



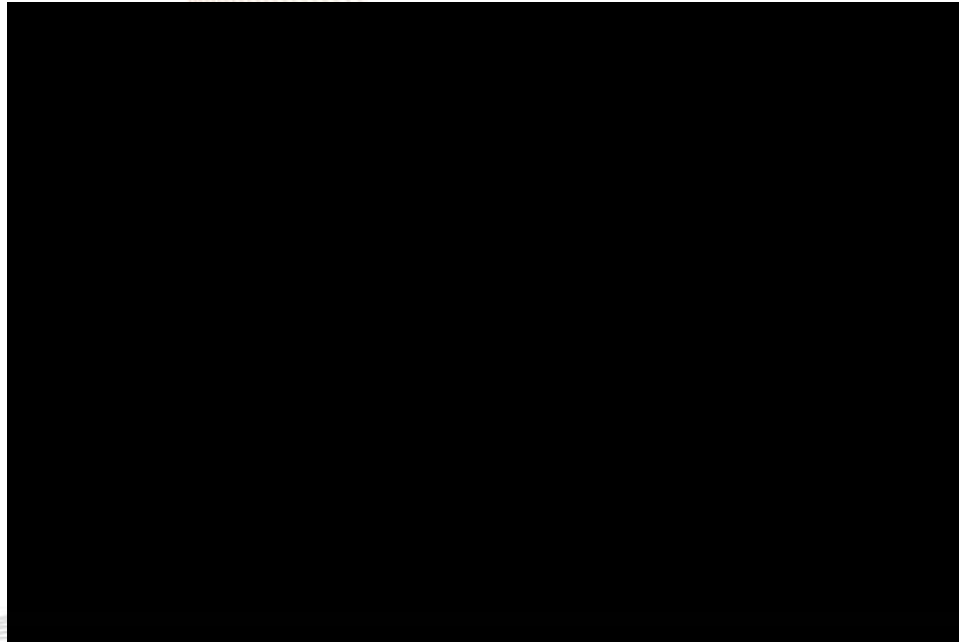
Mobile Devices Gathering Information and Protecting Organizations

Amber Schroeder, Paraben Corp.

Speaker Introduction

- Amber Schroader, CEO Paraben Corporation
- 20+ years in digital forensics
- Active investigator
- Good sense of humor
- Always learning...never an expert.

Perspective



What are the concerns of mobile devices of today?

- How much data can the device hold?
- Do you gain access to all the data?
- Do I need to change my techniques to get this data?
 - What is the largest risk to my evidence?
 - How long with acquisitions take?
- What is the latest security concerns for mobile devices?
 - Virus Issues
 - Spyware?

Trend 1. Storage

How Much Data Can It Hold?



32 Gig+
Internal User Storage



1 Gig
Internal User Storage



100 Meg
Internal User Storage



48 Meg
Internal User Storage



16 Meg
Internal User Storage

How to gather potential Evidence...

Compliments of Paraben Corporation

Special Promotional Edition

First Responder Guide to Mobile Forensics

Learn:

- Basic Guidelines for Dealing with Mobiles
- How to Seize a Mobile Phone
- Where Data Resides for your Investigation



