



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



Cases



Devices Everywhere

- PDA Devices
- Mobile Phones
- Hybrids
- Ultimate Hybrid
 - Android –iPhone -Pre
- GPS
- Vehicles



What is mobile forensics?

Computer Forensics

1. Storage device requiring file system
2. Device is “static”
3. Larger storage capacity
4. Forensic:
Bit Stream
Imaging

Mobile/Hybrid/PDA Forensics

1. Embedded systems
2. Device is “active”
3. Smaller on board storage capacity
4. Forensic:
Active Memory
Imaging

Ultimate Hybrid Forensics

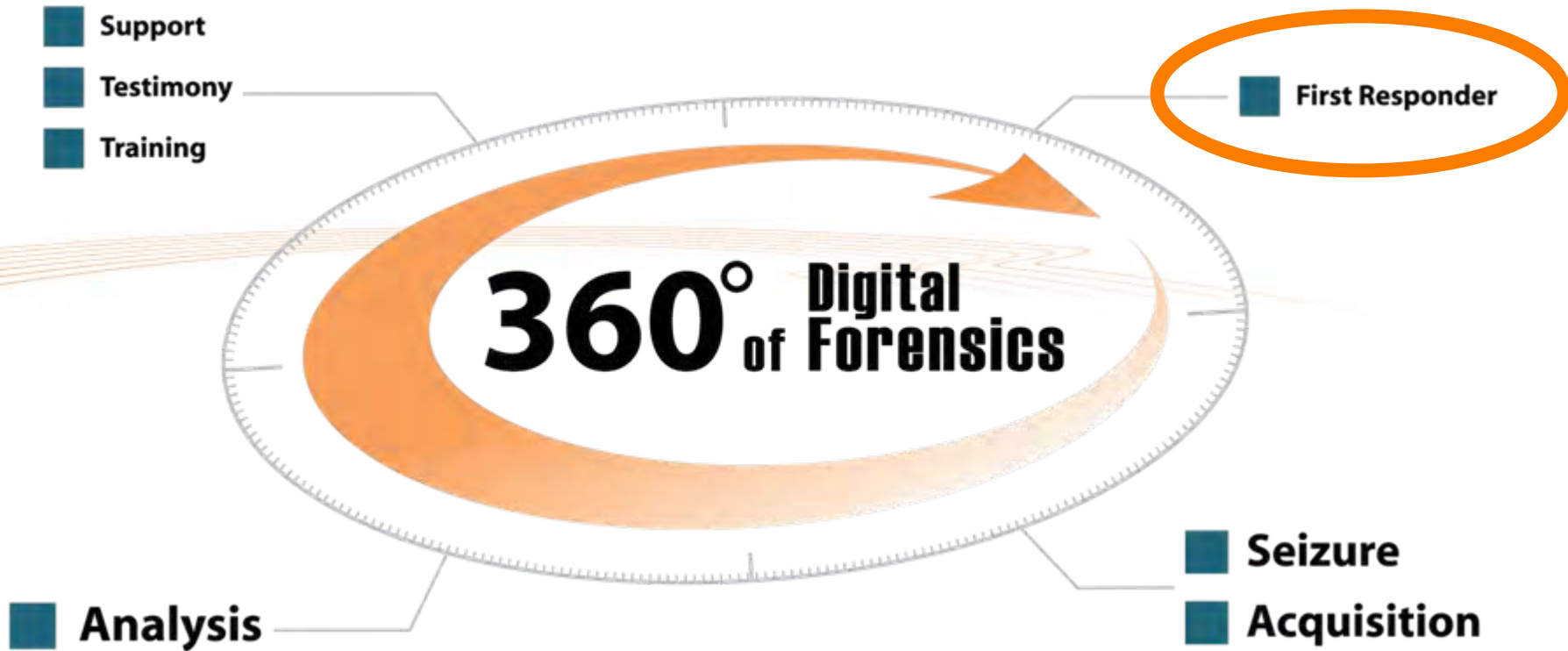
iPhone, Android, Palm Pre

1. Storage device requiring file system*, that depends on chip
2. Device is “very active” with multiple types of wireless
3. Larger storage capacity
4. Forensic:
Bit Stream Memory
Image (Typical)

What will be out next category?

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

The First Responder



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

```
graph TD
    ON_OFF[ON/OFF] -- ON --> DO_NOT[DO NOT turn it off]
    ON_OFF -- OFF --> LEAVE[Leave device OFF]
    DO_NOT --> FARADAY[Place in Faraday Bag with battery supply *]
    LEAVE --> GATHER[Gather any associated cables, accessories or documentation for device]
    FARADAY --> LAB[Return to Forensic Lab for evaluation by trained professional]
    GATHER --> LAB
    ON_OFF --> SAFETY[Be sure to maintain your own personal safety at all times and make sure appropriate legal documents have been obtained.]
```

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

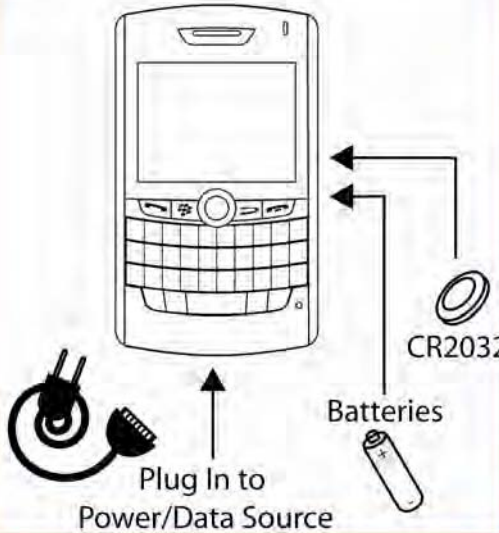
First Responder Cards

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.



