RIM Black-Berries or PDA/Phones to block wireless signals to preserve data.

www.paraben.com

2009 Copyright Paraben
First Responder Cards

General GPS Power/Accessories Reference

What is a GPS device: A mobile device that uses satellite trilateration via radio waves to provide a user their exact global location.

GPS: Global Positioning System

Basic GPS (Global Positioning System) Seizure Procedures

TURN OFF RULE

Turn Device off to cut satellite communication and preserve evidence integrity.

ON
- Turn Device Off

OFF
- Leave device OFF
- Place in Faraday Bag with battery supply
- Gather any associated cables, accessories or documentation for device
- Return to Forensic Lab for evaluation by trained professional
- Be sure to maintain your own personal safety at all times and make sure appropriate legal documents have been obtained.

Optional Seizure Tool
A Faraday Bag (Paraben's StrongHold Bag) will block the wireless signals that are being pushed to the device that can potentially change or harm your evidence.

www.paraben.com
First Responder Rules

1. Teach/Learn about the evidence
2. Bridge communication gap
3. Follow up with training
The Seizure

360° Digital Forensics

Support
Testimony
Training
First Responder

Seizure
Analysis
Acquisition
Second Degree: Seizure

• Maintain the best evidence
  – Seizure rules based on type of device

• It will not always go smoothly
  – Prepare for the worst

• Think outside the box
  – Look for all options for the mobile accessories
    think creative
Second Degree: Seizure

- Risks to Evidence
  - Wireless Communication
  - Power Supply Issues
  - No Legal Paperwork
  - No Training
Faraday Example

Paraben StrongHold Bag
Acquisition Tools

Are they forensic?

- BitPim
- .XRY
- Cellebrite
- Oxygen
- BK Forensics
- Neutrino
- SecureView
- Final Data
- Flasher Boxes
- MobilEdit!
- CSI Stick
- Device Seizure

2009 Copyright Paraben
What makes a good Mobile Forensic Tool?

• Is it read only?
  – Yes
  – No
• Can I repeat my results?
  – What are your validation steps?
  – Paraben Validator (Free Tool in 2010)
• Is the data verified and if so how?
  – What hash values are used?
  – Can those values be repeated?
  – Are there other validations?
• Was it designed for forensics, and are the images gathered valid?
  – Is it a commercial tool that is being used in forensics?
  – How is the image file created?
Do I need to change my techniques to find this data?

- Traditional Mobile Phone Techniques Work
  - Seize
  - Acquire
  - Analyze
- Follow Procedures for Seizure that are Generic
  - Simple Charts
- Document your Procedures by Device Type
  - SOP Seizure
  - SOP Acquisition
  - SOP Analysis
- Make sure you Update Procedures Regularly
  - Once a Quarter or if tools update so do you
Fourth Degree: Analysis

- What are your expectations of the data?
  - How much should I get?
- Do you know what to look for?
  - Where is the user data stored?
  - PROPRIETARY DATA
    - Must be parsed before analysis
Fourth Degree: Analysis

• Where is all the data?
  – Handset
  – SIM Card
  – Media Cards
  – Offsite Storage/Synchronization
  – Desktop
    • iTunes Backup
    • BlackBerry IPD
  – Provider
Data is not always on the Device

- Desktop Synchronizations
  - Example: iPhone
Available Data on a GPS Device

- All Logical GPS Points (Waypoints)
  - Issue with proof…
- Latitude, Longitude, Altitude
- Notes
- Time Stamps
  - Clocks UTC
Getting Trained

360° Digital Forensics

- Support
- Testimony
- Training
- First Responder
- Seizure
- Analysis
- Acquisition

2009 Copyright Paraben
Fifth Degree: Training

• Know what you are doing
• Learn the systems
• How do they store data
• Attend for more than a how to but a why
  – Paraben Certified Mobile Examiner

“Do or Do Not There is No Try.”
--Yoda
Giving Testimony

360° Digital Forensics

Support
Testimony
Training

First Responder

Seizure
Analysis
Acquisition

2009 Copyright Paraben
Sixth Degree: Testimony

- Can you answer the questions?
  - Global knowledge of systems and procedures
  - Do you have a set process?
- Are you certified?
  - What are the terms of your certification?
- What do you do to stay current?
  - Conferences
  - Training
  - Continuing Education
Receiving Support

360° Digital Forensics

- Support
- Testimony
- Training

- First Responder
- Seizure
- Acquisition

Analysis
Seventh Degree: Support

• COMMUNICATION
• Is the company there for you?
• Does the tool support model issues?
  – Logging
  – Support of drivers from manufacturers
Can a Handheld Device be SECURE?
Questions You Should Ask?

• What do you do for mobiles in infrastructure?
  – Run!

• How do you secure them?
  – Third Party
  – Home grown

• What risks exist that can cost you your data?
  – Virus
  – Theft
BlackBerry Security: Positive Points

• “Triple DES” Encryption
• Authentication for transfer of data
• E-mail is always secure
BlackBerry Security: Negative Points

- “Triple DES” Encryption
  - NO BREAK
- Authentication for transfer of data
  - NO Way to Gain Access in Transit
- E-mail is always secure
  - Employees can easily pass data
Windows CE Security: Positive Points

- Mobile no work around for password
- Lots of third party choices for applications
- Integration into Windows
Windows CE Security: Negative Points

• Mobile no “public” work around for password
• Lots of third party choices for applications
• Integration into Windows
  – Microsoft is NOT the most popular company = VIRUS ISSUES
Other Ultimate Hybrids
Moving to The Enterprise
Forensic Training for Everyone
To learn more about mobile forensics you can attend Paraben’s Annual PFIC Conference Nov 8-11 in Park City, Utah

www.pfic2009.com

$199.00 to Attend for 3 Days of Training
The Future is NOW
New Innovations

SEQUALS CAN BE BETTER!

Paraben’s CSi Stick® GEN 2

More Speed
More Devices
More Muscle

The ONLY Mobile Forensic Solution
Coming Early 2010
www.csistick.com
Choose data to acquire:

- Acquire text data only
- Acquire all data

Nokia

Choose another device  Cancel
Please email the speaker or provide a business card for FREE First Responder Cards or a copy of the presentation.