By: Amber Schroader

Trend 2. Accessories

- Encryption keys
- Additional Storage





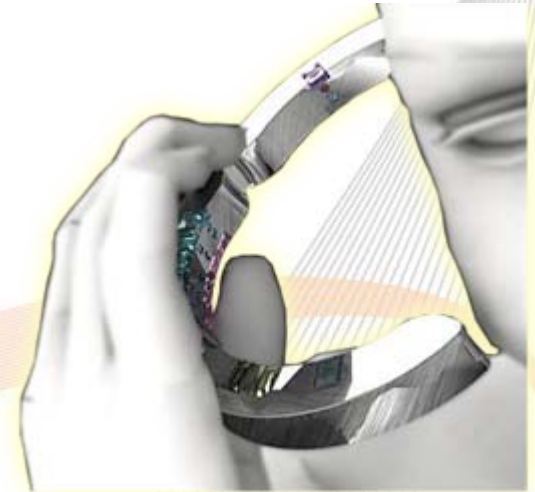
7. HiPhone

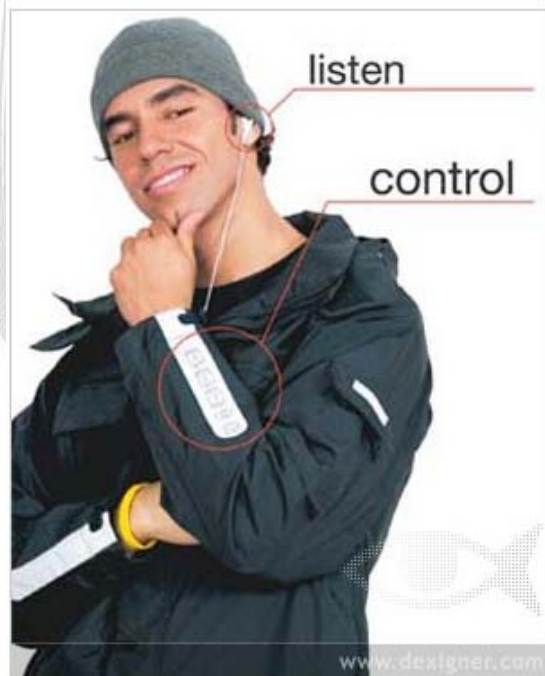
HiPhone is powered by [Windows Mobile 6.0](#) and has a GUI that 100% resembles the GUI of the original iPhone. Moreover it is even branded with a flipped Apple logo.

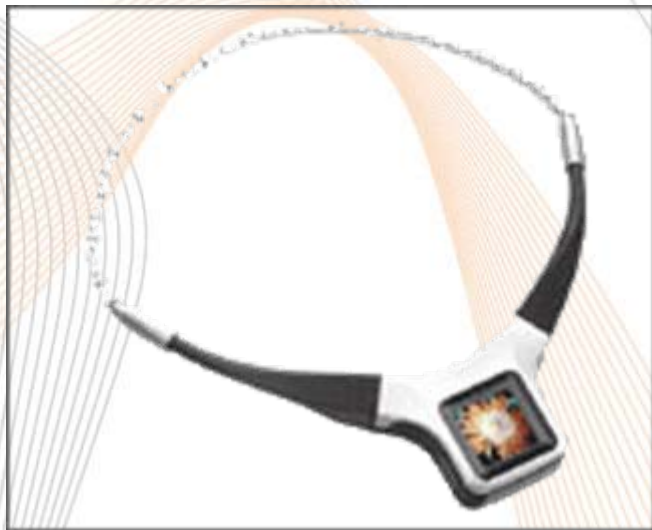


Pi

is what we call an ultimate iPhone clone. This phone imitates the Apple iPhone + and runs on an open-source platform thus giving away the freedom of installing third party applications and also supports 3G [wireless](#).









Trend 3. All About Signals



PUSH WIRELESS



Ring Tone
Data



Picture
Data



Data
SMS



Wireless
Provider

Data
Phone Call



Faraday Technology



Trend 4.

Consultants Geeking it up...

- Ask about certifications
- Ask about procedures
- Ask about training
- Don't trust learn the basics yourself.



Do you gain access to the data when you image the device?

- What is a physical image?
 - Hard Drive
 - Bit stream image of the device.
 - Mobile Phone
 - Physical acquisition of the memory storage on the device.
 - How often is that possible with Mobile Phones?
 - 40% of Phones Device Seizure can do Physical Images

How long is an acquisition?

- Average Processing Time
 - PDA
 - 30 Minutes
 - Hybrid
 - 15 Minutes to 1.5 Hours
 - Uber Device
 - 5 Hours Plus
 - Mobile
 - 25 Minutes
- Prioritize Your Exam
 - Mobile First
 - Hard Drive Second

Cell Phone

- Typically consumers can get:
 - Phonebook
 - Call Logs
 - SMS/MMS
 - Pictures
 - Videos
- Typically **Forensics** can get:
 - Phonebook
 - Call Logs (Including Deleted)
 - SMS/MMS (Including Deleted)
 - Pictures (Including Deleted)
 - Videos (Including Deleted)
 - File System (Shows spyware)



SHOW ME

Hybrid

- Typically consumers can get:
 - Phonebook
 - Call Logs
 - SMS/MMS
 - Pictures
 - Videos
- Typically **Forensics** can get:
 - Phonebook
 - Call Logs (Including Deleted)
 - SMS/MMS (Including Deleted)
 - Pictures (Including Deleted)
 - Videos (Including Deleted)
 - File System (Shows spyware)
 - Registry
 - Instant Messaging
 - Email (Including Deleted)