Plug In to Power/Data Source

CR2032

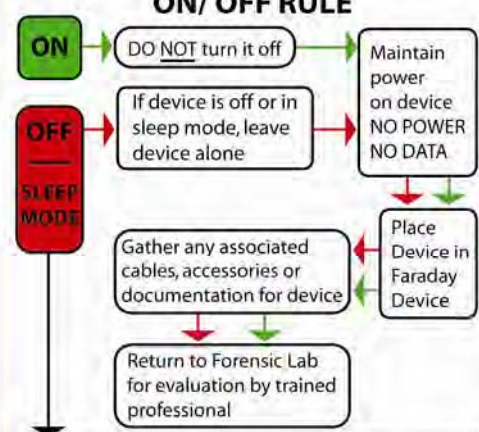
Batteries

First Responder Series

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 → Place Device in Faraday Device

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

Gather any associated cables, accessories or documentation for device → Return to Forensic Lab for evaluation by trained professional

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.

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

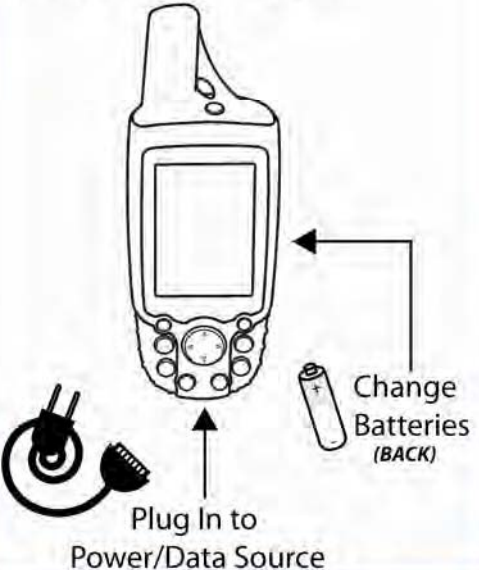
First Responder Series

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



Plug In to Power/Data Source

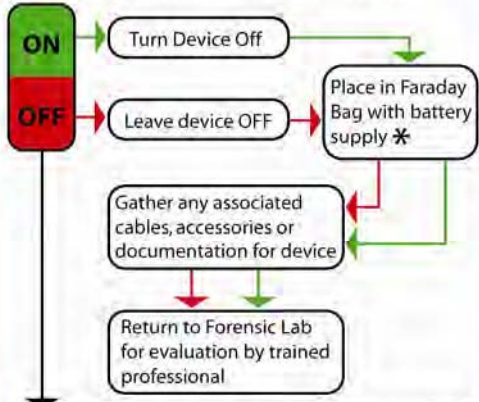
Change Batteries (BACK)

First Responder Series

Basic GPS (Global Positioning System) Seizure Procedures

TURN OFF RULE

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



```
graph TD; ON[ON] --> TurnOff[Turn Device Off]; OFF[OFF] --> LeaveOff[Leave device OFF]; TurnOff --> Faraday[Place in Faraday Bag with battery supply *]; LeaveOff --> Faraday; Faraday --> Gather[Gather any associated cables, accessories or documentation for device]; Gather --> Lab[Return to Forensic Lab for evaluation by trained professional]; ON --> Lab; OFF --> Lab;
```