SHOW ME

Ultimate Hybrid

- Typically consumers can get:
 - Phonebook
 - Call Logs
 - SMS/MMS
 - Pictures
 - Videos
- Typically **Forensics** can get:
 - Phonebook
 - Call Logs (Including Deleted)
 - SMS/MMS (Including Deleted)
 - Pictures (Including Deleted)
 - Videos (Including Deleted)
 - File System (Shows spyware)
 - Registry
 - Instant Messaging
 - Email (Including Deleted)
 - Backup Records (lots of deleted)
 - Web Surfing History



SHOW ME

GPS

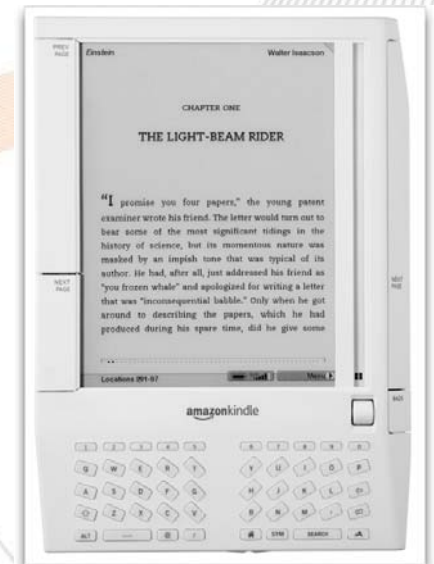
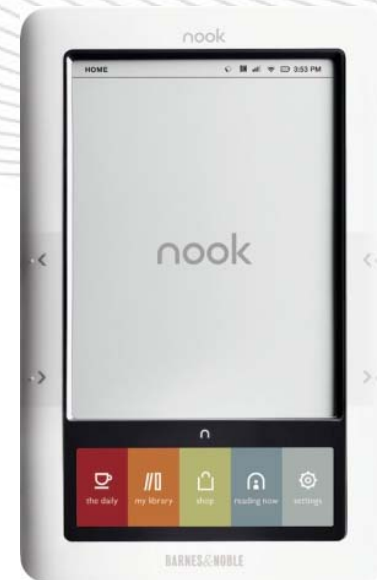
- Typically consumers can get:
 - Recently Visited
 - Home
 - Favorites
- Typically **Forensics** can get:
 - Recently Visited
 - Home
 - Favorites
 - All Tracks (Including some deleted)
 - All Waypoints (Including some deleted)
 - Date and Time Stamps
 - Synronization Data with Mobile Phone
 - Phonebook
 - SMS
 - Call Logs

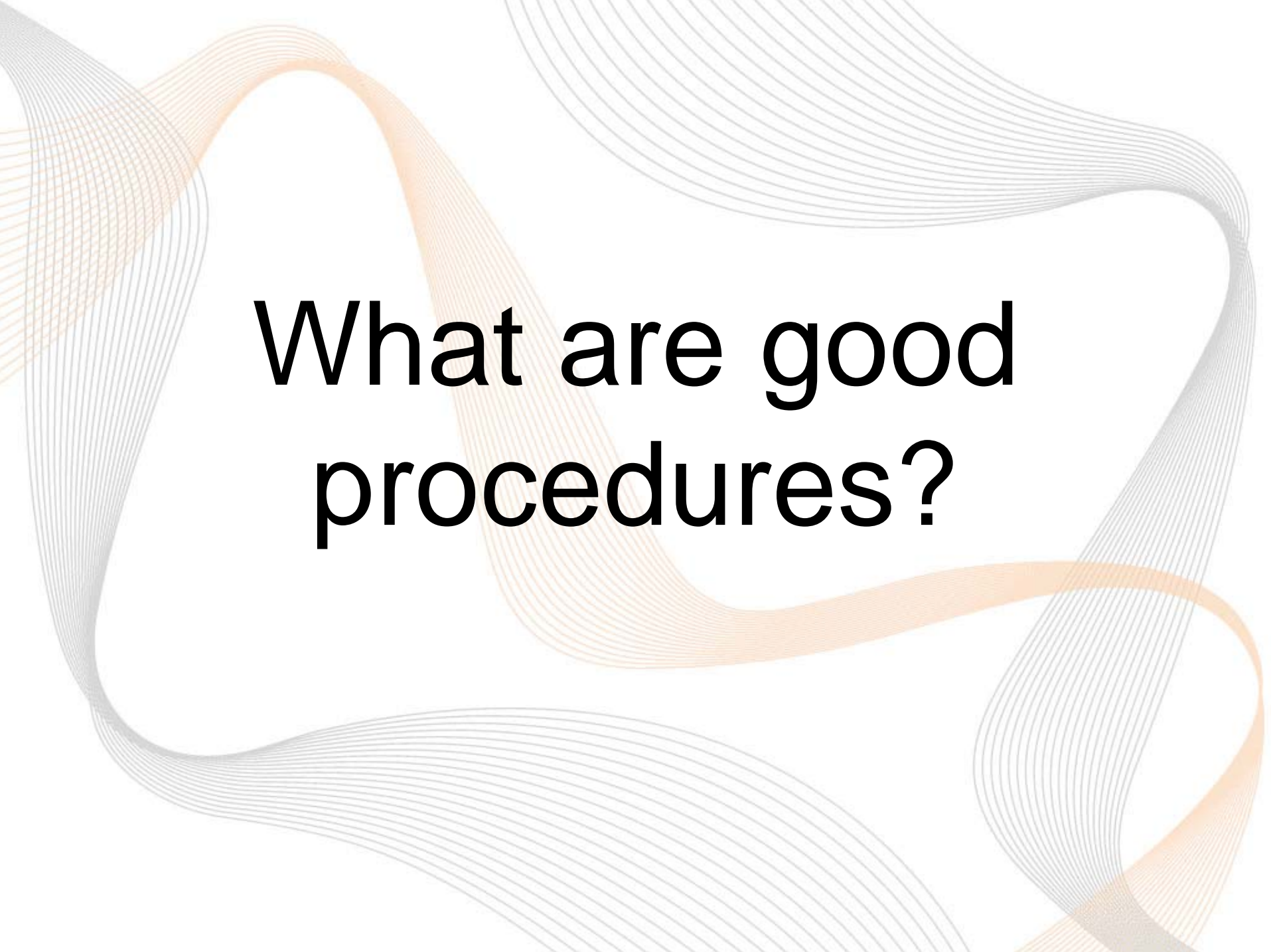


SHOW ME

eReader

- Typically consumers can get:
 - Downloads
 - MP3
 - Pictures
- Typically **Forensics** can get:
 - Downloads
 - MP3
 - Pictures
 - Non Active Files
 - Physical Images of Device