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

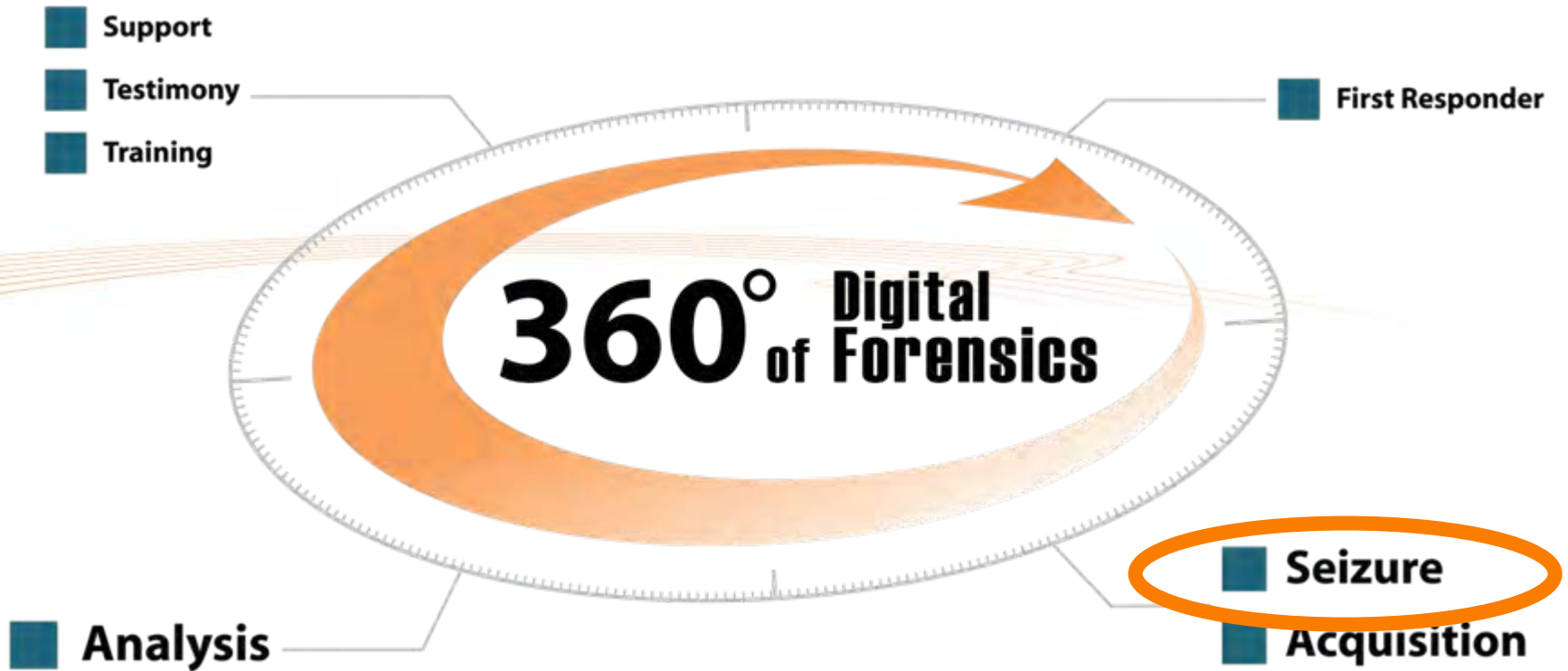
First Responder Series

First Responder Rules

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



The Seizure

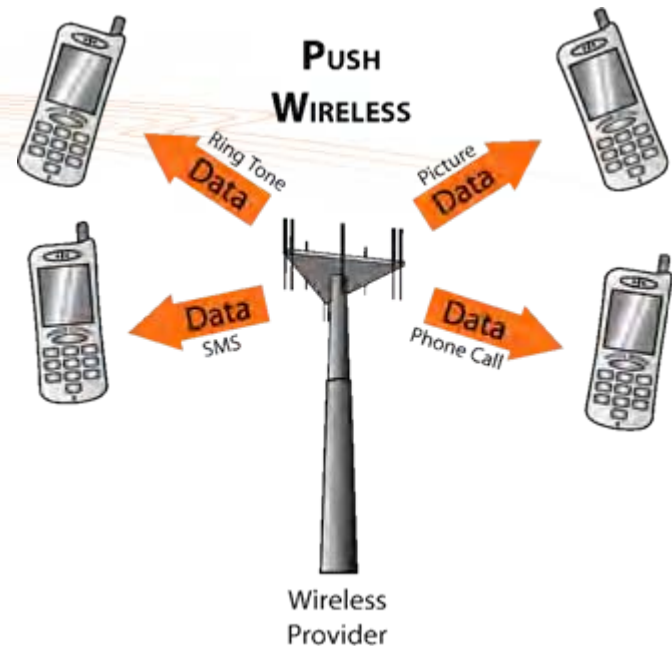


Second Degree: Seizure

- 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

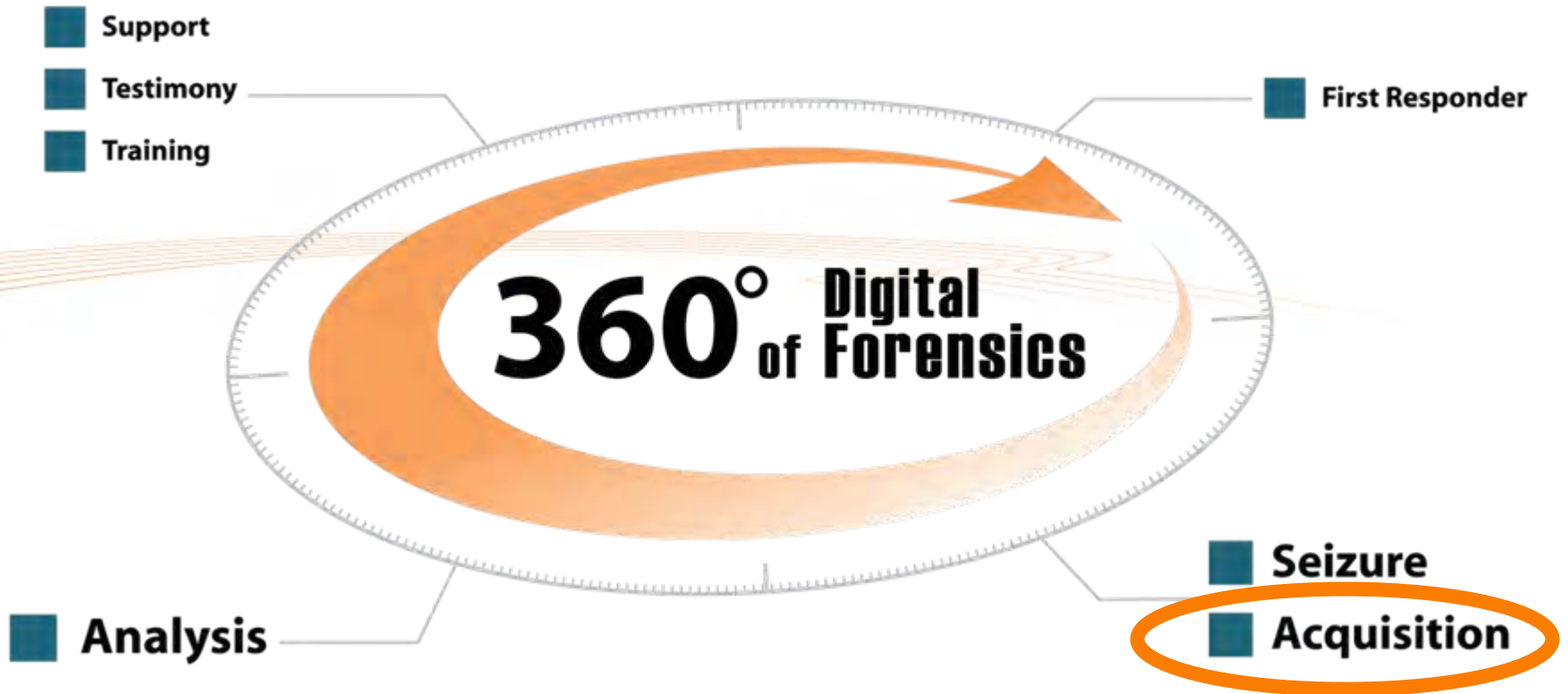


Faraday Example



Paraben StrongHold Bag

The Acquisition



Acquisition Tools

Are they forensic?

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

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?**

The Analysis

■ Support

■ Testimony

■ Training

■ First Responder

360° of Digital Forensics

■ Seizure

■ Acquisition

■ Analysis

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

Name	Size	Type	Date Modified
0b1fe6f87c054ebb6d00cfa6b6acd343a7f...	14 KB	MDBACKUP File	3/8/2008 12:04 PM
0cc4f6ba3f9ea2cfd03eedf5c435743d330...	1 KB	MDBACKUP File	3/7/2008 12:58 AM
2dc93f7fe22197e0a8735b2da05806cd199...	27 KB	MDBACKUP File	3/8/2008 12:04 PM
4d817d876031e5fa2166aa2cc84c257a41...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
5bbcc8473f10984d4f8778b092f4dfb39de...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
6ba2c420da4bbfe39511345a9d82114de8...	2 KB	MDBACKUP File	3/8/2008 12:04 PM
6be4a1f28c9c1e496eddafee86f20ac1454...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
06f1e2751da492eef0741f55555dfa36572...	2 KB	MDBACKUP File	3/8/2008 12:04 PM
7df5971cdb662bdd1409a4c6c1e92e582d...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
07e177bf07c599ea0b6b849f7e71c746ec3...	5 KB	MDBACKUP File	3/8/2008 12:04 PM
8b91e0430a206d42828119da8aad3794e3...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
9f87f716e233d830d775bbe0358c7700f18...	1 KB	MDBACKUP File	3/8/2008 12:50 PM
14ee8cdc3e6e0220399ff210246e1c92b7d...	49 KB	MDBACKUP File	3/8/2008 12:50 PM
37d63b7039815a7aad2ca5ac6807c33376...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