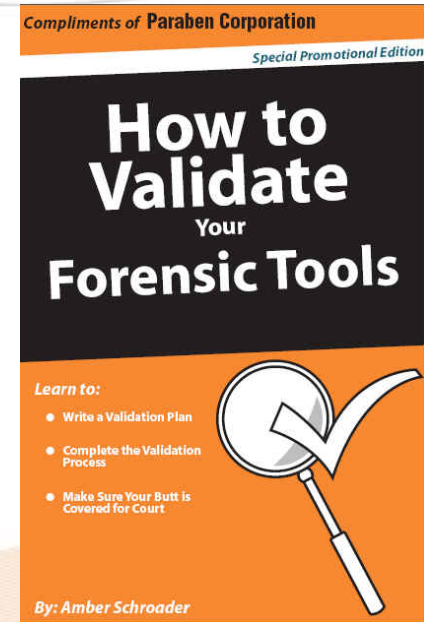


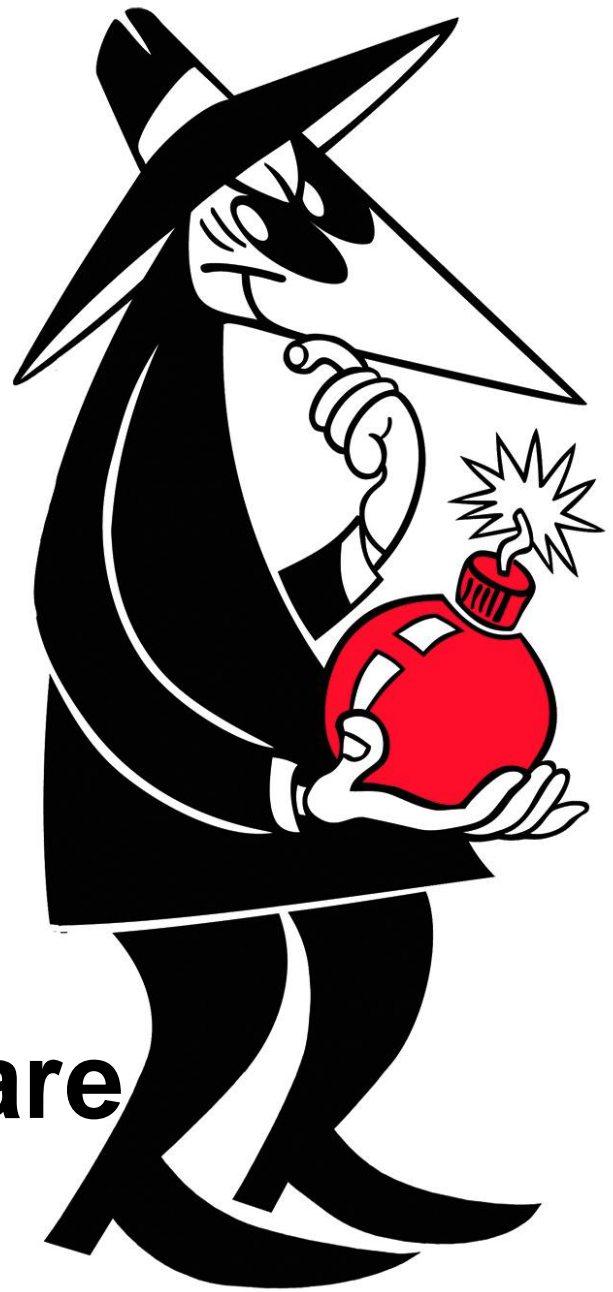
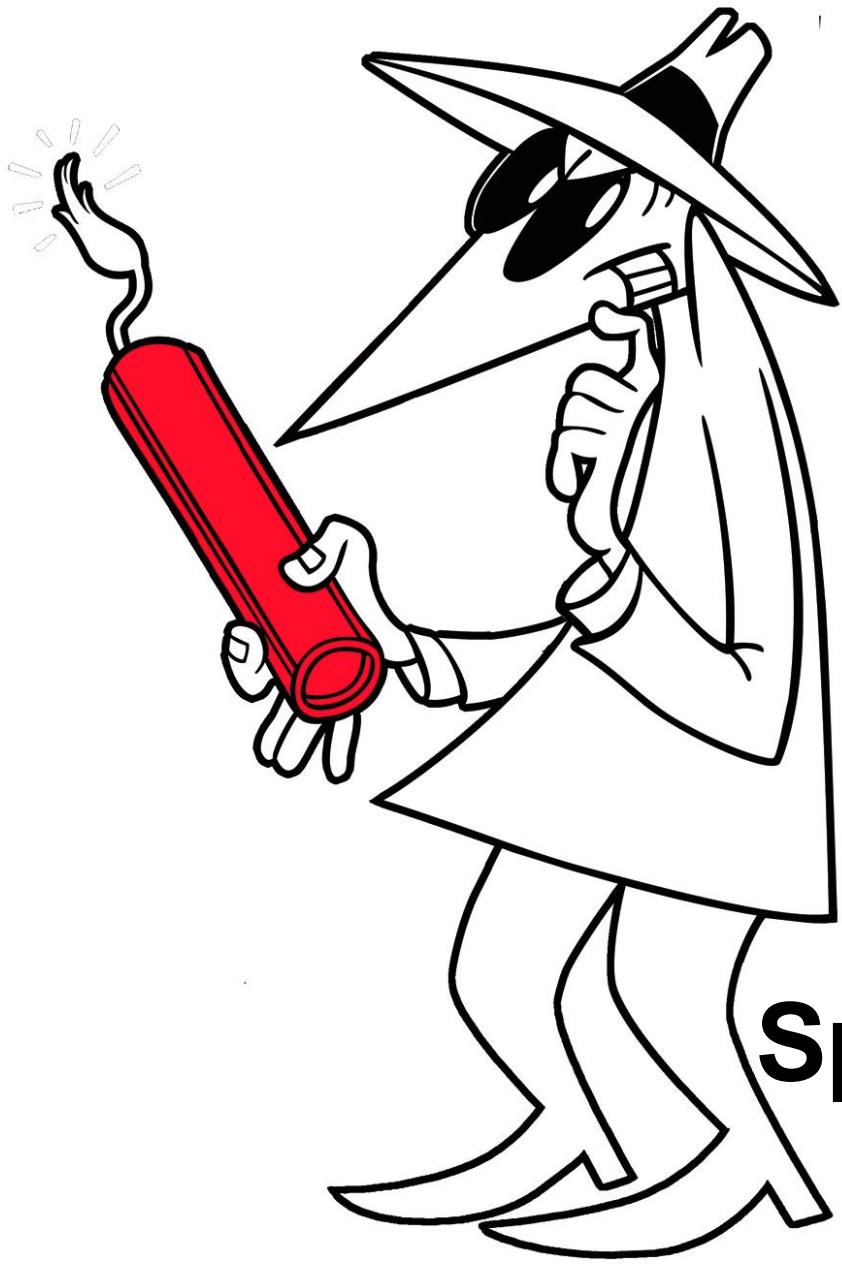


**What are good
procedures?**

What makes a good Mobile Forensic Tool?