41b7f659d75018a57319fc8be8d66bb423c...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
41cee1eef3f1affc045d6a08dea0865246c...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
44b6749460d357453814172e4db4b30782...	2 KB	MDBACKUP File	3/8/2008 12:04 PM
54a6608b488dc370b2e5a9a2b61235f198...	2 KB	MDBACKUP File	3/8/2008 12:04 PM
65db4f72943b9946b187b6e71555e7616f...	1 KB	MDBACKUP File	3/8/2008 12:50 PM
312c96d34056816a37a0340d4b2bcd0b7b...	1 KB	MDBACKUP File	3/7/2008 12:58 AM
527b22aa9691deefc8a8853052f1b42c147...	1 KB	MDBACKUP File	3/7/2008 12:58 AM
676af23ccebcce55479a65978bf04689e1fc...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
2420ebf4608b21593afd765132f17019951...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
a49bfab36504be1bf563c1d1813b05efd60...	11 KB	MDBACKUP File	3/8/2008 12:50 PM
adb8c77534444e97c31ff15924d50f3ed1f...	52 KB	MDBACKUP File	3/8/2008 12:50 PM
af3d1a9068086e7aa99626f1f4e62fd97a9...	1 KB	MDBACKUP File	3/7/2008 12:58 AM
b2e1bd7f19028524e59e887ff8d3975391d...	1 KB	MDBACKUP File	3/8/2008 12:50 PM
b2e877bcf4d3a42663cd2faa8cb8f93bbc...	1 KB	MDBACKUP File	3/7/2008 12:58 AM
be71679a4167272085a3f99924e97c9a1...	1 KB	MDBACKUP File	3/7/2008 12:58 AM
c3fdd5afb9fe84e83ad126fbc41435c09e0...	1 KB	MDBACKUP File	3/7/2008 12:58 AM
c5ac8af87a3850c95f4fecb7f118128d699c...	2 KB	MDBACKUP File	3/8/2008 12:04 PM
c22fa6d0608745dcbeda1b7f98869857ccd...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
d21bbf8c16844dc975d0c0ee9db42dbe8a...	3 KB	MDBACKUP File	3/8/2008 12:04 PM
e96874516f16021830335f15e1150b9bd1...	1 KB	MDBACKUP File	3/7/2008 12:58 AM
ea0f2402c60cf95f64746397c13c0c8a1b8...	282 KB	MDBACKUP File	3/7/2008 12:58 AM
eab4244681224785cbd17caa07a4718299...	1 KB	MDBACKUP File	3/8/2008 12:04 PM
fe593c5f143b9f519970844edbccb8eb702...	2 KB	MDBACKUP File	3/8/2008 12:04 PM
Info.plist	14 KB	QuickTime Preferences	3/8/2008 12:50 PM
Manifest.plist	6 KB	QuickTime Preferences	3/8/2008 12:50 PM

Available Data on a GPS Device

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

Search

Fly To Find Businesses Directions

e.g., Hotels near JFK

Search input field with magnifying glass icon

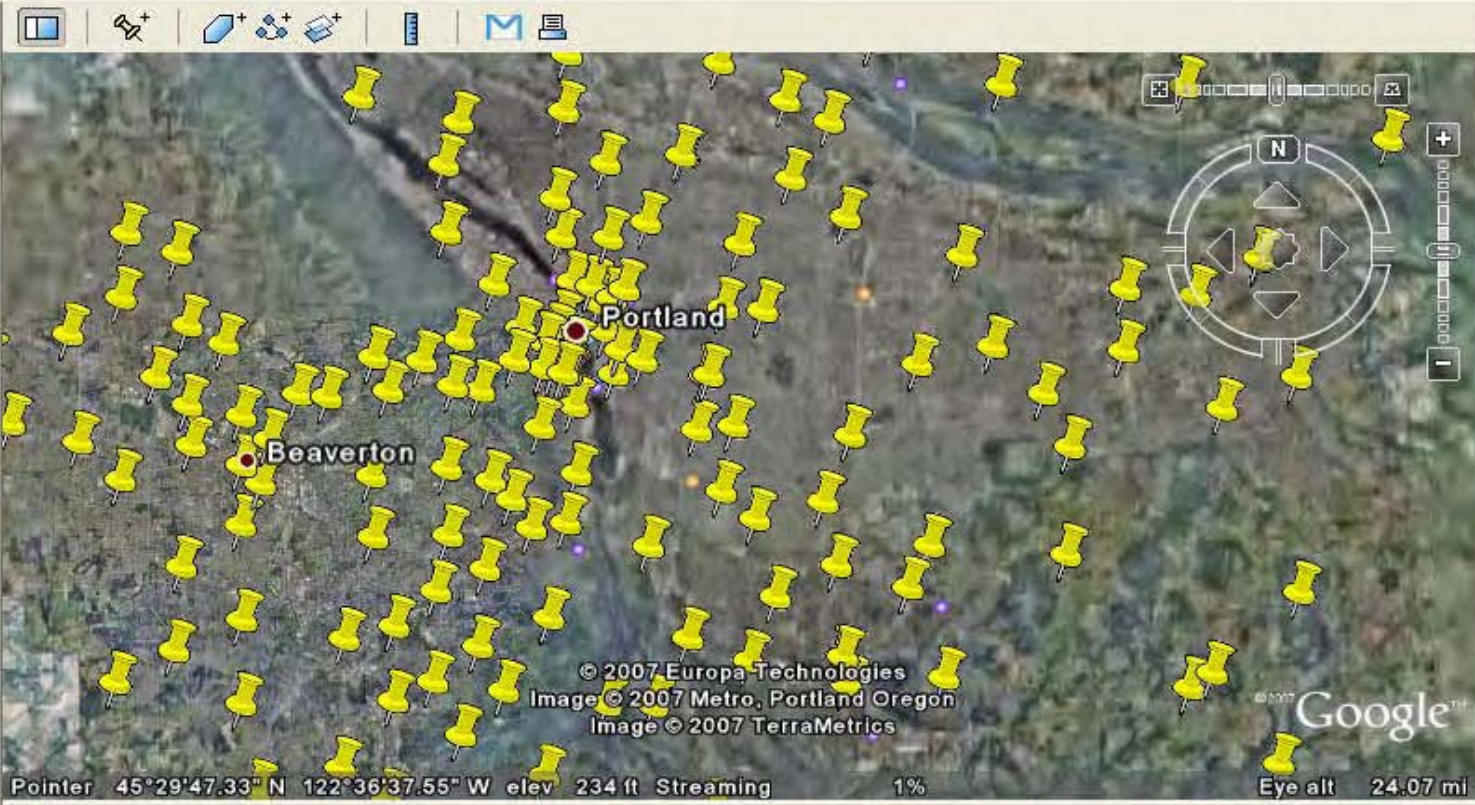
Places

- [no name], OR, Portland OR, ... PTLDORPG23, 6940 SW
- [no name], OR, Portland OR, ... PTLDORPG33, 1122 NW
- [no name], OR, Portland OR, ... PTLDORPG33, 1122 NW
- [no name], OR, Portland OR, ... PTLDORPG33, 1122 NW
- [no name], OR, Portland OR, ... PTLDORPG33, 1122 NW
- [no name], OR, Portland OR, ... PTLDORPG33, 1122 NW

Layers

View: Core

- Primary Database
- Terrain
- Geographic Web
- Featured Content
- Global Awareness
- roads
- 3D Buildings
- borders
- Populated Places