- **Is it read only?**
 - Yes
 - No
- **Can I repeat my results?**
 - What are your validation steps?
- **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?





Spyware

Trend 5. Spyware

- Yes, but it is not easy!
- Not traditional
 - Designed as a consumer wire tap
 - Legal Issues
 - Install Issues
 - Required Services



BlueStealth

- Bluetooth System Spy Tool

Just Awarded **Software of the Year** by Softglare Magazine.

Track your child's cell phone activity
Catch that cheating spouse

ALL OF THIS INCLUDED



IN ONE COMPLETE SOFTWARE PACKAGE

NEW 2009 Edition!

MORE BANG FOR YOUR BUCK & MORE COMPATIBLE THAN EVER



Bluestealth

Implementing the same technology used by law enforcement agencies around the world. PI's. FBI. CIA.

Now LEGAL for you!

The very latest technology and programs to allow you to spy on any bluetooth enabled device, mobile phone, or laptop - our technology covers them all.

- **VIEW CONTACTS LIST**
- **READ TEXT MESSAGES (SMS)**
- **VIEW CALLS MADE / CALLS RECEIVED**
- **SET THE TARGET PHONE TO CALL YOU WHENEVER IT MAKES OR RECEIVES A CALL**
- **VIEW PHOTOS**
- **...AND MUCH MORE**

ALL THE ABOVE INFORMATION CAN EASILY BE DOWNLOADED TO YOUR PHONE

BUY FROM A TRUSTED SOURCE

Certified and Verified by Trust-Guard for your protection.
Our competitors can't say that!

Big Daddy is committed to catching CHEATERS!

See our most recent Ad on



ULTIMATE BLUETOOTH CELL PHONE SPY SOFTWARE

COMPLETE PACKAGE

INSTANT DOWNLOAD!

Nothing will be mailed
No wait!

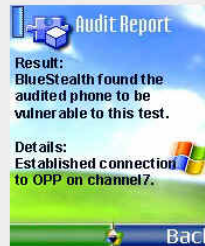
Bluestealth

MAKE CALLS VIA THE PHONE YOU HAVE TARGETED

into calls.

There is no trace or logging of your phone's details on the target phone

That means: **THEY WILL NEVER KNOW**



No need to carry on wishing you knew what was going on...no need to wish you had those vital contact numbers..you can easily find out today. Why punish yourself any longer?

Think that your wife is secretly text messaging at night?

Or that your husband is making secret calls when you're not paying attention?



We **GUARANTEE** BlueStealth 2008 will work on **All** mobile devices that are bluetooth enabled. Not just phones but also laptops, computers, etc. **YOU WILL RECEIVE SEPERATE SOFTWARE FOR OLD MODELS AND NEW MODELS (INCLUDING SYMBIAN PHONES).** We don't need to list compatible phones - this works on **ALL** phones!

Bluestealth

PLEASE READ our 3 easy steps for installation:



- Instantly download the software by clicking the link below.
- Save the software to a location you will easily remember
- Open/Run the file you downloaded by double-clicking on the EXE or ZIP file.



- Now that you have the software on your PC, move the JAR files to your phone
- Please refer to your Phone's users guide for instructions on transferring files.



- Target a phone and begin spying immediately



If you have any trouble, please submit a ticket via our Support Ticket System, or call our Toll Free Support Line at 1-877-467-5311

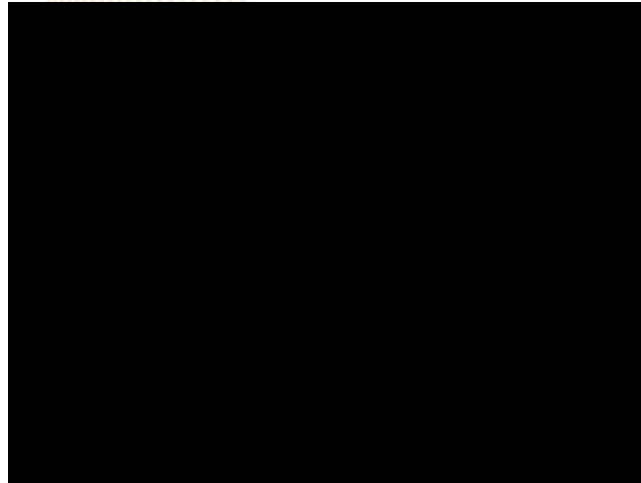
Bluestealth

It is a federal and state offense to install surveillance software onto a phone which you do not have proper authorization.