URL: http://www.google.com/

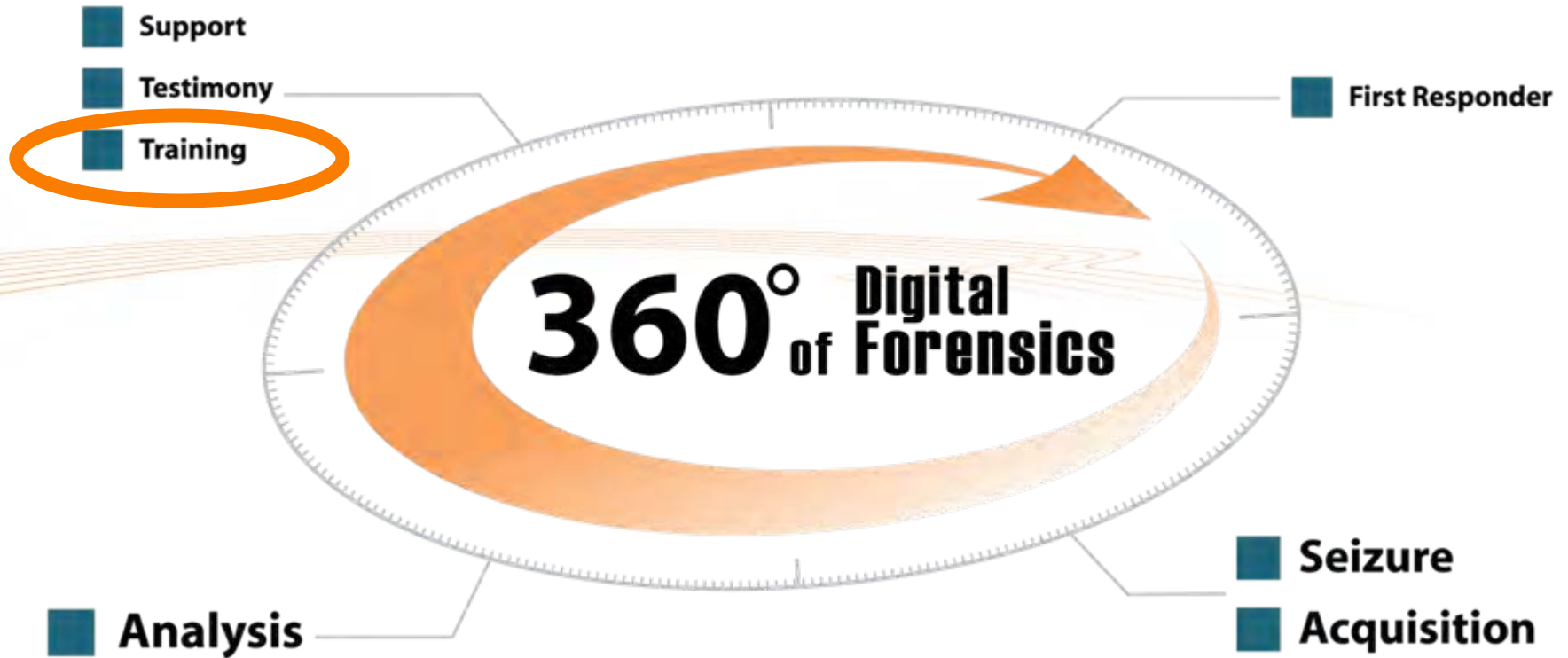
Web Images Video News Maps Gmail more iGoogle | Sign in



Google Search and I'm Feeling Lucky buttons



Getting Trained



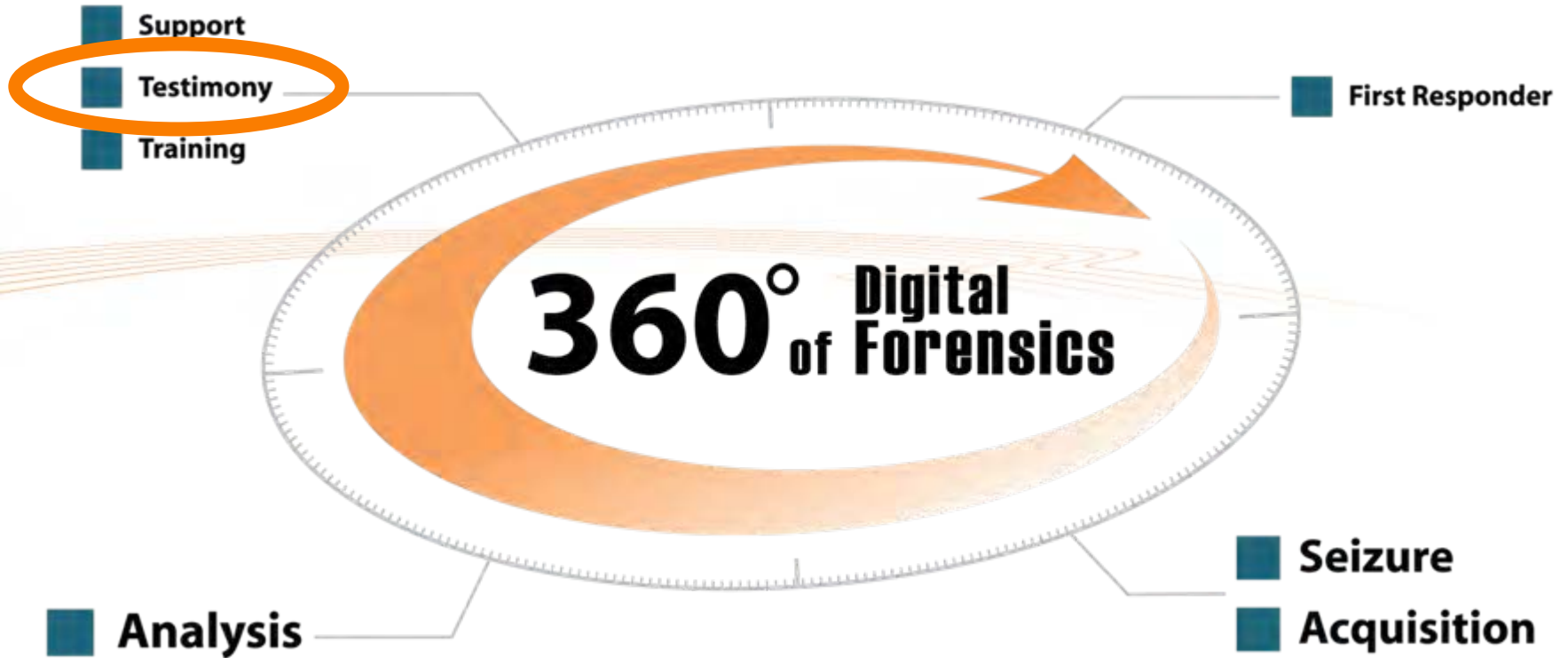
Fifth Degree: Training

- 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

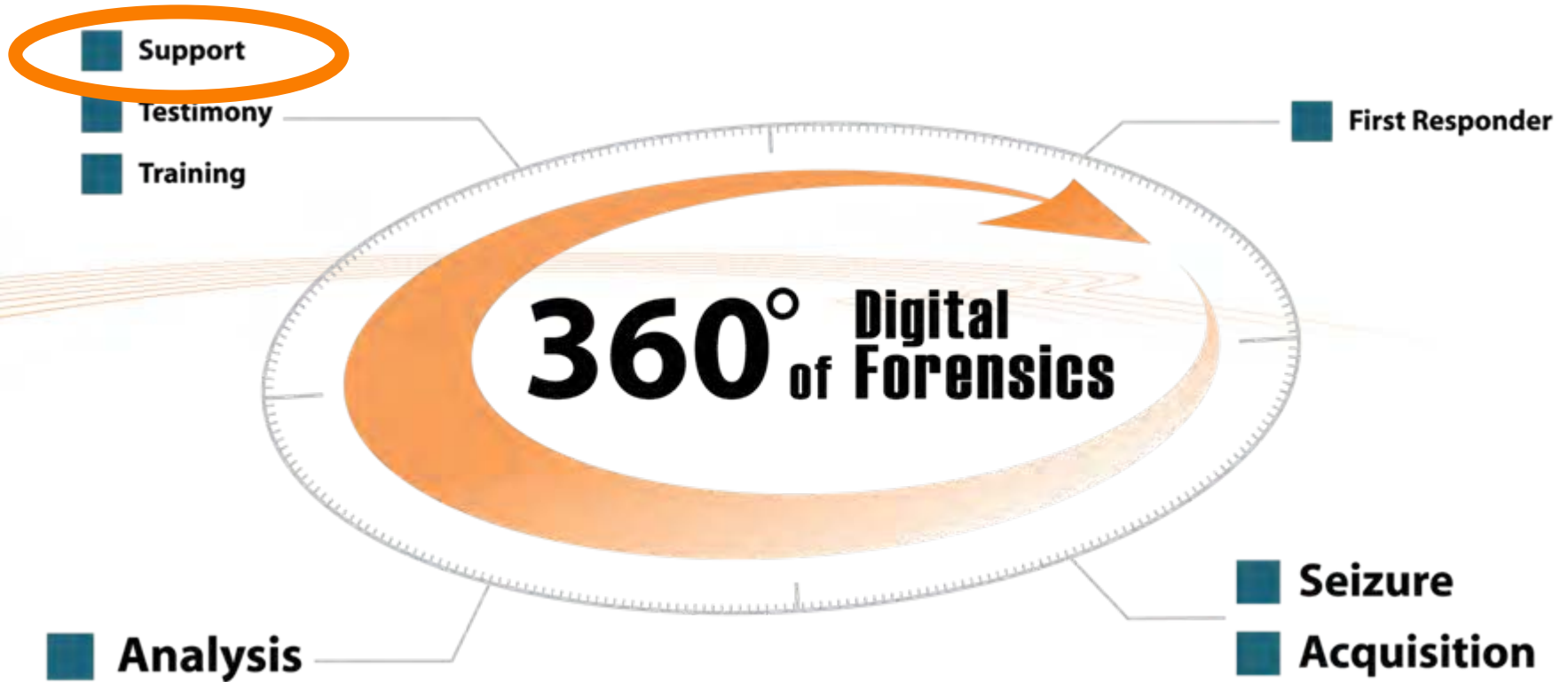
Giving Testimony



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



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?

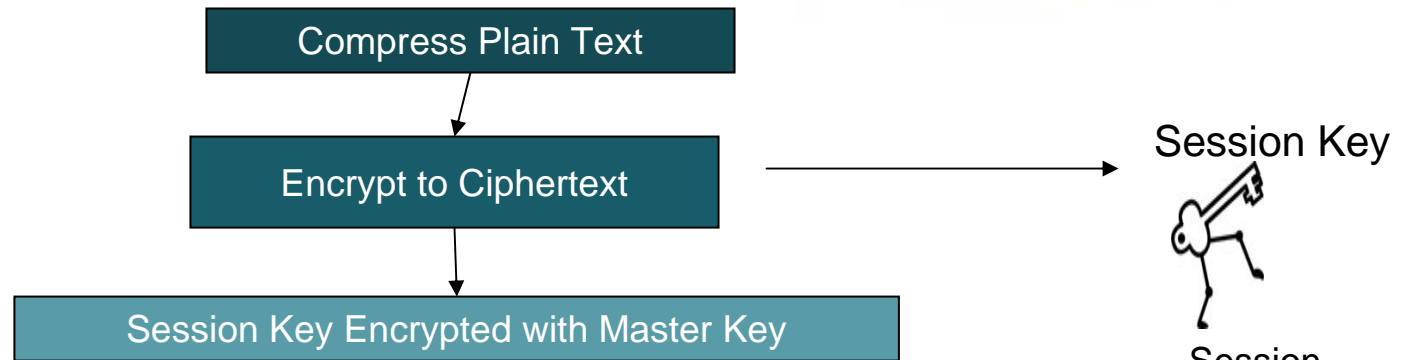
- What do you do for mobiles in infrastructure?
 - Run!
- How do you secure them?
 - Third Party
 - Home grown
- What risks exist that can cost you your data?
 - Virus
 - Theft



SHOW ME

BlackBerry Security: Positive Points

- “Triple DES” Encryption
- Authentication for transfer of data



Session key is random for each message.