We absolutely do not condone the use of our software for illegal purposes.
In order to register you MUST agree to the following conditions.

- 1.** You acknowledge and agree that you own the mobile phone you will install the software onto OR that you have the expressed written consent of the owner to be an authorized administrator of the phone and its users.
- 2.** If you install our software onto a phone which you do not own or have proper consent, we will cooperate with law officials to the fullest extent possible. This includes turning over requested customer data, and any other purchase/product related information.
- 3.** You agree that you will check all local, state and federal laws to make sure you are complying with all laws in your region. It may be illegal in your region to monitor other individuals on your own device. You will never monitor any adult without their valid permission.
- 4.** You agree that we are not liable for any type of damage, litigation, or legal predicaments that may arise due to use or abuse of E-Stealth or any other PhoneStealth.com product.

Trend 6. New Communication



Text Messaging

- IDK
- WWSD
- TTYL
- ?4U
- 121
- LBAY
- LH6
- LGH
- LHSX
- LMIRL
- 4COL
- LOL
- ROFL
- 6Y
- 831
- 9
- LULT
- MoF
- MOS
- MTFBWU
- AITR
- N1
- NIFOC
- AYS

Text Messaging Decoded

- IDK-I don't know
- WWSD-What would Spock do?
- TTYL-Talk to you later
- ?4u-Question for you
- 121=private chat
- LBAY-Laughing Back at you
- LH6-Lets have sex
- LGH-Lets get high
- LHSX-lets have sex
- LMIRL-lets meet in real life
- 4COL-for crying out loud
- LOL-Laugh out loud
- ROFL-Roll on floor laughing
- 6Y-sexy
- 831 -I love you (8 letters, 3 words, 1 meaning)
- 9-parent is watching
- LULT-love you long time
- MoF-male or female
- MOS-mother over shoulder
- MTFBWU May the force be with you
- AITR-Adult In the Room
- N1-nice one
- NIFOC-naked in front of computer
- AYS-Are you serious

Decisions to be made

- Do you process it yourself?
- Who do you hire?
- Do you know what you should be doing?
- Are you ignoring potential facts?

Trend 7. The Future



The Global Market is HUGE



Clones



Meizu miniOne



Teclast T59



LG Prada KE850



ASUS Aura



iSoftPhone



MeeGo

MeeGo operating system is ready to run devices including touch screen tablets and phones. MeeGo is a Linux-based, open source project created by merging Intel's Moblin and Nokia's Maemo operating system projects early this year.



ON THE RADAR

A sneak peek at your mobile future.

by Sean Ludwig

Who's at the Wheel? Google

No one ever said Google wasn't driven. The search giant recently demonstrated cars that drive themselves using sophisticated artificial-intelligence software. In theory, these vehicles could eliminate accidents and speeding tickets, and the "driver" could watch a movie or catch up on work instead of driving.

There are obvious safety benefits to computer-controlled car. The World Health Organization estimates more than 1.2 million lives are lost in traffic accidents each year, and Google believes it could cut that number by as much as half with its autonomous vehicles.

Google has deployed modified Toyota Prius vehicles with an array of tech tacked on. The cars are equipped with a position estimator, a rotating sensor on the roof (for generating a 3D map of the vehicle's surroundings), a video camera near the rear-view mirror (for detecting traffic lights and moving obstacles), and four radar sensors (for determining the position of distant objects). Add in a GPS receiver and an inertial motion sensor, and it's easy to see how Google's seven test cars have logged more than 140,000 miles with only occasional human intervention—and 1,000 miles without any.

To be clear, Google hasn't completely ceded the future to robots. Each Google car has a human driver in case something goes wrong. So far, the company has reported only a single accident—and it was because someone rear-ended the car.