- E-mail is always secure

BlackBerry Security: Negative Points

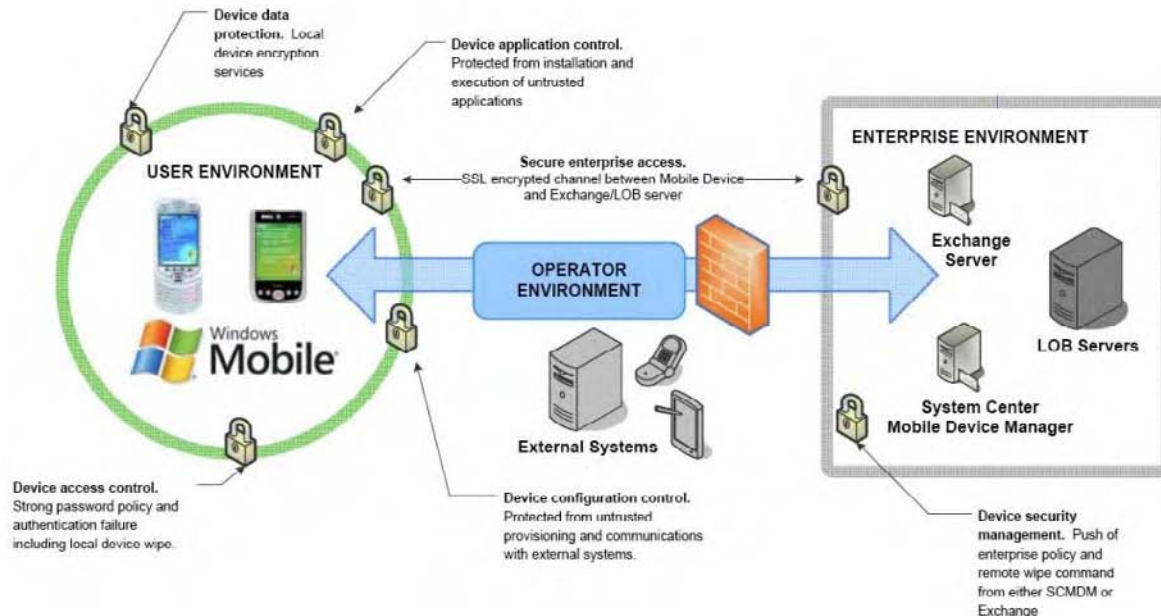
- “Triple DES” Encryption
 - NO BREAK
- Authentication for transfer of data
 - NO Way to Gain Access in Transit
- E-mail is always secure
 - Employees can easily pass data



WM 6.0,
I don't love you anymore

Windows CE Security: Positive Points

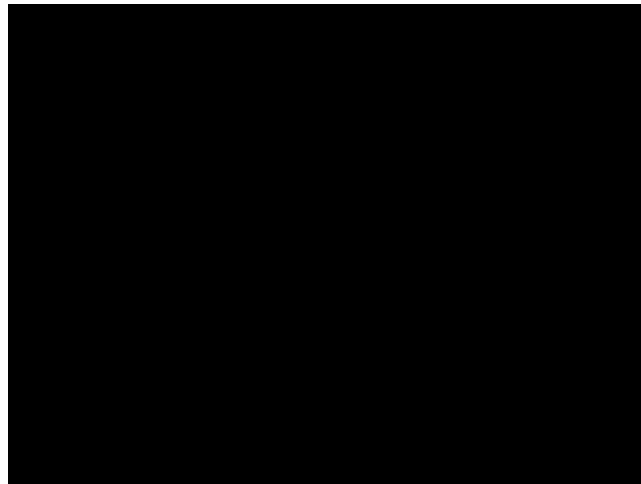
- Mobile no work around for password
- Lots of third party choices for applications
- Integration into Windows



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

PFIC



Paraben's Forensic Innovations Conference

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**

SEQUALS CAN BE BETTER!

New
Innovations



More Speed
More Devices
More Muscle

The ONLY Mobile Forensic Solution

Coming Early 2010
www.csistick.com



← Main Page

Choose data to acquire:



Nokia

Acquire text data only

Acquire all data

Choose another device

Cancel



← Main Page

Acquired Data



SMS History



Graphics



Phonebook

Data Seized From:



SAMSUNG CDMA

View Details

View Bookmarks



w_fox_bikeposter_1280x1024.png



w_fox_bikeposter_800x600.png



w_1280_1024_talas.png



w_1280_1024_40.png



w_1280_1024_vanilla.png



w_1280_1024_float.png



Loaded: (13 Items)

Amber Schroader

Chief Executive Officer

amber@paraben.com

Paraben Corporation

PO Box 970483

Orem, UT 84097

Phone: 801.796.0944

Fax: 801.796.0610



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