"We've always been optimistic about technology's ability to advance society, which is why we have pushed so hard to improve the capabilities of self-driving cars beyond where they are today," wrote Sebastian Thrun, a Google software engineer, on Google's official blog. "While this project is very much in the experimental stage, it provides a glimpse of what transportation might look like in the future thanks to advanced computer science."



PC + Phone + Projector

The Mozilla Seabird concept phone merges the benefits of a full computer with the mobility of a handset. The phone is the result of Mozilla Labs' open call for ideas from the Mozilla Foundation community. Conceptualized by product designer Billy May, the Seabird was created with the goal of showing how users might one day interact with their mobile devices.

While the Seabird looks like a slab-style smart phone with a large screen, the sides are anything but standard: Two pico projectors are installed. For productivity, the phone can be docked to project images of a monitor and keyboard

onto flat surfaces. The user will then be able to

Reading, the Video Game

Staffers at design firm IDEO must have enjoyed "Choose Your Own Adventure" books when they were kids because the company's new "Alice" concept takes that idea into the future. Alice is tablet-based software that lets the reader be part of the narrative. As you read along, you get to communicate with characters, unlock plot twists, and solve puzzles.

Today's enhanced eBooks offer a glimpse of this capability with short videos or pictures added to stories, but Alice is more involved and adds a videogame-like element to the reading experience. The goal? To blur the line between reality and fiction, and literally influence how



Nokia Universal Inbox

- One box to rule them all
 - E-mail
 - Text
 - Call Logs
 - Tweets
 - Facebook Updates
 - Flickr

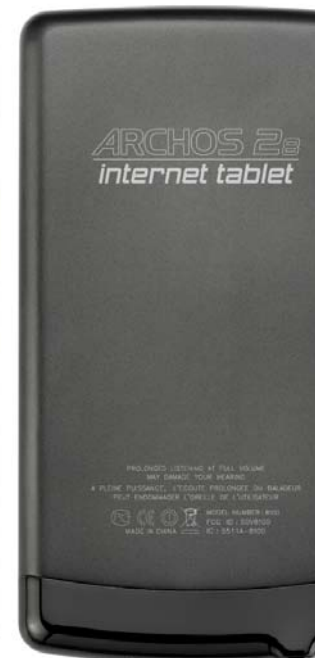


PORTABLE DEVICE SALES COMPARED

(in millions of units)

| | July 2008 to 2009 | July 2009 to 2010 |
|------------------------------|----------------------|-----------------------|
| GPS NAVIGATORS | 8.7 million | 9 million ▲ 3% |
| PORTABLE GAMING DEVICE | 14.2 million | 12.3 million ▼ 13% |
| DIGITAL CAMERA | 21.6 million | 20.7 million ▼ 4% |
| MP3 PLAYER | 25.3 million | 21.8 million ▼ 14% |
| | 2009 | 2010 |
| SMART PHONES | 173.5 million | 270 million ▲ 56% |

Sources: The NPD Group and IDC



Wristy business **Griffin Slap Case** £20 | griffintechology.com

Nothing says the '80s like a nice splash of eyeball-assaulting colour. Like a cross between a squashed Rubik's Cube and a retro digital Casio, the Slap houses your iPod Nano in a watch-shaped silicone case that wraps around your wrist. There's a hole in the side to attach your earphones and you can choose from a whole rainbow of hues including blue, black, pink, red, purple, orange, green and yellow. Pick one to match your shell suit.



ANNUAL NOTEBOOK BUYERS' GUIDE 10 THINGS YOU NEED TO KNOW p. 50

LAPTOP

THE PULSE OF MOBILE TECH

LONGEST-LASTING
ANDROID PHONES p. 41

BEST SUB-\$100
NOTEBOOK UPGRADES p. 64

SHOPPING APPS
THAT HELP YOU SAVE p. 58

TABLET EXPLOSION

THE iPad IS JUST THE BEGINNING...

HOTTEST SLATES
PREVIEWED p. 64

DOES GOOGLE KNOW TOO MUCH ABOUT YOU? p. 72



\$5.99

11

November 2010 www.laptopmag.com

PFIC



Paraben's Forensic Innovations Conference

To learn more about mobile forensics you can
attend Paraben's Annual PFIC Conference

Nov 5-9 in Park City, Utah

www.pfic-conference.com

\$99.00 to Attend for 3 Days of Training Special ISSA-DC

Contact Details



Amber Schroader

Chief Executive Officer 'The Geek'

e-mail: amber@paraben.com

phone: 703.595.2979

cell: 801.319.6347